



Chambers Global Practice Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy 2022

Japan: Law & Practice
Yoshifumi Onodera, Hiroyuki Tanaka
and Naoto Shimamura
Mori Hamada & Matsumoto

practiceguides.chambers.com

Law and Practice

Contributed by:

*Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura
Mori Hamada & Matsumoto see p.22*



CONTENTS

1. Basic National Regime	p.3	4. International Considerations	p.17
1.1 Laws	p.3	4.1 Restrictions on International Data Issues	p.17
1.2 Regulators	p.4	4.2 Mechanisms or Derogations that Apply to International Data Transfers	p.18
1.3 Administration and Enforcement Process	p.5	4.3 Government Notifications and Approvals	p.18
1.4 Multilateral and Subnational Issues	p.5	4.4 Data Localisation Requirements	p.18
1.5 Major NGOs and Self-Regulatory Organisations	p.5	4.5 Sharing Technical Details	p.18
1.6 System Characteristics	p.5	4.6 Limitations and Considerations	p.18
1.7 Key Developments	p.5	4.7 "Blocking" Statutes	p.18
1.8 Significant Pending Changes, Hot Topics and Issues	p.5	5. Emerging Digital and Technology Issues	p.18
2. Fundamental Laws	p.6	5.1 Addressing Current Issues in Law	p.18
2.1 Omnibus Laws and General Requirements	p.6	5.2 "Digital Governance" or Fair Data Practice Review Boards	p.20
2.2 Sectoral and Special Issues	p.10	5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.	p.20
2.3 Online Marketing	p.13	5.4 Due Diligence	p.20
2.4 Workplace Privacy	p.13	5.5 Public Disclosure	p.21
2.5 Enforcement and Litigation	p.14	5.6 Other Significant Issues	p.21
3. Law Enforcement and National Security Access and Surveillance	p.15		
3.1 Laws and Standards for Access to Data for Serious Crimes	p.15		
3.2 Laws and Standards for Access to Data for National Security Purposes	p.16		
3.3 Invoking Foreign Government Obligations	p.16		
3.4 Key Privacy Issues, Conflicts and Public Debates	p.16		

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

1. BASIC NATIONAL REGIME

1.1 Laws

Major Laws

The Act on the Protection of Personal Information (APPI) is the principal data protection legislation in Japan. It provides the basic principles for the government's regulatory policies and authority, as well as the obligations of private business operators who handle personal information (the handling operator). An amendment to the APPI was approved in June 2020, which will fully come into force on 1 April 2022.

Another set of amendments to the APPI was also approved in May 2021. Currently, national administrative bodies are regulated by the Act on the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Independent Administrative Agencies. One of the main purposes of the 2021 amendments is to integrate the obligations prescribed in these two laws into the APPI. The amendments relating to the foregoing integration will be effective from 1 April 2022.

In addition, local government bodies are regulated under their own local regulations (*kyorei*), but these vary from one body to the other. The 2021 amendments to the APPI will introduce nationwide principles for *kyorei* and related implementing guidelines to homogenise the administration of national data protection regulations. Under this set of amendments, standard rules regarding personal information handled by local governments are uniformly stipulated in the APPI, and *kyorei* can only stipulate local rules in very limited situations allowed under the APPI. The aforesaid amendments will be effective from the spring of 2023 (the effective date has not been announced yet).

This article will treat the APPI as if the new amendments set to take effect on 1 April 2022 have already taken effect.

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.

There are no laws or regulations that target artificial intelligence (AI) at this time. Please refer to **5.1 Addressing Current Issues in Law** (Artificial Intelligence (including Machine Learning)) for more details.

Furthermore, the Personal Information Protection Commission (PPC), which is the regulator primarily responsible for the APPI and the My Number Act, 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 (FSA) and the PPC have jointly published data protection guidelines for the financial sector, and the Ministry of Internal Affairs and Communications (MIC) has issued data protection guidelines for telecommunication business operators.

Enforcement and Penalty Trends

For the period from 1 April 2021 to 30 September 2021, no administrative orders were issued, one administrative recommendation was made, 113 issuances of administrative guidance or advice were made and 179 administrative requests for reports and materials were made under the APPI. The reason that few administrative orders or recommendations have been issued is because ordinary companies were in compli-

ance with the PPC's administrative guidance and advice. Moreover, companies are typically concerned with their social reputation and, thus, endeavour to comply with laws and regulations.

Key Concepts and Terminology

In order to understand the regulations under the APPI, it is important to distinguish between three key categories: personal information, personal data and retained personal data.

The APPI defines personal information as information about living individuals that (i) can identify specific individuals or (ii) contains an individual identification code (Article 2.1).

