GDR

INSIGHT HANDBOOK
2024

The GDR *Insight Handbook 2024* delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

Japan: Updated Data Protection Regime Provides Clarity for Private Sector

Akira Matsuda, Tomonori Fujinami and Riko Suzuki

Iwata Godo

Key statutes, regulations and adopted international standards

In Japan, data protection regulation of the private sector and public sector differ significantly. This chapter mainly focuses on the private sector.

Rules for business operators in the private sector

APPI

The Act on the Protection of Personal Information (APPI) (Act No. 57 of 2003) is the principal legislation in Japan dealing with data protection. It came into force in 2005 and was drastically overhauled in 2017 and 2020 to take into account rapid technological developments (artificial intelligence, big data, etc) and globalisation, which have brought about new challenges and the increasing need to protect personal data.

The APPI imposes obligations on 'business operators'. After an exemption applicable to small and medium-sized enterprises was abolished as part of the 2017 amendments, almost all Japan-based business operators are covered by the APPI, regardless of the amount of personal data they handle or the size of their business (see 'The effect of local laws on foreign businesses' below).

To clarify and ensure the enforcement of these obligations, the APPI:

- sets forth a basic regulatory framework (see 'Regulatory bodies' and 'The effect of local laws on foreign businesses');
- established the Personal Information Protection Commission (PPC) and defined its roles as the national data protection authority (see 'Regulatory bodies'); and
- provides for a set of enforcement measures, such as imprisonment and fines (see 'Overview of the main enforcement measures in the APPI').

Guidelines

The PPC has adopted guidelines to ensure the proper and effective implementation of the APPI by business operators. The PPC's general guidelines supplement the APPI. Specific guidelines apply to certain sectors such as the finance, medical and telecommunications sectors.

Regulation of local public bodies

In the past, all prefectures and municipal governments in Japan had local regulations on the protection of personal information, which covered the prefectures and municipal governments, public schools and public hospitals; however, after the amendment of the APPI, which came into force on 1 April 2023, local regulations on the protection of personal information have now been made uniform under the APPI.

Regulatory bodies

The PPC is the sole national data protection authority in Japan. It is independent from other government bodies. The main roles of the PPC are as follows:

- It formulates basic policies on the protection of personal information in accordance with the APPI and promotes the protection of personal information in the public and private sectors. These basic policies include guidelines[1] that are updated from time to time.
- It has the power to issue guidance and advice, request reports, conduct on-site inspections, make recommendations and issue orders to government institutions and business operators. The range of enforcement measures available is prescribed under the APPI.
- It promotes cooperation with data protection authorities in foreign countries through formal and informal exchanges of views.
- For the purpose of ensuring the proper handling of personal information, the PPC accredits private organisations (ie, accredited personal information protection organisations) that provide certain data protection-related

1 Guidelines for the Act on the Protection of Personal Information (General Rules); Guidelines for the Act on the Protection of Personal Information (Obligations of Confirmation and Recording at the Time of Provision of Personal Data to Third Parties); Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country); Guidelines for the Act on the Protection of Personal Information (Pseudonymously Processed Information and Anonymously Processed Information); Guidelines for the Act on the Protection of Personal Information (Accredited Personal Information Protection Organisations); Guidelines on Personal Information Protection in the Credit Industry; Guidelines on Personal Information Protection in the Claim Management and Collection Business Industry; and Guidelines on Personal Information Protection in the Financial Industry, etc.

services, such as receiving complaints about the handling of personal information, the provision of advice to those making a complaint and the investigation of the circumstances surrounding a complaint. In addition, it supervises these accredited organisations, requiring them to report on the conduct of their services, and may order them to improve their services or take any other necessary action.

The effect of local laws on foreign businesses

Foreign groups with an office located in Japan

The APPI imposes obligations on business operators handling personal information (ie, business operators). A business operator is defined as 'an entity using a personal information database for use in its business'. There is no carve-out for the benefit of companies incorporated in a foreign country or entities having their head office located in a foreign country (ie, a foreign company). This definition reflects the official position of the PPC that the APPI obligations and provisions apply equally to foreign companies if those foreign companies fall under the definition of a business operator in Japan.

The PPC takes the view that a foreign company is a business operator if it uses a personal information database for its business conducted in Japan, regardless of the place of incorporation or location of the head office; therefore, if a foreign company has a branch office or a business office in Japan, or if a foreign company conducts its business in Japan, and uses a personal information database for its business in Japan, it will fall under the definition of 'business operator'.

