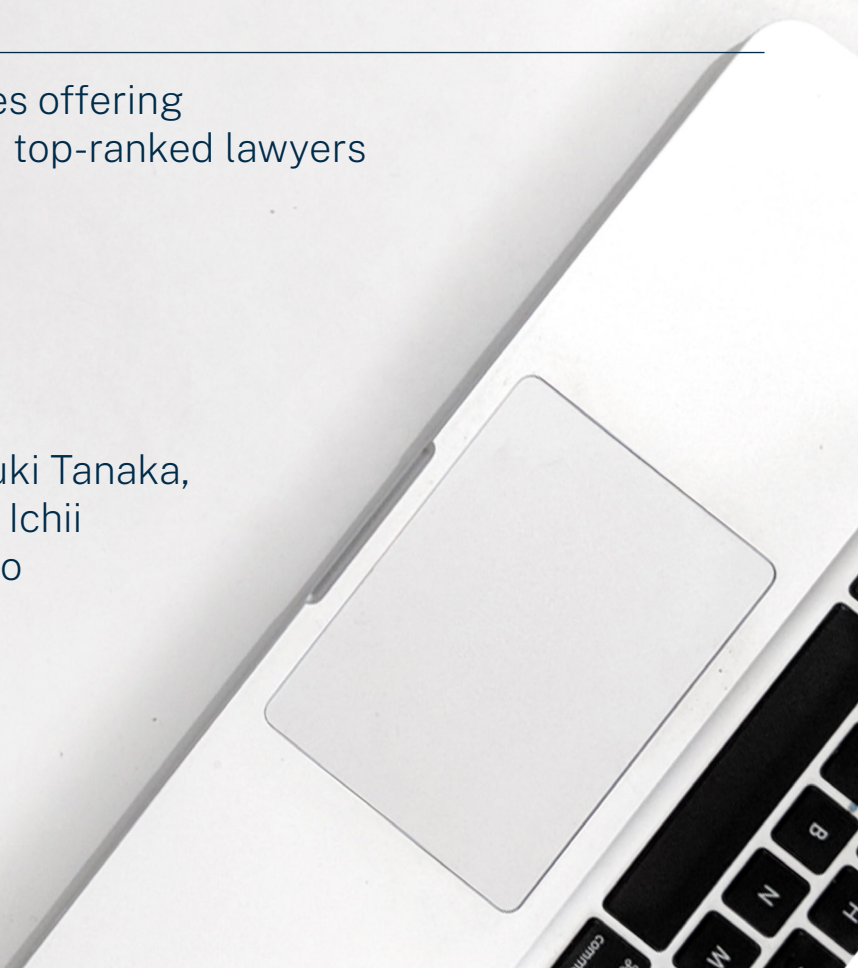

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

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

Japan: Law & Practice

Yoshifumi Onodera, Hiroyuki Tanaka,
Naoto Shimamura and Rio Ichii
Mori Hamada & Matsumoto



JAPAN



Law and Practice

Contributed by:

Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii
Mori Hamada & Matsumoto

Contents

1. Legal and Regulatory Framework p.5

- 1.1 Overview of Data and Privacy-Related Laws p.5
- 1.2 Regulators p.6
- 1.3 Enforcement Proceedings and Fines p.7
- 1.4 Data Protection Fines in Practice p.7
- 1.5 AI Regulation p.8
- 1.6 Interplay Between AI and Data Protection Regulations p.8

2. Privacy Litigation p.8

- 2.1 General Overview p.8
- 2.2 Recent Case Law p.8
- 2.3 Collective Redress Mechanisms p.9

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services p.9

- 3.1 Objectives and Scope of Data Regulation p.9
- 3.2 Interaction of Data Regulation and Data Protection p.13
- 3.3 Rights and Obligations Under Applicable Data Regulation p.13
- 3.4 Regulators and Enforcement p.13

4. Sectoral Issues p.13

- 4.1 Use of Cookies p.13
- 4.2 Personalised Advertising and Other Online Marketing Practices p.13
- 4.3 Employment Privacy Law p.14
- 4.4 Transfer of Personal Data in Asset Deals p.15

5. International Considerations p.15

- 5.1 Restrictions on International Data Transfers p.15
- 5.2 Government Notifications and Approvals p.16
- 5.3 Data Localisation Requirements p.16
- 5.4 Blocking Statutes p.16
- 5.5 Recent Developments p.16

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

Mori Hamada & Matsumoto is a full-service law firm that has served clients with distinction since its establishment in December 2002. The firm 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 130 lawyers.

