iclg

Data Protection 2025

12th Edition

Contributing Editors:

Tim Hickman & Dr. Detlev Gabel

White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Cloud Computing, Privacy Impact Assessments and Record-Keeping Regarding Data Protection in Japan


Yusaku Akasaki


Hiroki Minekawa


Ronald Kaloostian

Chuo Sogo LPC

1. Introduction

Data protection in Japan is governed by the Act on the Protection of Personal Information and its amendments ("APPI"), which was enacted in 2003 and fully came into force in 2005. Thereafter, the APPI was amended in 2015, 2020 and 2021. Currently, there are discussions regarding amendments to the APPI that may introduce an administrative penalty system in addition to the current fines, and establish systems for injunction claims and remedies for damages on behalf of consumer organisations.

The most notable change with the 2015 amendment, which fully came into force in 2017, was the establishment of the Personal Information Protection Commission ("PPC"). The extraterritorial application of the APPI was expanded as well.

The 2020 amendment fully came into effect in 2022 and included clarifications about personal information with regard to its ability to identify an individual, i.e. "person-related" rather than personal information, as well as pseudonymous information. It introduced a prohibition on a business operator handling personal information using personal information to potentially facilitate illegal or inappropriate acts. It also introduced the requirement that the APPI has to be reviewed every three years.

In this chapter we will address three specific topics under the APPI, as follows:

- privacy and security in cloud computing, focusing on a recent administrative case;
- Privacy Impact Assessments ("PIA") in Japan; and
- records concerning the provision of personal data[1] to third parties in Japan.

2. Privacy and Security in Cloud Computing

Below we will discuss the evolving requirements for data protection in Japan for organisations using cloud computing. This could include the security and privacy challenges of storing and processing data in the cloud, and Japan's regulations concerning cloud service providers and data centres.

In the context of information and communication technology, the term "cloud computing", or simply "cloud", refers to the provision of certain computing resources "as a Service" over the internet, or to such computing systems that are used to provide such services. There are many instances where a company stores and uses personal data of its customers or employees in the cloud; however, in some cases, this can cause a problem in relation to the regulation under the APPI. This section discusses the relationship between cloud usage and the APPI, focusing on the regulations on the provision of personal data to third parties (as well as the issues related to the restrictions on the provision of personal data to third parties in foreign countries).

When a company stores and uses personal data of its customers or employees in the cloud, that personal data is transferred from the company to the cloud service provider. In view of the regulations imposed under Japanese law on the "provision" of personal data to third parties, a cloud service provider planning to operate cloud services in Japan may adopt one of the following three legal solutions: (1) obtaining the consent from the individuals; (2) entrustment; and (3) the so-called "cloud exception".

1. Obtaining the consent from the individual

Japanese law allows the provision of personal data to third parties, provided that the consent from the individual to whom the personal data belongs (hereinafter the "individual") is obtained (Article 27, paragraph (1) of the APPI). In reality, however, it may not always be easy for companies to comply with this provision, because obtaining consent from the individuals may not be straightforward when companies hold various types of personal data. For example, in the case where a company collects the personal data of its customer's family, to store the collected data in the cloud it uses, it must obtain, directly or indirectly, the prior consent of each family member concerned, otherwise it cannot use the cloud for dealing with the collected data. As this is extremely impractical, the company may give up using the cloud after all.

It should also be noted that Japanese law puts an additional restriction on the provision of personal data to "third parties in foreign countries"[2] (Article 28 of the APPI). A foreign business operator (i.e., a business operator established in a foreign country) that receives personal data from a business operator handling personal information in Japan does not fall into the category of "third parties in foreign countries", provided that the former is also a "business operator handling personal information" in Japan (Section 2-2 of *the Volume on Provision to a Third Party in a Foreign Country, the Guidelines for the Act on the Protection of Personal Information* (the "APPI Guidelines")), because Japanese law applies to business operators handling personal information in Japan. On the other hand, however, it is also provided that whether a foreign business operator qualifies as a "business operator handling personal information" under Japanese law is determined on a case-by-case basis, taking into consideration the actual state of its business in Japan,[3] from which it can be said that the criteria for such determination are yet to be clearly defined. If a foreign

business operator takes "appropriate and reasonable means" (Article 16 of the APPI enforcement rules) in appropriate ways, the "restriction on the provision of personal data to third parties in foreign countries" does not apply to the foreign business operator. However, this is also determined on a case-by-case basis (Section 4-1 of the APPI Guidelines).

Accordingly, it can be said that, for foreign business operators planning to operate a cloud business in Japan, it should be hard to establish such a business based on the self-procurement of individual consent and hence they should adopt other solutions, namely entrustment or cloud exception (discussed below).

2. Entrustment

If the act of storing and using personal data in the cloud can be deemed to constitute the "entrustment" of personal data-handling to a cloud service provider, it does not fall under third-party provision (Article 27, paragraph (5), item (i) of the APPI). "Entrustment" of personal data-handling means that "a 'business operator handling personal information' is having another party handle personal data by any form or type of contract" (GL3-4-4 of the General Rules of the APPI), and is considered one of the grounds for exceptions to third-party provision regulations under Japanese law. As explained below, there are cases where it is difficult to adopt the solution of "cloud exception" and the only available solution is "entrustment". Please be advised that if the cloud service provider is located in "foreign countries" under the PPC, the "entrustment" theory cannot be used.

The entrustor has an obligation to supervise the entrustee (Article 25 of the APPI). Hence, a business operating cloud services in Japan is subject to the supervision by the entrustor (i.e., the cloud user). The entrustor is required to supervise the entrustee to ensure that the entrustee takes security control measures equivalent to those the entrustor should take under Article 23 of the APPI; cloud users may thus demand strict supervision of cloud service providers.