Information that 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, information collected by cookies by itself is not personal information; however, if the handling operator can easily collate information collected by cookies with the name of the individual (which typically occurs when registered customers log in to the website of a company, and the company knows the cookie ID of the registered customer), the information collected by the cookies will be deemed to be personal information.

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 that 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 them 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 data means personal information contained in a personal information database (Article 16.3), 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 16.1).

Retained personal data means personal data that a handling operator has the authority to disclose, correct, add, or delete content from; discontinue the use of; erase; or discontinue the provision of to a third party, excluding certain limited personal data (Article 16.4).

1.2 Regulators

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

- to require a handling operator to report or submit materials regarding its handling of personal information and to enter a handling operator's offices or other places to investigate, make enquiries and check records or other documents (Article 143);
- to provide guidance or advice to a handling operator (Article 144);

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

- to recommend that a handling operator cease any violation of the APPI and take other necessary measures to correct the violation (Article 145.1);
- to 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 145.2 and 145.3); and
- when the PPC issues an order pursuant to Articles 145.2 and 145.3, and a handling operator violates the order, the PPC may publicly announce the violation (Article 145.4).

1.3 Administration and Enforcement Process

The PPC does not have the authority to conduct criminal investigations and the APPI explicitly stipulates that the PPC's power to conduct on-site inspections does not include criminal investigations (Article 143.3).

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 or makes any false report in response to an investigation by the PPC (Article 173), provides to unauthorised persons or misuses a personal information database for unlawful gains (Article 175), or violates any order given by the PPC as a part of an administrative sanction (Article 176). Please also see **2.5 Enforcement and Litigation**.

1.4 Multilateral and Subnational Issues

While local governments have enacted *kyorei* on data protection, those regulations are applicable only to the public sector. Please note that, from the spring of 2023, *kyorei* will be regulated by the APPI, as discussed in **1.1 Laws**.

1.5 Major NGOs and Self-Regulatory Organisations

The PPC accredits private organisations called accredited personal information protection organisations (*Nintei Kojin Jyohou Hogo Dantai*) to handle and promote the protection of the personal information of handling operators. These accredited organisations process complaints against handling operators or provide information on them 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 Organisation for Economic Co-operation and Development's eight Privacy Principles. Japan has reached an agreement with both the EU and the UK to certify each other's country or territory as an "adequate" country for Japan's and the EU/UK's data protection purposes; however, this does not mean that the APPI is identical to Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR).

Japanese data protection law is, nonetheless, closer to the EU omnibus model than the US sectoral/subnational approach, in the sense that Japan has a comprehensive data protection law, the APPI.

1.7 Key Developments

As discussed in **1.1 Laws** (Major Laws) the APPI was amended in 2020 and 2021.

1.8 Significant Pending Changes, Hot Topics and Issues

As explained in **1.1 Laws** significant portions of the APPI amendments, which were approved in 2020 and 2021, will come into force on 1 April 2022, while the remaining part is expected to be effective from Spring 2023. In line with the

amendment of the APPI, the relevant Cabinet Order, the PPC Ordinance, guidelines, and FAQs of the APPI will also be updated.

2. FUNDAMENTAL LAWS

2.1 Omnibus Laws and General Requirements

Handling Operator Duties

The various obligations of a handling operator under the APPI, are set out below.

It must specify and make known to the data subject the purpose of collecting their personal information (Articles 17 and 21).

It cannot use personal information for any other specified purpose without the consent of the data subject (Article 18). Exceptions to the consent requirement include instances when the use is required by law, or is necessary to perform governmental duties, to protect the life, body or property of a person, or to improve public health (Article 18.3). A handling operator must not utilize personal information in a way that entails the possibility of fomenting or prompting unlawful or unfair acts (Article 19).

It has to establish appropriate safeguards to protect personal data (Article 23).

It cannot transfer personal data to another entity without the opt-in consent of the data subject, unless it meets the requirements of any of the exceptions provided by the APPI (Article 27.1). These exceptions include instances when the transfer is required by law; is necessary to perform governmental duties; is necessary to protect the life, body or property of a person; is necessary to improve public health; or is necessary for academic or research purposes (Article 27.1(i) through (vii)). Other major exceptions include cases of entrustment of the handling of

personal data to another entity, joint use of the personal data with another entity, business succession resulting from a merger or other legal reasons (Article 27.5), or the filing of a notification of opt-out consent with the PPC (Article 27.2), as detailed in other sections below.

It cannot transfer personal data to countries that do not have sufficient data protection safeguards without the consent of the data subject (Article 28). For details, please see **4.1.Restrictions on International Data Issues**.

It must keep a record of the provision of personal data to a third party (Article 29).

Upon receiving personal data from another handling operator, it must confirm the providing handling operator's compliance with applicable regulations regarding the provision of the personal data and keep a record of the confirmation process (Article 30).

It must handle pseudonymously processed information and anonymously processed information in certain ways (Article 41 to 46).