Furthermore, if a foreign company has a subsidiary in Japan using a personal information database for its business in Japan, that subsidiary will fall within the definition of a 'business operator'. Accordingly, if a foreign company has an office in Japan, which falls under the definition of 'business operator', then regardless of whether the office is branch, business office or subsidiary, APPI-complaint compliance systems must be put in place.

Foreign groups without an office in Japan

Even if a foreign company has no office in Japan, if it is collecting personal information from individuals in Japan in connection with a supply of goods or services to these individuals, obligations under the APPI would apply to it on an extra territorial basis. Accordingly, these entities must take measures to comply with these provisions of the APPI.

Core principles on personal data

The APPI distinguishes between:

- personal information: information by which a specific living individual is identifiable or information containing an individual identification code (ie, a passport number or driver's licence number). Personal information includes information that can be readily combined with other information and make the identification of a specific individual possible; and
- personal data: in summary, the part of personal information constituting a collective body of personal information systematically organised to be able to easily search for particular personal information.

The APPI applies additional protection to certain sensitive personal information as categorised and defined under the APPI. This includes but is not limited to the individual's race, creed, social status, medical history, criminal record, and status as the victim of a crime.

Overview of the main obligations under the APPI

The following table provides a brief outline of the obligations imposed on business operators for each phase during which personal information is handled.

Phase		Type of information	Summary of duties
I	Collection	Personal information	Disclosure of the purpose of use prior to collection of personal information
			No need to obtain the individual's consent (except for sensitive personal information)
II	Utilisation	Personal information and personal data	No need to obtain the individual's consent when utilising within the scope of a previously disclosed purpose
			Duty to take reasonable security measures including preventing the leakage, loss of, or damage to, personal data when handling personal data
III	Third-party disclosure	Personal data	**Consent requirement**
			In principle, individual consent is required for disclosure of personal data to a third party
			No need to obtain the individual's consent in the cases of entrustment of the handling of personal data, disclosure upon business succession (eg, M&A) and joint use
			Regarding joint use, if a business operator informs the individual in advance or ensures that the individual can easily become aware of five statutory elements, the business operator can jointly utilise personal data with a third party, such as a subsidiary, without obtaining any prior individual consent to the disclosure

Phase	Type of information	Summary of duties
		If the business operator meets certain requirements, there is no need to obtain the individual's consent upon each disclosure of personal data
		Traceability requirement
		An entity disclosing personal data to a third party must keep track (ie, records) of disclosure
		Cross-border transfer restrictions
		In principle, individual consent is required for disclosure to a third party in a foreign country
		No need to obtain the individual's consent in the circumstances explained in 'Cross-border transfer restrictions' below

Cross-border transfer restrictions

Unless certain exemptions apply, a business operator disclosing personal data to a third party in a foreign country must obtain the individual's prior consent; however, consent is not required in the following cases:

- transfer to a country that is designated by the PPC as having established a personal information protection system equivalent to Japan with regard to the protection of an individual's rights and interests (as at July 2023, only the EU and the UK are designated as such);
- the disclosing business operator and the recipient ensure that the recipient develops and implements arrangements through appropriate and reasonable measures for the handling of personal data to be performed in a manner consistent with the APPI's obligations. These measures may include:
    - contracts between the disclosing business operator and the recipient; or
    - internal rules that are commonly applied to the disclosing business operator and the recipient; and
- the recipient receives certification based on the APEC cross-border privacy rules framework (CBPR).

Furthermore, a business operator disclosing personal data to a third party in a foreign country must follow restrictions as follows:

- the disclosing business operator must provide data subjects with certain information, including information on the data protection regime of the foreign country of destination, when seeking their consent; and

- the disclosing business operator must take necessary steps to ensure that recipients of personal data continuously implement appropriate processing and security measures, and must provide data subjects on request with relevant information on such necessary steps.

Overview of the main enforcement measures in the APPI

The main enforcement measures are:

- imprisonment or criminal fine;
- an order to cease, desist and take other necessary action to rectify a violation of the APPI against the business operator; or
- any other action deemed necessary by the PPC within its authority.

Data breach

A business operator must report certain leakage or loss of, or damage to, personal data (a data breach) to the PPC and affected data subjects.