Authors



Yoshifumi Onodera is a partner at Mori Hamada & Matsumoto. He is highly experienced in data-related matters involving communication, media, competition, consumer and/or

information laws, and particularly adept at advising both foreign and domestic clients on complex business structures spanning vast content and communication-related industries, including internet-related services, social networking services, games, music, movies and telecommunications. His expertise also extends to IP-related transactions, concerning licensing and dispute resolution aspects 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 (Daini Tokyo Bar Association) and New York. His practice areas are data protection, IT and

IP, and he has substantial experience in 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 counsels. He advises on AI (especially generative AI) and the protection of cybernetic avatars, and is an adjunct project professor at Keio University Graduate School of Law.

JAPAN LAW AND PRACTICE

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



Naoto Shimamura is a senior associate at Mori Hamada & Matsumoto, licensed in Japan (Daini Tokyo Bar Association), California and New York, and a lecturer at Ochanomizu

University and Japan Women's University. He uses his in-depth knowledge of computers and the internet to engage in technology-related cases, including those involving e-commerce, consumer protection, licensing, privacy, data protection, cybersecurity, defamation on the internet, intellectual property and dispute resolution. Naoto 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.



Rio Ichii is a junior associate at Mori Hamada & Matsumoto, licensed in Japan (Daiichi Tokyo Bar Association). She has a broad portfolio and a wealth of experience across a number of

practice areas, including IT, intellectual property, healthcare and trade law. She has written many articles on these 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: info@morihamada.com
Web: www.morihamada.com

MORI HAMADA

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

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Japan's principal data protection legislation is the Act on the Protection of Personal Information (APPI). It provides the basic principles for the government's regulatory policies and authority, as well as the obligations of private business operators that handle personal information (handling operators).

Before April 2022, national administrative bodies were 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, etc. However, after April 2022, the obligations prescribed in these two laws were integrated into the APPI.

Local government bodies are regulated under their own local regulations (*jourei*), but these vary between bodies. In April 2023, the APPI introduced nationwide principles for *jourei* 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, while *jourei* can only stipulate local rules in very limited situations allowed under the law.

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

In June 2023, the Telecommunications Business Act (TBA) introduced a regulation about sending cookies to external parties. It also imposed new obligations regarding user information on large telecommunications service providers (TSPs) that have either 5 million paid users or 10 million free users.

There are no laws or regulations that target artificial intelligence (AI) at this time.

Furthermore, the Personal Information Protection Commission (PPC – the regulator primarily responsible for the APPI and the My Number Act) has published guidelines for handling personal information (PPC Guidelines). The ministries with jurisdiction over some industrial sectors have 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 telecommunications business operators.

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; this decision was renewed in March and April 2023. However, this does not mean that the APPI is identical to Regulation (EU) 2016/679 (General Data Protection Regulation – 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.

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

According to a supplementary provision of the APPI, a review of whether to amend the law is conducted every three years. Based on this provision, on 27 June 2024 the PPC published an “Interim Summary”, outlining its current thinking based on discussions and examinations to date. On 4 September 2024, the commission then published the results of a public consultation, covering the following main topics:

- new regulations on biometric data;
- specifying and categorising the regulations on improper use and unauthorised acquisition;
- aggravating obligations on the opt-out scheme for the provision of personal data to third parties;
- regulations regarding children’s personal information;
- strengthening APPI enforcement (including implementation of an administrative fine system and establishing a new system of injunctive relief and restoration of damages);
- streamlining the scope and details of data breach reports and data subject notifications;
- exempting certain data processing from data subject consent that is currently required by law; and
- privacy impact assessments (PIAs) and those in charge of handling personal data.

However, it remains unclear whether legislation based on the Interim Summary will be submitted to the next regular Diet session (January–June 2025). If the amended law is enacted, its implementation is expected to begin in either 2026 or 2027.

On 31 July 2024, an expert panel was established to discuss issues regarding strengthening APPI enforcement, with the report being published on 25 December 2024. In addition, on 21 October 2024, the PPC published its “Per-

spectives for Enhancing the Triennial Review of the Personal Information Protection Act”. These perspectives could possibly be interpreted as suggesting a shift towards GDPR-style legislation to some extent, but such fundamental institutional changes may not be realistic in the short term, particularly as passage at the next regular Diet session would face significant hurdles. The PPC has conducted hearings with various stakeholders regarding these perspectives, with the results being published on 17 December 2024.