The 2020 amendments to the APPI introduced mandatory obligations to report data breach incidents to the PPC and to notify affected data subjects in cases where their rights and interests are likely to be infringed (Article 26).

Entrustment

Under Article 27.5 (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 27.1.

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

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

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 data, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted personal data (Article 25).

Joint Use

A handling operator may share and jointly use personal data with specific individuals or entities as long as the handling operator, before any information sharing and joint use, notifies the data subject or makes the following information accessible to them (Article 27.5(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 (the address of the responsible individual or entity, and if it is a corporate body, the name of its representative, are also required).

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 27 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.

Business Succession

A handling operator may transfer personal data to a third party without the opt-in consent of data subjects if the transfer accompanies a business succession caused by a merger or other legal reason (Article 27.5 (ii)).

Filing of Notification of Opt-Out Consent

Under Article 27.2 of the APPI, a handling operator may provide personal data (excluding special-care-required personal information and personal data which was acquired by improper means or provided by another handling operator pursuant to the opt-out mechanism) to a third party without the opt-in consent of data subjects if the following conditions are satisfied:

- it agrees to stop providing personal data to the third party upon the demand of the data subject;
- it notifies the data subjects in advance of certain matters set forth in Article 27.2 or makes such notification of matters readily accessible to the data subject; and
- it submits a notification of certain matters to the PPC.

Please note that, in practice, the PPC does not readily accept the foregoing opt-out notification unless it is not practical to seek the data subjects’ consent and it is difficult to use the other exceptions.

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 the 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 such handling;
- HR security measures, including educating/training employees;

*Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura,
Mori Hamada & Matsumoto*

- physical security measures, including controlling the area where personal data is handled, such as servers and offices;
- technical security measures, including controlling access to personal data; and
- understanding of the external environment – this security measure, introduced by the amendments to the guidelines, requires a handling operator which processes personal data in a foreign country to understand the foreign country’s legal system for personal information protection and, taking into consideration that legal system, to take necessary and appropriate measures to ensure the security of personal data.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of personal data 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.

Privacy by Design/Default and Privacy Impact Analyses

The APPI does not mandate obligations regarding privacy impact analyses, but the PPC has issued a report titled “Promoting the implementation of PIA—Significance of PIA and points to keep in mind in the implementation procedure” and encourages business operators to follow the report voluntarily. The APPI does not refer to the concepts of privacy by design or by default, but PPC guidelines on accredited personal information protection organisations recommend that these organisations promote privacy by design.

Internal or External Privacy Policy

The PPC Guidelines recommend releasing a privacy policy or statement.

Article 32.1 of the APPI requires handling operators to make the following information regarding retained personal data available to data subjects:

- the name of the handling operator, an address for the responsible individual or entity, and if it is a corporate body, the name of its representative;
- the purposes of the use of retained personal data;
- the procedures for responding to requests from data subjects to disclose, correct, suspend, or erase the use of retained personal data;
- contact information for accepting complaints regarding the processing of retained personal data; and
- security measures being implemented by the handling operator.

Most handling operators typically comply using internal and external privacy policies.

The PPC Guidelines also recommend stating the following in a handling operator’s basic policies as security control measures regarding personal data:

- the name of the handling operator;
- compliance with the relevant laws, regulations and guidelines;
- an explanation regarding security control measures regarding personal data; and
- contact details for complaints and questions.

Most handling operators typically comply using internal and external privacy policies.

The PPC Guidelines also recommend being transparent in disclosing entrustment of work involving personal data (eg, disclosing whether entrustment has been made and what kind of work has been entrusted).

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

Data Subjects' Rights

A data subject may request a handling operator to disclose their retained personal data and the record of the provision of their personal data to a third party. The handling operator must comply with the request, unless there is a possibility that the disclosure could harm the data subject's or a third party's life, body, property or other rights and interests, or could seriously interfere with the handling operator's business (Article 33).

A data subject may also request a handling operator to correct, add to or delete retained personal data. The handling operator must investigate without delay and, based on the results of the investigation, comply with the request to the extent necessary to achieve the purposes of use of the retained personal data (Article 34).

Furthermore, 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:

- that data was or is being acquired, processed or provided to a third party in violation of the APPI;
- the retention of retained personal data has become unnecessary;
- a data breach has occurred regarding the retained personal data; or
- there is a possibility that the handling of the retained personal data would harm the rights or legitimate interests of the data subject.

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 (Article 35).

The APPI has no provision on data portability.

Anonymisation, De-identification or Pseudonymisation

The APPI recognises the concept of anonymously processed information, which 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 2.6). This framework intends 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. 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 (Article 43.1);
- takes measures for security control in compliance with the standards set forth in the PPC Ordinance to prevent leakage (Article 43.2);
- discloses items that will be included in the anonymously processed information pursuant to the PPC Ordinance (Article 43.3);
- 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 (Article 43.4);
- does not do anything to identify the individual (Article 43.5); 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 43.6).