Reporting to the PPC and affected data subjects is mandatory in the following cases:

- the personal data includes or is likely to include sensitive personal information;
- financial damage is likely to arise in light of the nature of the personal data (eg, credit card number);
- persons with malicious intentions are likely to be involved in the data breach; or
- it has a significant scale (ie, 1,000 or more individuals).

A business operator is required to provide preliminary reports to the PPC within approximately three to five days of becoming aware of the events mentioned above. A business operator is also required to report to the PPC within 30 days (or 60 days if 'malicious persons' are likely to be involved in the data breach) of the final report.

Automated processing, profiling and data analytics

There is currently no Japanese legislation specifically restricting automated processing, profiling and data analytics. Under the current interpretation of the APPI, even if information that is equivalent to sensitive personal information is generated or presumed as a result of profiling, this information does not qualify as sensitive personal information under the APPI.

Under the APPI, a business operator handling anonymously processed information is not allowed to collate this information with other information to identify an individual to whom the anonymously processed information relates; however, if a business operator identifies a certain individual as a result of profiling using anonymously processed information, the business operator is not considered to be subject to that restriction.

As part of the last review of the APPI, there were discussions on whether rules specifically restricting automated processing, profiling and data analytics should be added to the APPI. As an alternative to addressing these issues in the APPI, data subjects' rights to obtain the deletion of their data or suspension of its use or transfer were strengthened. In particular, under the 2020 amendment of the APPI, data subjects are now able to make these requests if their rights or legitimate interests are likely to be infringed.

Further, APPI guidelines clarify that if the processing of personal data exceeds what the data subject would have expected, such as in the case of profiling, the purpose of use must be disclosed in detail at the time of acquisition or prior to processing of such personal information.

Communications and marketing

Telecommunications

Telecommunications businesses in Japan generally handle large amounts of personal information. Accordingly, the Ministry of Internal Affairs and Communications (MIC), acting as supervisory authority for the telecommunications sector, has issued the following guidelines.

Guidelines regarding the protection of personal information for the telecommunications sector

These guidelines contain rules that telecommunication business operators should comply with when they collect, use and transfer information such as communications history or information on callers (eg, caller ID and location information for phone calls).

Guidelines regarding personal information of the caller in caller information notification service

Certain telecommunication business operators provide a service of notifying the caller's information to the receiver of the call (the caller information notification service). Because caller information is treated as personal information, the MIC has adopted the 'Guidelines regarding personal information of the caller in the context of caller information notification services'.

These guidelines contain rules that caller information notification service providers should comply with when they record, use and transfer caller information.

Other

The MIC has established a working group regarding the handling of information stored in smartphones, such as location information and communications history (smartphone user information). The working group has published a Smartphone Privacy Initiative paper that reports their conclusions on how smartphone user information should be protected.

The MIC has also established a committee for the review of the handling of location information in emergencies. The committee has reviewed how location information should be utilised for accident prevention and issued a non-binding report on how such information should be protected.

Marketing

The APPI does not restrict the scope of the purposes for which personal information may be used (eg, for marketing purposes) as long as the purpose of use has been disclosed to the public (ie, via a privacy policy) or notified to individuals. E-marketing is also regulated by the Act on Specified Commercial Transactions (Act No. 57 of 1976) and the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002).

The Act on Specified Commercial Transactions

Under this Act, sellers or service providers can only advertise to consumers via email when recipients opt in to receive emails; however, the following are exceptions:

- sellers or service providers sending email advertisements with notice of matters regarding contracts (eg, finalisation of an agreement and shipment of goods); or

- sellers or service providers including email advertisements with email newsletters that are sent with consent from a recipient.

The Act on Regulation of Transmission of Specified Electronic Mail

Under this Act, senders can only advertise via email when recipients opt in to receive such emails; however, the following are exceptions:

- when recipients provide their email addresses to the sender in writing (for instance, by providing a business card);
- when recipients have a business relationship with the sender; and
- when recipients make their email addresses available on the internet for business purposes.

Individuals' rights

Right to request disclosure

A data subject may request disclosure of retained personal data[2] to a business operator that holds that data. A business operator must disclose the retained personal data without delay by the means that the person requests.[3]

The business operator is exempt from disclosing the retained personal data, in whole or in part, if:

- there is a possibility of harming a data subject or a third party's life, body, assets or other rights and interests;
- there is a risk of seriously interfering with the business operator's proper running of its business; or
- the disclosure violates other laws and regulations.