1.2 Regulators

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

- to require handling operators to report or submit materials regarding their handling of personal information, and to enter handling operators’ offices or other locations to investigate, make enquiries and check records or other documents (Article 146);
- to provide guidance or advice to handling operators (Article 147);
- to recommend that handling operators cease any violations of the APPI and take other necessary measures to correct the violations (Article 148.1);
- to order handling operators to take necessary measures to implement the PPC’s recommendations mentioned above and rectify certain violations of the APPI (Articles 148.2 and 148.3); and
- to publicly announce any handling operators’ violations of orders issued by the PPC pursuant to Articles 148.2 and 148.3 (Article 148.4).

For some sectors, other government authorities also enforce the APPI – for example, the FSA is the relevant authority for banks, whereas MIC is the appropriate authority for TSPs. There are no regulators specifically overseeing AI data.

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

The PPC does not have the authority to conduct criminal investigations, and the APPI explicitly stipulates that the commission's power to conduct on-site inspections does not include criminal investigations (Article 146.3).

It is important to note that the APPI imposes no administrative fines. Criminal sanctions may only be imposed if a handling operator:

- refuses to co-operate with or makes any false report in response to an investigation by the PPC (Article 178);
- provides a personal information database to unauthorised persons or misuses the database for unlawful gains (Article 180); or
- violates any order given by the PPC as part of an administrative sanction (Article 181).

The PPC empowers private organisations called accredited personal information protection organisations (*nintei kojiri jouchou hogo dantai*) to handle and promote the protection of the personal information held by handling operators. These accredited organisations process complaints against handling operators or provide information on them to ensure the reliability of the businesses of those handling operators, and promote the protection of personal information. They also establish their own rules, with which their members must comply.

1.3 Enforcement Proceedings and Fines

The PPC finds potential violations of the APPI through:

- data breach reports submitted by handling operators;
- telephone consultations made through their business support desk; and
- media coverage.

It has the power to enforce administrative sanctions, but the APPI does not provide for administrative fines; please see **1.2 Regulators** for details. The introduction of administrative fines is under discussion.

The PPC provides guidance or advice, and does not take further action in most cases, although the commission takes strong action such as issuing orders in serious cases.

Please see **1.4 Data Protection Fines in Practice** for recent statistics about administrative sanctions enforced by the PPC.

1.4 Data Protection Fines in Practice

The APPI does not provide for administrative fines, but enforcement statistics are as follows.

- Between 1 October 2023 and 31 March 2024, no administrative orders were issued, three administrative recommendations were made, 168 issuances of administrative guidance or advice were made, no on-site inspections were conducted, and 13 administrative requests for reports and materials were made against handling operators under the APPI.
- Between 1 April 2023 and 30 September 2024, no administrative orders were issued, no administrative recommendations were made, 1,203 issuances of administrative guidance or advice were made, three on-site inspections were conducted, and 61 administrative requests for reports and materials were made against handling operators under the APPI.

No administrative orders have been issued because ordinary companies have been in compliance with the PPC's administrative guidance and advice. Moreover, companies are typically

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

concerned with their social reputation, so they endeavour to comply with laws and regulations.

1.5 AI Regulation

Legal problems concerning AI have been the subject of intense discussion of late, including matters such as liability for the actions of AI and ownership of rights regarding AI-created content; however, no laws or regulations target the emerging technology itself at this time. The government plans to submit a new bill to the Diet in 2025 that will promote the use of AI and address cases of malicious use.

The PPC published an announcement on 2 June 2023, stating its interpretation of the APPI in the context of generative AI and requesting generative AI service providers and users to comply with the law. MIC and the Ministry of Economy, Trade and Industry (METI) published their AI Business Guidelines for AI developers, service providers and users on 19 April 2024. These guidelines include cautions and points to note regarding privacy and data protection.

The Institute for Information and Communications Policy (IICP) and MIC have jointly published the Draft AI R&D Guidelines for International Discussions, which explain the R&D and nine other principles for research into and development of AI. These are tentative guidelines for further international discussion. MIC also published the Guidelines for AI Utilisation in August 2019, which summarise the issues that users (including service providers) are expected to pay attention to in their utilisation phase of AI in the form of “principles”, and provide explanations based on the principle of a human-centred AI society. Some other AI-related associations have also published the same principles or guidelines for research into and development of artificial intelligence.