According to the PPC Guidelines, statistical information, meaning information that can be obtained by extracting items concerning a common element from information taken from several people and tallying them up by category, is not anonymously processed information because statistical information is not information regarding an individual and, thus, is not covered by any regulations under the APPI.

The 2020 amendment of the APPI introduces the concept of pseudonymously processed information. This is information that is processed so that it cannot be used to identify a specific individual without collation with other information (Article 2.5). Pseudonymously processed information is exempted from certain regulations under the APPI, such as restrictions on changing the purpose of use and the obligation to comply with the data subject's rights, and report/notification obligations in the case of a data breach (Article 43).

Profiling, Microtargeting, Automated Decision-Making, Online Monitoring or Tracking, Big Data Analysis and Artificial Intelligence

There is no specific statutory law on microtargeting, online monitoring or tracking. However, any activity relating to the collection, use and provision of personal information will be subject to the rules of the APPI.

Under the 2020 amendment of the APPI, certain types of cookies, web beacons, online identifiers, and so forth are subject to new regulations. Under the APPI, the transfer of personal data to third parties – and the question of whether the data is personal data or not – is judged based on the circumstances surrounding the transferor, not the transferee. In brief, if the data is not personal data in the hands of the transferor, regulations regarding the transfer of personal data to third parties are not applicable. In recent years,

some schemes have emerged whereby data management platforms provide non-personal information such as user data collected by cookies (eg, user browsing histories/interests and preferences) to third parties, with the knowledge that the data will be personal data in the hands of the recipient. The PPC was concerned by the expansion of this kind of data sharing without the involvement (control) of the data subjects. As a result, the concept of personally referable information is introduced and is defined as a collective set of information comprising information relating to a living individual which does not fall under personal information, pseudonymously processed information or anonymously processed information but which has been systematically organised so as to be searchable using a computer for specific personally referable information or similar information prescribed by Cabinet Order. The amended APPI regulates the provision of personally referable information if the provider assumes that a recipient will acquire a database of the provided personally referable information as personal data. In this case, the transferor must confirm that the transferee has obtained the consent of the data subjects to the transfer of their data as personal data.

See **5.1 Addressing Current Issues in Law** for other items relating to profiling, microtargeting, automated decision-making, big data analysis and artificial intelligence.

Injury/Harm

There is no definition of “injury” or “harm” under the APPI. However, an infringement of privacy is a tort under the Civil Code if the individual suffers from mental burden or mental uneasiness regarding the disclosure of information.

2.2 Sectoral and Special Issues

Health Data

The APPI contains the concept of special-care-required personal information, which is defined

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

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 (Article 2.3). The handling operator must get prior consent to obtain special-care-required personal information (Article 20.2) and transfer the same (opt-out consent is not allowed) (Article 27.2).

The Act Regarding Anonymised Medical Data to Contribute to Research and Development in the Medical Field (the so-called Medical Big Data Act) was enacted. Under this act, government-accredited medical information anonymisation entities can obtain medical information from medical institutions (eg, hospitals) unless the data subjects opt out. Those entities are entitled to anonymise the acquired medical information and distribute the anonymised medical information for the purpose of R&D in the medical area.

Financial Data

Financial data is not categorised as special-care-required personal information; however, if the information can identify an individual then the financial data will be treated as ordinary personal information.

Communications Data

A voice recording by voice telephony itself is not personal information, but can be considered as such if the speaker can be identified from its contents or with other information. Even if a 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, the Telecommunication Business Act (TBA), the Radio Act and the Wire Telecommunications Act, which specifically protect the secrecy of telecommunication data.

The same applies to text messaging.

Other Categories of Sensitive Data

Information on political or philosophical beliefs generally falls within special-care-required personal information as a personal belief.

The APPI has no provision on personal information related to union membership or sexual orientation. However, since that type of information is protected under the GDPR, the PPC has issued Supplementary Rules under the APPI for the handling of personal data transferred from the EU based on an adequacy decision, which provides that if any information is transferred from member countries of the EEA and the UK based on an adequacy decision, the information must be protected under the same standards as special-care-required personal information. In addition, data protection guidelines for the financial sector, published jointly by the FSA and the PPC, stipulate that information on union membership and sexual orientation is considered sensitive information and financial companies should not acquire, use or collect any such information unless specific exceptions apply.

Internet

There is no mandatory requirement under the APPI to set up privacy policies; however, as explained in **1.1 Laws** (Key Concepts and Terminology), it is common and highly recommended for handling operators who have websites to publish their privacy policy on their websites.