2 Retained personal data is defined as personal data held by a business operator. Following amendment of the Act on the Protection of Personal Information (APPI), the personal data now falls under the category of retained personal data definition regardless of the length of period it is held by a business operator. As there is practical overlap with the Act on Specified Commercial Transactions, both regulations apply.

3 Following amendment of the APPI, a data subjecting making request may choose the methods of disclosure in the request, including provision through electronic means, such as emails.

Right to request correction, addition or deletion

A data subject may request a business operator make a correction, addition or deletion (collectively, correction) in relation to the content of retained personal data if the personal data is incorrect. The business operator must conduct a necessary investigation without delay to the extent necessary to achieve a purpose of use (ie, for what type of business and for what purpose retained personal data will be used) and, based on the result thereof, make a correction of the content of the retained personal data when having received the request pursuant to the APPI.

The business operator is exempt from that correction obligation under the APPI if a special procedure concerning a correction of the content is prescribed by other laws or regulations.

Right to request suspension of use, deletion or suspension of third-party transfers

A data subject may request a business operator to suspend use, delete or suspend third-party transfers of retained personal data (collectively, 'suspension and deletion measures') if that data is handled in violation of the APPI, has been acquired in violation of the APPI or has been disclosed to a third party in violation of the APPI. Subject to certain exemptions (see below), a business operator must take suspension and deletion measures to the extent necessary to remedy the violation without delay, following receipt of a request made pursuant to the APPI and when it has become clear that there is a reason for the request.

The business operator is not obliged to take suspension and deletion measures if taking those measures would require a large expense or otherwise be difficult to carry out, provided (in each case) that necessary alternative action is taken to protect the rights and interests of the data subject.

In addition, recent amendments to the APPI have relaxed the requirements for data subjects requesting suspension and deletion measures when there is a risk of a violation of an individual's rights or legitimate interests.

The role of the data protection officer

The APPI has no provision mandating the appointment of a data protection officer; however, a business operator is required to take necessary and appropriate action to secure personal data including preventing the leakage, loss or damage of its handled personal data.

In connection with this provision, the PPC guidelines require a business operator to take security control measures, including the following:

- Organisational security control measures: appointing a person responsible for handling personal data, establishing a system to respond to leakage, loss or damage of personal data, and conducting safety audits on systems that manage personal data.
- Human security control measures: employee training on the handling of personal data.
- Physical security control measures: access control to areas where important personal data is handled, and storage of documents containing personal data in a cabinet that can be locked.
- Technical security control measures: for example, installing a firewall on computers connected externally through networks, and putting restrictions on access to systems that handle personal data.

Since the appointment of a person responsible for handling personal data is listed as one example of organisational security control measures in the PPC guidelines, it is the prevailing practice in Japan for a business operator to appoint a responsible person whose tasks or roles are similar to that of a data protection officer in many other jurisdictions.

Dealing with data protection breaches and the consequences

The PPC has the power to require a business operator to submit necessary information or materials relating to the handling of personal information or have its officials enter a business office or other necessary premises of a business operator, enquire about the handling of personal information, or inspect books, documents and other properties.[4]

Regarding corrective measures, the PPC has the power to:

- issue guidance or advice to a business operator with regard to handling personal information;[5]
- recommend that a business operator suspend non-compliant activities or take other necessary action to rectify a violation when there is a need to protect an individual's rights and interests in cases where the business operator has violated the various provisions of the APPI; and

4 During fiscal year 2022, there was one case in which the PPC investigated business premises, but there were 81 cases in which the PPC required business operators to submit information or materials.

5 During fiscal year 2022, there were 115 cases in which the PPC issued guidance or advice to business operators.

- order a business operator to take action in line with the recommendation when a serious infringement of an individual's rights and interests is imminent in cases where the business operator, having received an earlier recommendation pursuant to the APPI, failed to take action in line with it without a legitimate excuse.

A business operator who has violated an order pursuant to the APPI may be punished by imprisonment with labour for not more than one year or a criminal fine of not more than ¥1 million. If a representative, agent or employee of a business operator has violated an order pursuant to the APPI, that individual may be punished as above, but the business operator itself may also be punished with a criminal fine of up to ¥100 million.

Surveillance laws

CCTV

Images of individuals captured by a surveillance camera and facial recognition data obtained from these images fall under the definition of personal information if the images or data can be used to identify a specific individual.