1.6 Interplay Between AI and Data Protection Regulations

There are no regulations specific to AI data, but please note that general regulations are applicable. For example, if AI data includes personal information, the APPI applies to the processing of that data. Please also refer to 1.5 AI Regulation for more details.

2. Privacy Litigation

2.1 General Overview

Data subjects may go to court to seek compensation for damages or distress caused by breaches of data protection. There are two major types of legal causes.

- First, Japanese courts recognise the right to privacy, which is the right of persons not to have their private lives disclosed except for legitimate reasons. Breaching the right to privacy constitutes tort under Article 709 of the Civil Code.
- Second, 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.

2.2 Recent Case Law

In a decision issued in October 2017, the Supreme Court found that breaching the right to privacy may give rise to claims for compensation for distress caused by the leakage of personal information (eg, names, birthdates, addresses, telephone numbers). The case was appealed to the Osaka high Court, which awarded JPY1,000 to the claimant on 20 November 2019. In addition, the Tokyo high Court awarded JPY3,300 to other plaintiffs on 25 March 2020 for the same data breach. The Supreme Court denied appeals

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

of these cases in December 2020, so these appellate court decisions are deemed final.

2.3 Collective Redress Mechanisms

The Act on Special Measures Concerning Civil Court Proceedings for the Collective Redress for Property Damage Incurred by Consumers allows for class actions to be filed by consumers. Please note that claims allowed under the law are limited to property damage and emotional distress within the scope of the class action itself if the distress is caused along with property damage or by intentional conduct.

As a practical matter, multiple data subjects may select the same lawyer to represent them, and that lawyer can file a single lawsuit on their behalf, which is similar to a class action.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation IoT Services

Legal problems regarding the IoT and ubiquitous sensors have been the subject of intense discussion of late, but no specific laws or regulations are currently targeting either issue. However, MIC has published guidelines regarding comprehensive measures for IoT securities (July 2016).

The Information-technology Promotion Agency will introduce the security requirement compliance evaluation and labelling system for security features of IoT products in March 2025.

Big Data

As for big data analytics, data sharing will typically happen between companies subject to

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

Please also refer to **1.5 AI Regulation**.

Handling Operator Duties

The various obligations of handling operators under the APPI are as follows.

- They must specify and make known to data subjects the purpose of collecting their personal information (Articles 17 and 21).
- When a handling operator changes the purpose of use beyond what can be reasonably recognised as having relevance to the original purpose of use, the data subjects' consent is required (Articles 17.2 and 18.1). Exceptions to this consent requirement include instances when the use of information 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). Handling operators must not utilise personal information in a way that possibly foments or prompts unlawful or unfair acts (Article 19).
- When a handling operator obtains personal information of a person directly from documents (including electronic records) provided by that person, it must explicitly inform that person of the purpose of use in advance (Article 21.2).
- They must establish appropriate safeguards to protect personal data (Article 23).
- They must report data breach incidents to the PPC and notify affected data subjects in cases where their rights or interests are likely to be infringed (Article 26).
- They may not transfer personal data to another entity without the opt-in consent of the data subjects, unless they meet the require-

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

ments of any of the exceptions provided by the APPI (Article 27.1). These exceptions include instances where a transfer 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, or is necessary for academic or research purposes (Article 27.1(i)–(vii)). Other major exceptions include cases of entrustment of the handling of personal data to another entity, joint use of 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).

- They may not transfer personal data to countries that do not have sufficient data protection safeguards without the data subjects' consent (Article 28).
- They must keep records of the provision of personal data to third parties (Article 29).
- Upon receiving personal data from other handling operators, they must confirm the providing handling operator's compliance with applicable regulations regarding the provision of personal data and keep a record of the confirmation process (Article 30).
- They must handle pseudonymously and anonymously processed information in certain ways (Articles 41 to 46).

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 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 appropriate supervision as necessary over the entrusted person to ensure security control over the entrusted personal data (Article 25).

Joint Use

Handling operators may share and jointly use personal data with specific individuals or entities as long as the handling operator notifies the data subjects or makes the following information accessible to them (Article 27.5(iii)) before any information sharing or joint use:

- 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 managing 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 this information is published or the data subjects are notified of it, 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

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

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

Filing of Notification of Opt-Out Consent

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

- they agree to stop providing personal data to the third party upon the data subject's demand;
- they notify the data subjects in advance of certain events outlined in Article 27.2 or make such notification of events readily accessible to the data subjects; and
- they submit 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 privacy or data protection officers; however, handling operators must 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 who is responsible for supervising such handling;
- HR security measures, including educating/training employees;

- 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 was introduced in the amendments to the guidelines and requires handling operators that process personal data in foreign countries to understand the foreign country's legal system for personal information protection and, taking that legal system into consideration, to take necessary and appropriate measures to ensure the security of personal data.