The use of cookies, web beacons and other tracking technology is not directly regulated under the APPI. Information collected by cookies or web beacons is not personal information; however, if the handling operator can easily collate information collected by cookies or web beacons with the name of the individual (for example, when an internet-based company is able to identify the cookie ID of customers when logged in to its website), the information collect-

*Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura,
Mori Hamada & Matsumoto*

ed by cookies or web beacons will be deemed to be personal information.

Behavioural advertising is not directly regulated under the APPI, but any personal information collected to provide behavioural advertising is subject to the APPI.

It is good practice to have a cookie policy and to offer an opt-out from the use of cookies (especially behavioural advertising). The Japan Interactive Advertising Association's Guidelines are useful for an understanding of good practice in Japan.

The 2020 amendment of the APPI introduced regulations for certain cookies, web beacons, and other tracking technology underlying behavioural or targeted advertising. Please see **2.1 Omnibus Laws and General Requirements** (Profiling, Microtargeting, Automated Decision-Making, Online Monitoring or Tracking, Big Data Analysis and Artificial Intelligence).

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 a 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 then the provider will be subject to the 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 indi-

vidual wanted his criminal record deleted from search results. While the Court of First Instance admitted the individual's right to be forgotten, the Supreme Court did not mention the right to be forgotten in its decision on appeal and 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 exists, 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.

Intermediary Liability for User Generated Content

Under the Provider Liability Limitation Act, even if an online platform has distributed information posted by a third party which infringes the rights of another person, the general rule is that the service provider will not be liable unless it is aware of or has a good reason to be aware of the infringement.

Children's Privacy

A Q&A issued by the PPC states that for minors between the ages of 12 and 15, the consent of a person with parental authority over the minor must be obtained for data processing which requires the consent of data subjects (eg, provision of personal data to third parties and collection of special-care-required personal information).

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

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

Rights to Object to Sale of Data and Tracking

There are no rights to object to the sale of personal data, but the APPI sets forth a similar scheme regarding the provision of personal data. In general, providing personal data to a third party is permissible only with consent or under an opt-out mechanism. If a data subject does not want their personal data to be provided or sold to another entity, then they should either withhold their consent or object to any such provision/sale (opt-out.) For more details of opt-out, please see **2.1 Omnibus Laws and General Requirements** (Filing of Notification of Opt-Out Consent). As for tracking, the APPI will introduce some regulations. Please see **2.1 Omnibus Laws and General Requirements** (Profiling, Microtargeting, Automated Decision-Making, Online Monitoring or Tracking, Big Data Analysis and Artificial Intelligence).

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.

Furthermore, the Act on Special Commercial Transactions has restrictions on marketing regarding mail order businesses, including online shopping, but does not provide for excep-

tions similar to items (ii) to (iv) of the preceding paragraph.

As discussed in **2.1 Omnibus Laws and General Requirements**, behavioural and targeted advertising is not directly regulated under the APPI, but any personal data collected to provide behavioural and targeted advertising is subject to the APPI. There are no specific restrictions for behavioural and targeted advertising. However, the latest amendment of the APPI will introduce some regulations governing the underlying technology of behavioural and targeted advertising. Please see **2.1 Omnibus Laws and General Requirements** for more details.

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

The Ministry of Health, Labour and Welfare 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.

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

The employer has the right to monitor workplace communications in relation to work and to use cybersecurity tools and insider threat detection

and prevention programmes, and digital loss prevention technologies, but a privacy issue may arise regarding private communications and other privacy matters at the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and email addresses for private use, and disclose the possibility of monitoring those devices and data including e-mails.

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 Whistle-Blower Protection Act prohibits employers from dismissing whistle-blowers. The Act itself does not have requirements for companies to have whistle-blower hotlines or systems, but the Consumer Affairs Agency has published guidelines for private entities to establish and operate whistle-blower hotlines. The guidelines also specify several measures that 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

The PPC has power to enforce administrative sanctions. Please see **1.2 Regulators** for the details of administrative sanctions.

Please see **1.1 Laws** for recent statistics about administrative sanctions enforced by the PPC. From May 2017, when the PPC became the regulator and enforcement authority of the APPI, until August 2019, the PPC had not issued any official recommendations or administrative orders. However, subsequently, the PPC has issued them for cases entailing a large social

impact. For example, on 26 August 2019, the PPC first made an official recommendation to a company operating an online job platform. It was considered that the company captured users' likelihood of declining a job offer based on their web browsing history and sold the data to potential employers. The PPC decided that the company did not comply with the required procedures under the APPI.

On 29 July 2020, the PPC first issued two administrative orders regarding non-compliance with an official recommendation. In these cases, two anonymous internet-based companies published the personal data of bankrupts, including names and addresses in violation of required procedures in the APPI.

Please note that even after May 2017, the PPC entrusts its enforcement powers to relevant public authorities for some industries.