In addition, when such images or facial recognition data are stored in a systematically organised manner, they fall under the definition of 'personal information database' and are treated as personal data.

The regulations under the APPI would, therefore, apply to the collection, use or transfer of images of individuals captured by a surveillance camera and facial recognition data obtained from those images.

Email monitoring

Article 21, paragraph 2 of the Constitution guarantees the secrecy of any means of communications as a basic human right. In accordance with the Constitution, the Telecommunications Business Act, the Wire Telecommunications Act and the Radio Act contain provisions protecting the secrecy of telecommunications.

For example, the Telecommunications Business Act provides that 'the secrecy of communications being handled by a telecommunications carrier shall not be violated', which prohibits a third party other than originators and recipients from intentionally viewing communications managed by the telecommunications carrier. Any person who violates provisions of the Telecommunications Business Act is subject to criminal punishment. For example, any person who has violated the secrecy of communications handled by a telecommunications carrier may

be punished by imprisonment with labour for up to two years or subject to a criminal fine of up to ¥1 million.

Accordingly, private organisations may not conduct email monitoring in principle. If a company investigates employees' emails that are stored on an internal server to investigate misconduct in the company, this investigation may not violate the secrecy of communications or the right of privacy; however, when conducting an investigation, a cautious approach would be to obtain the consent of the data subject and, if that is not possible, obtain qualified legal advice.

Case studies

Benesse Corporation (Benesse) contracted Synform Co Ltd (Synform) for the development and operation of a system to analyse the personal information of Benesse's customers. In 2014, it became known that an employee of a subcontractor of Synform had leaked personal information of multiple customers of Benesse (including details such as name, gender, date of birth, address, telephone number and email address). The incident garnered significant attention.

Several civil (Japanese-style) class action lawsuits have been led against Benesse and Synform by customers based on tort, claiming damages for mental suffering. In one of those lawsuits, the Tokyo High Court entered a judgment on 27 June 2019, finding Benesse and Synform liable and ordering them to pay ¥2,000 to each individual plaintiff. In another separate lawsuit, the Tokyo High Court entered a judgment on 25 March 2020, confirming the liability of Benesse and Synform and ordering them to pay ¥3,300 to each individual plaintiff. The decision of 25 March 2020 has been upheld by the Supreme Court of Japan.

Furthermore, the Tokyo High Court referred to the fact that Benesse had paid voluntary compensation to each victim (¥500 per person to approximately 35 million people). As a result of the incident, Benesse recorded a ¥26 billion special loss during one fiscal year, including ¥6 billion to strengthen security controls and ¥20 billion to fund voluntary compensation.

This case demonstrates that it is important to comply with Japanese data protection regulations to mitigate risks of dispute.

Akira Matsuda

Iwata Godo

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and data protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including M&A, international disputes (litigation and arbitration), and advice on digital and TMT-related matters. Mr Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore's Personal Data Protection Act and the EU General Data Protection Regulation), including on the structuring of global compliance systems. He also advises on complicated cross-border corporate investigation matters.

He is a graduate of the University of Tokyo (LLB) and Columbia Law School (LLM).

Tomonori Fujinami

Iwata Godo

Tomonori Fujinami is a Japanese attorney-at-law and an associate at Iwata Godo. He deals with a wide range of corporate legal affairs, focusing on commercial lawsuits and disputes. He also has advised many clients on data protection and privacy issues, including under Japanese laws and the EU General Data Protection Regulation. He graduated from Waseda University (LLB) and Keio University (JD).

Riko Suzuki

Iwata Godo

Riko Suzuki is a Japanese attorney-at-law and an associate at Iwata Godo. Her practice focuses on corporate law and includes corporate governance and competition law, shareholders' meetings (listed companies) and dispute resolution. She has advised several clients on data protection and privacy issues. She graduated from Hitotsubashi University (LLB and JD).

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 80 attorneys, and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection.

Marunouchi Building 15F
2-4-1 Marunouchi,
Chiyoda-ku
Tokyo 100-6315
Japan
Tel: +81 3 3214 6205

www.iwatagodo.com

Akira Matsuda
amatsuda@iwatagodo.com

Tomonori Fujinami
tomonori.fujinami@iwatagodo.com

Riko Suzuki
riko.suzuki@iwatagodo.com