Effective since 1 April 2024, the PPC Guidelines also require handling operators to take security control over personal information that will be collected and expected to be treated as personal data so that cyber-attackers cannot intercept such information on behalf of the operator.

The PPC Guidelines indicate the appointment of a person to be in charge of the handling of personal data as an example of a proper and necessary measure. However, although handling operators are expected to adopt the measures described in the PPC Guidelines, any failure to adopt such measures is not a direct breach of the APPI.

Under the TBA, large TSPs are required to appoint a chief manager responsible for handling user information.

Privacy By Design/Default and Privacy Impact Analyses

The APPI does not mandate obligations regarding PIAs. However, the PPC has issued a report titled "Promoting the implementation of PIAs – Significance of PIAs and points to keep in mind

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

in the implementation process”, which business operators are encouraged to follow 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 individual or entity responsible and, if it is a corporate body, the name of its representative;
- the purposes of use of retained personal data;
- the procedures for responding to requests from data subjects to disclose, correct, suspend the use of or erase 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 by using internal and external privacy policies.

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

- the name of the handling operator;

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

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

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

Data Subjects’ Rights

Data subjects may request handling operators to disclose their retained personal data and the record of its provision to third parties. Handling operators must comply with these requests 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 or interests, or that it could seriously interfere with the handling operator’s business (Article 33).

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

Furthermore, data subjects may request that handling operators discontinue the use of or erase retained personal data and stop providing retained personal data to third parties if:

- the data was or is being acquired, processed or provided to a third party in violation of the APPI;

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

- 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 subjects.

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 subjects (Article 35).

3.2 Interaction of Data Regulation and Data Protection

See 3.1 Objectives and Scope of Data Regulation.

3.3 Rights and Obligations Under Applicable Data Regulation

See 3.1 Objectives and Scope of Data Regulation.

3.4 Regulators and Enforcement

See 1.2 Regulators.

4. Sectoral Issues

4.1 Use of Cookies

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 automatically deemed to be personal information, but it will be 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 can identify the cookie IDs of customers when logged in to its website).

In this regard, the transfer of personal data to third parties – whether the data is personal data or not – is determined 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 the past, some schemes emerged whereby data management platforms provided non-personal information such as user data collected by cookies (eg, user browsing histories, interests, 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 of (or control by) the data subjects. As a result, the concept of personally referable information was introduced in April 2022, defined as a collective set of information comprising information relating to living individuals that does not fall under personal information or pseudonymously or anonymously processed information but that has been systematically organised to be searchable using a computer for specific personally referable information or similar information prescribed by Cabinet Order.

The 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 such cases, the transferor must confirm that the transferee has obtained the data subjects' consent to transfer their data as personal data.

4.2 Personalised Advertising and Other Online Marketing Practices

Behavioural advertising is not directly regulated under the APPI, but any personal information

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

collected to provide such advertising is subject to the law. For example, the APPI has regulations for certain cookies, web beacons and other tracking technology underlying behavioural or targeted advertising (please see **4.1 Use of Cookies**). It is good practice to have a cookie policy and to offer an opt-out from using cookies (especially for behavioural advertising). The Japan Interactive Advertising Association's guidelines are useful for gaining an understanding of good practices in Japan.

Effective since June 2023, the TBA imposed new obligations on TSPs, which have a non-trivial impact on users' interests. More specifically, a TSP is an entity that provides:

- any services of intermediating telecommunication of others, such as email or direct messaging services;
- social media services, bulletin board systems, movie sharing services, online shopping malls, live streaming services, online games, online education or the like;
- online search engines; or
- various information, such as news, weather, movies and maps, to unspecified people.

When a TSP makes users send their information (typically including cookies) to an external party, the TSP is required to make a notification or public announcement, obtain opt-in consent or provide an opt-out mechanism with respect to certain information, including the content of the information, the name of the recipient party and the recipient's purpose of use of the information.