Criminal Sanctions

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) 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 one year, or a fine of up to JPY1 million (Article 173). If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY one hundred million (Article 179.1 (i)).

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 such a database for unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

JPY500,000 (Article 175). If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY100 million (Article 179.1 (i)). 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 JPY500,000 (Article 176). If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY500,000 (Article 179.1 (ii)).

The APPI does not provide the legal procedures that the PPC or the prosecutors must follow 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.

Private Actions

A data subject may go to court to seek compensation for damages or distress caused by the breach of data protection. There are two major types of legal causes. Firstly, Japanese courts recognise the right to privacy, which is the right of a person not to have their private life disclosed except for a legitimate reason. A breach of the right to privacy consists of torts under Article 709 of the Civil Code. Secondly, if a business promises to keep personal data confidential in an agreement such as terms of use, but then compromises the data, the legal cause of breach of contract may also be available.

Class actions

The Act on Special Measures Concerning Civil Court Proceedings for Collective Redress for Property Damage Incurred by Consumers allows for 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, as a practical matter, a number of data subjects may select the same lawyer to represent them and that lawyer can file one litigation for those 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, names, birth dates, addresses, and telephone numbers). The case was remanded to the Osaka Appeal Court, which awarded JPY1,000 to the claimant on 20 November 2019. In addition, the Tokyo Appeal Court awarded JPY3,300 to other plaintiffs on 25 March 2020 for the same data breach. The Supreme Court denied appeals of these cases in December 2020; thus, these Appeal Court decisions are deemed final.

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 to 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 considered as being subject to the restrictions discussed in **3.1 Laws and Standards for Access to Data for Serious Crimes**.

Judicial review acts as a safeguard to protect privacy.

3.3 Invoking Foreign Government Obligations

Without relying on international assistance in investigation schemes, a foreign government may not forcibly request a Japanese entity to turn over personal information. In addition, a handling operator may face a problem if it voluntarily gives personal data to a foreign government. The reason is that 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 27.1). These specified cases are where the provision of personal data is:

- based on laws;
- necessary to protect the life, body or property of an individual and it is difficult to obtain the consent of the data subject;
- specially necessary to improve public hygiene or promote the sound growth of children and it is difficult to obtain the consent of the data subject;

- 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; or
- necessary for academic or research purposes.

It is understood that a “state institution” referenced in the fourth point above refers only to the Japanese government and not foreign governments, and the “laws” referenced in the first point above do not include foreign laws.

If a handling operator is required to disclose the personal data of Japanese residents in accordance with a foreign law or by the action of a foreign governmental institution, it may use the exception in the second point 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.

Japan does not participate in a Cloud Act agreement with the United States of America.

3.4 Key Privacy Issues, Conflicts and Public Debates

As discussed in **1.1 Laws (Major Laws)**, 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.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

While there were discussions concerning the introduction of the My Number, and there was dissenting public opinion, the system has now been fully implemented and the scope of its use is slowly expanding. From January 2018, it has been used in the financial sector; for example, to obtain information regarding bank saving accounts. The government uses My Number to manage COVID-19 vaccination status.

4. INTERNATIONAL CONSIDERATIONS

4.1 Restrictions on International Data Issues

Basic Regulation

There are special restrictions on the transfer of personal data to a foreign country. In principle, the APPI requires the transferor to obtain the prior consent of individuals whose personal data will be transferred to a third party located in a foreign country (Article 28). 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 cases of entrustment and joint use, which are exceptions to local third-party data transfer restrictions. The data subjects' consent to overseas data transfers is not necessary only if the following applies.

- The foreign country is designated by the PPC as a country with a data protection regime with a level of protection equivalent to that of Japan (only member countries of EEA and the UK have been designated to date).
- The third-party recipient has an equivalent 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 data in accordance with the spirit of the requirements for handling personal data under the APPI; or
- (b) the recipient has been certified under an international arrangement, recognised by the PPC, regarding its system of handling personal data.

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 data importer and the data exporter, or inter-group privacy rules, which ensure that the data importer will treat the disclosed personal data in accordance with the spirit of the APPI. With respect to the second item above, the PPC Guidelines have identified the APEC CBPR as a recognised international framework on the handling of Personal Information.

Additional Obligation under the 2020 Amendments

Under the 2020 amendment of the APPI, international data transfers are permitted with additional requirements. First, when handling operators transfer personal data to a foreign country based on the aforementioned consent mechanism, they will be required to provide a data subject with certain information as specified by the amended Ordinance issued by the PPC (the amended PPC Ordinance) (Article 28.2). According to the PPC Ordinance, information about the name of the foreign country, the personal information protection system in the foreign country, and the measures to be taken by a recipient party to protect personal information are required to be provided to the data subject.

Secondly, when handling operators transfer personal data relying on the recipient's equivalent

system of data protection, they will be required to take steps necessary to ensure that the overseas recipient continuously takes equivalent measures and to provide a data subject with certain information about the measures to be taken upon a request in accordance with the amended PPC Ordinance (Article 28.3). In this regard, according to the PPC Ordinance, one of the measures to ensure such matters is to periodically confirm the implementation status of the equivalent measures taken by the recipient and the presence or absence of a system in the foreign country that might affect the implementation of the equivalent measures. The other measure is to take necessary and appropriate measures if the implementation of the equivalent measures by the recipient party is interfered with in some way and to suspend the provision of personal data if it becomes difficult to ensure the continuous implementation of the equivalent measures.

The PPC Ordinance also states that the information to be provided to a data subject upon request is:

- the recipient party's equivalent system of data protection;
- an outline of the equivalent measures taken by the recipient;
- the frequency and method of confirmation of the status of the equivalent measures and of the system in the foreign country that might affect the implementation of the measures;
- the name of the foreign country;
- the presence or absence of a system in that foreign country that might affect the implementation of the equivalent measures;
- the presence or absence of any impediment to the implementation of the equivalent measures; and
- an outline of the measures to be taken in response to any such impediment.

As a result, data transfer to countries where improper government access is implemented can be difficult. An example of this difficulty is the international data transfer regulations under the GDPR raised by the Schrems II case.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

International data transfers are allowed under some requirements. Please see **4.1 Restrictions on International Data Issues**.

4.3 Government Notifications and Approvals

As discussed in **4.1 Restrictions on International Data Issues**, overseas data transfer restrictions do not require any government notification or approval.

4.4 Data Localisation Requirements

There are no data localisation requirements under the APPI.

4.5 Sharing Technical Details

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

4.6 Limitations and Considerations

See **3.3 Invoking Foreign Government Obligations**.

4.7 “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 has a concept of anonymously processed information, to which the regulations regarding personal information will not apply.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

The 2020 amendment of the APPI introduces a concept of pseudonymously processed information. Please see **2.1 Omnibus Laws and General Requirements** (Anonymisation, De-identification or Pseudonymisation) for further details on anonymously processed information and pseudonymously processed information.

As for big data analytics, the sharing of data will typically happen between companies subject to contracts between those companies. The Ministry of Economy, Trade and Industry (METI) has published guidelines on contracts regarding sharing (big) data between companies.

Automated Decision-Making, Profiling and Microtargeting

There are currently no specific laws or regulations regarding automated decision-making, profiling, and microtargeting; however, the improper use of relevant technology may in theory be deemed to be fomenting or prompting unlawful or unfair acts which are prohibited under Article 19 of the amended APPI. The amended guidelines stipulate that when analysing information on the behaviour and interests of an individual, handling operators must specify the purpose of use so that the data subject can predict or assume what kind of data processing is being performed, and the process of profiling may need to be explained accordingly.

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 the actions of an AI and ownership of rights regarding contents created by an AI; however, there are no laws or regulations that target AI 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 AI. These are tentative guidelines for further international discussion. The MIC also published Guidelines for AI Utilisation in August 2019. These summarise the issues that AI users (including AI service providers) are expected to pay attention to in the utilisation phase in the form of “principles” and provide explanations based on the principle of a human-centred AI society. Some other associations regarding AI have also published the same principles or guidelines for research into and the development of artificial intelligence.

Internet of Things (IoT) and Ubiquitous Sensors

Legal problems regarding the IoT and ubiquitous sensors have been the subject of intensive discussions of late, but there are no specific laws or regulations targeting the IoT or ubiquitous sensors at this time.

That said, the 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 intensive recent discussions in Japan. The Road Traffic Act was amended in April 2020, allowing autonomous vehicles to drive under some requirements.

Facial Recognition

Facial recognition data is considered personal information and is subject to the regulations

explained in **2.1 Omnibus Laws and General Requirements**. 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 **2.1 Omnibus Laws and General Requirements**.

Geolocation

The geolocation of persons is considered personal information and is subject to the regulations explained in **2.1 Omnibus Laws and General Requirements**. In practice, it is highly recommended to obtain the consent of data subjects before collecting accurate GPS data because of privacy concerns. If the geolocation information is obtained through the use of mobile communication provided by a telecommunications company, it will be protected under secrecy of communication.

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.

Disinformation, Deepfakes, and Other Online Harms

There are currently no laws or regulations regarding disinformation and deepfakes. However, online harm – such as through anonymous online defamation, privacy infringement, and insults – are viewed as serious problems. In order to address these, there is a legal procedure to mandate server operators and internet service providers to disclose the identity of relevant

personal information. However, this procedure is complicated, costly and lengthy, and thus, an amendment of a relevant law which eases the legal procedure was approved in April 2021 and will take effect by October 2022.