Unsolicited marketing by email is regulated principally by the Act on the Regulation of Transmission of Specified Electronic Mail (Anti-Spam Act), under which marketing emails can only be sent to recipients who:

- have given prior consent to receive them;
- have provided the sender with their email addresses in writing (for instance, by providing a business card);
- have a business relationship with the sender; or
- make their email addresses available on the internet for business purposes.

The Anti-Spam Act also requires the sender to allow the recipients to opt out.

Furthermore, the Act on Specified Commercial Transactions restricts marketing regarding mail order businesses, including online shopping, but does not provide exceptions similar to the last three items above.

There are special restrictions on telecommunications business operators regarding location information under MIC's guidelines on personal information for telecommunications businesses. Under these guidelines, telecommunications business operators can obtain or transfer location information from mobile devices only with the data subjects' prior consent or if there is a justifiable cause.

4.3 Employment Privacy Law

The Ministry of Health, Labour and Welfare has issued a notice regarding the handling of health information of employees by employers, including a condition that the employer shall not handle such information beyond the scope necessary to secure their employees' health.

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

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

The employer has the right to monitor workplace communications in relation to work and to use cybersecurity tools, insider threat detection and prevention programmes, and digital loss prevention technologies, but privacy issues may arise regarding private communications and other privacy matters at the workplace. Thus, employers are recommended to establish internal rules prohibiting the use of company PCs and email addresses for private use, and to disclose the possibility of monitoring those devices and data, including emails.

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.

4.4 Transfer of Personal Data in Asset Deals

See 3.1 Objectives and Scope of Data Regulation for the regulations on transferring personal data to other entities.

5. International Considerations

5.1 Restrictions on International Data Transfers

Basic Regulation

There are special restrictions on the transfer of personal data to foreign countries. In principle, the APPI requires the transferor to obtain the prior consent of individuals whose personal data will be transferred to third parties located in foreign countries (Article 28). Thus, overseas transfer restrictions will apply if a foreign company transfers user data to another company outside Japan. However, if it does so to a company in Japan, overseas transfer restrictions will not

apply. These restrictions apply even in cases of entrustment and joint use, which are exceptions to local third-party data transfer restrictions.

Data subjects' consent to overseas data transfers is not necessary only if either of the following applies:

- the PPC designates the foreign country as a country with a data protection regime with a level of protection equivalent to that of Japan (only member countries of the EEA and the UK have been designated to date); or
- the third-party recipient has an equivalent system of data protection that meets the standards prescribed by the PPC Ordinance – i.e. 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.

Implementation of the PPC Ordinance is provided for in the PPC Guidelines, under which the “appropriate and reasonable methodologies” referred to above include agreements between the data importer and exporter, or intergroup 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 recognised international arrangements, the PPC Guidelines have identified the APEC Cross Border Privacy Rules (CBPR) as a recognised international framework for the handling of personal information.

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

Please also refer to **5.5 Recent Developments** for additional obligations effective since April 2022.

5.2 Government Notifications and Approvals

Overseas data transfer restrictions do not require government notification or approval.

5.3 Data Localisation Requirements

There are no data localisation requirements under the APPI.

5.4 Blocking Statutes

There are no blocking statutes under Japanese law.

5.5 Recent Developments

Additional Obligations Since April 2022

Effective since April 2022, international data transfers are permitted only when additional requirements are met. First, when handling operators transfer personal data to foreign countries based on the consent mechanism, they will be required to provide data subjects with certain information, as specified by the amended Ordinance issued by the PPC (Article 28.2). According to the PPC Ordinance, the foreign country's name, information about its personal information protection system and the measures to be taken by the recipient party to protect personal information are required to be provided to the data subjects.

Second, when handling operators transfer personal data relying on the recipient's equivalent system of data protection, they will be required to take the necessary steps to ensure that the overseas recipient continuously takes equivalent measures and to provide data subjects with certain information about the measures to be taken upon request under the amended PPC Ordinance

(Article 28.3). In this regard, according to the PPC Ordinance, one of two assurance measures is to periodically confirm the implementation status of the equivalent measures taken by the recipient and the presence or absence of systems 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 recipient party's implementation of the equivalent measures 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 following information must be provided to data subjects upon request:

- 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 systems in that foreign country that might affect the implementation of the equivalent measures;
- the presence or absence of any impediments to the implementation of the equivalent measures; and
- an outline of the measures to be taken in response to such impediments.

As a result, data transfers to countries where proper government access is not implemented can be difficult. An example of this difficulty is the international data transfer regulations under the GDPR raised by the Schrems II case.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com