“Dark Pattern” or Online Manipulation

There are currently no specific laws or regulations regarding “dark patterns” or online manipulation. However, if a business obtains consent in a deceitful or unfair manner, the consent or the contract may be cancelled.

Fiduciary Duty for Privacy or Data Protection

Directors of companies owe a fiduciary duty to those companies. This fiduciary duty typically includes the duty to establish an internal risk management system for privacy or data protection. The Corporate Privacy Governance Guidebook for the DX Era, issued by the METI, can be useful for corporate privacy governance.

5.2 “Digital Governance” or Fair Data Practice Review Boards

The METI takes necessary measures to improve transparency and fairness in trading on digital platforms under the Act on Improvement of Transparency and Fairness in Trading on Specified Digital Platforms. The Japan Fair Trade Commission is authorised to exercise certain measures against unreasonable restraint of trade and unfair trade practices taking advantage of market power under the Anti-monopoly Act.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Please refer to **2.5 Enforcement and Litigation** for examples of significant privacy and data protection regulatory enforcement or litigation.

5.4 Due Diligence

In the context of due diligence in M&A, an analysis of the legal issues related to privacy and data

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto

protection that come with an acquired business is necessary given the potential for such issues to crystallise into a significant risk.

5.5 Public Disclosure

There are no non-cybersecurity-specific laws which legally mandate the disclosure of an organisation's cybersecurity risk profile or experience; however, in practice, it is common for publicly listed companies to disclose cybersecurity risks in the "risk of business" section of their annual securities reports. Both the Cybersecurity Management Guidelines issued by the METI and

the Information-Technology Promotion Agency, and the Point of View Regarding Cybersecurity for Enterprise Management issued by the NISC, mention the possibility of public disclosure. The MIC has published Manuals for Information Disclosure of Cybersecurity Measures (28 June 2019).

5.6 Other Significant Issues

There are no data protection or privacy issues of major importance not already covered in this chapter.

*Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura,
Mori Hamada & Matsumoto*

Mori Hamada & Matsumoto is a full-service law firm that has served clients with distinction since its establishment in December 2002. Mori Hamada & Matsumoto has experienced lawyers with considerable expertise in the constantly evolving and increasingly complex areas of information technology, life sciences and intellectual property, providing a variety of legal services in response to the diverse legal needs

of its clients. These legal services include advising on regulatory requirements, setting up business, corporate housekeeping, contract negotiations and dispute resolution. In terms of data protection, the firm has noted expertise in leveraging user information while protecting clients' businesses. Mori Hamada & Matsumoto's data protection team comprises approximately 40 lawyers.

AUTHORS



Yoshifumi Onodera is a partner at Mori Hamada & Matsumoto. Highly experienced in all kinds of data-related matters, he is particularly adept in the delivery of advice to both foreign and

domestic clients on complex business structures in vast industries, including internet-related services, social networking services, games, music, movies and telecommunications. The majority of his cases are subject to communication, media, competition, consumer and information laws. His expertise also extends to IP-related transactions, licensing, and the dispute resolution aspects of cases in the subsidiary fields of infringement litigation, invalidity trials, appellate litigation and arbitration, and licensing in relation to intellectual property, including patents, trade marks, and copyright.



Hiroyuki Tanaka is a partner at Mori Hamada & Matsumoto, admitted to practice in Japan and New York. Hiroyuki's practice areas are data protection, IT and IP. He has

extensive experience advising foreign clients on Japanese data protection law. He is also familiar with global data protection regulations, including the GDPR and CCPA, and helps Japanese clients with global data protection compliance by working closely with local counsel. He has extensive experience as legal counsel in various IP infringement disputes as well as disputes related to IT, including software, games, and apps. He has published widely in his areas of expertise.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka and Naoto Shimamura, Mori Hamada & Matsumoto



Naoto Shimamura is a senior associate at Mori Hamada & Matsumoto, licensed in Japan, California and New York. Taking advantage of his in-depth knowledge of computers and the internet, he engages in technology-related cases, including those involving e-commerce, licensing, privacy, data protection, cybersecurity, defamation on the internet, intellectual property, and dispute resolution in this area. He is also qualified as a Certified Information Privacy Professional/Europe (CIPP/E), a Certified Information Privacy Professional/United States (CIPP/US), and a Registered Information Security Specialist, which is recognised as the highest level of security engineering qualification in Japan. He has contributed to a variety of specialist publications on these and related topics.

Mori Hamada & Matsumoto

16th Floor, Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
Tokyo
Japan
100-8222

Tel: +81 3 6212 8330
Fax: +81 3 6212 8230
Email: mhm_info@mhm-global.com
Web: www.mhmjapan.com

MORI HAMADA & MATSUMOTO