However, if, at the request of a cloud user, a cloud service provider discloses its server configuration details to the cloud user or allows the cloud user to enter into its data centre without careful consideration, the cloud service provider risks losing trust from other cloud users. On the other hand, the cloud service provider may not refuse all of the user's demands on supervision, due to the strict obligation of supervision imposed on the user.

The PPC closely monitors compliance with such obligation. For example, in the Notice it issued on March 25, 2024, the PPC called for the attention of business operators handling personal information by reminding them of the key consideration for employing a cloud service provider, as follows:

- Before selecting cloud service providers and services, fully understand and confirm not only the functions and support system of the target services but also the security measures included in the services.
- Clearly document the content of necessary and appropriate security control measures (including the roles and responsibilities in the handling of personal data) agreed with the cloud service provider concerning the handling of personal data as objectively as possible in the form of terms and conditions or a contract (Q5-8 of *FAQs on the APPI Guidelines*).
- Review the statuses of the security measures and the security control measures of the service being used, by, for example, obtaining regular reports from the cloud service provider.

In this context, it can be said that an extremely careful judgment must be made regarding the extent to which a cloud service provider should accept the cloud users' demands on supervision.

There are hardly any examples of administrative advice on the level of supervision required for cloud use, and the PPC does not have any explicit judgment criteria. Such being the situation, consulting a law firm specialised in the APPI may be essential for those engaged in the cloud businesses.

3. Cloud exception

The "cloud exception" is a concept that in a third-party provision of personal data, no consent thereto is required in the cases where the contract stipulates that the recipient of the data shall not "handle the received personal data" because such cases do not constitute provision of personal data from a company to a cloud service provider (Q7-53 *op. cit.*). Such a concept of excluding an act of storing in and using the cloud from the scope of "provision" is unique to Japan, as by contrast, the General Data Protection Regulation includes the act of storing personal information *per se* in the definition of the term "processing".

It is said that to "not handle personal data" refers to the cases where the contract stipulates that the cloud service provider shall not handle the personal data stored on the server and where appropriate access control is in place (Q&A7-53 *op. cit.*). As mentioned above, the "cloud exception" is a concept unique to Japan, and the conditions for applying the "cloud exception" are not clear, with many issues remaining unresolved also in the APPI. For example, while it is required that the contract contains a provision of "no handling of personal data", in practice, virtually no business operators stipulate "no handling of personal data" in any case. It is thus very difficult to determine what kind of cases are appropriate for stipulating disclosure of personal data.

In recent years, there was a case where the PPC denied the applicability of the cloud exception. It is a case involving information leakage at MKSystem Corporation ("MK"), a provider of business systems services dedicated to certified social insurance and labour consultants. The PPC denied the applicability of the cloud exception to that case on the grounds that MK had been in fact a cloud service provider entrusted with the handling of personal data, rather than a provider "not handling personal data", which is recognised as a case that put a brake on the mass-producing of cloud exception cases.

Specifically, the PPC denied the applicability of the cloud exception for reasons including the following:

- The terms of use stipulated specific cases where MK was allowed to use personal data pertaining to the clients of the certified social insurance and labour consultants or others using the service.
- MK had a maintenance ID that provided MK with access to the personal data in the system where no technical access control or other measures were taken to prevent MK's unauthorised handling of the data.

It is said that until this decision was presented, there were many cases that were easily configured as cloud exceptions.

In the event where the applicability of the "cloud exception" is denied, the relevant business operator handling personal information and the cloud service provider may face the risk of having to drastically reorganise their cloud business operation. Hence, failure to comply with Japanese law can be a major blow to both business operators handling personal information and cloud service providers. However,

the option of "entrustment" is not quite user-friendly in view of the supervisory obligations. After all, for foreign business operators planning to operate a cloud business in Japan, use of the last option, namely the "cloud exception", should be the best solution.

On the other hand, as can be seen from the fact that the PPC also denies, in general terms, the applicability of the "cloud exception" to cases involving processing of personal data including editing and analysing ("Response from the competent authority to the request for consideration, FY2022, No. 307"), it is difficult to rely on a legal position to the deployment of SaaS (i.e., software and services made available over the internet) in Japan. Consequently, the option of "entrustment" should also be legally positioned as a secondary solution, because relying solely on the option of "cloud exception" is too risky. In the future, as the PPC's administrative advice examples accumulate, the legal positioning of cloud use should become clearer. Until then, at least for the time being, a safe way to operate may be to take a two-tier approach with the "cloud exception" as the primary solution and "entrustment" as the secondary solution.

3 PIA

Are PIA required under Japanese law? If so, in what circumstances and what should they include?

Under Japanese law, PIA is not considered a mandatory obligation for business operators handling personal information. However, when handling personal information, it is crucial to incorporate the protection of individual rights and interests, including personal information protection, into the design stage of business operations. PIA, a risk management method that evaluates potential impacts in advance to reduce or avoid risks of infringing on privacy and other individual rights and interests during the initiation or modification of businesses involving the collection of personal information, is encouraged as a voluntary initiative. In 2021, the PPC published a report titled "Promotion of PIA Initiatives – Points to Consider in Line with the Significance and Implementation Procedures of PIA", which discusses the significance and specific methods of PIA.

The significance and effects of implementing PIA include the following:

1. Gaining trust from stakeholders, including consumers: It serves as proof of appropriate measures taken to comply with laws and reduce risks, contributing to social credibility. Additionally, by publishing results, it fulfils accountability, enhances transparency and helps eliminate information asymmetry between consumers and business operators handling personal information.
2. Reducing total business costs: Necessary measures can be taken before deciding on significant system investments or business discontinuation, ultimately controlling total business costs.
3. Improving governance, including employee education: Employees become aware, and management can grasp the handling status of personal information, thereby improving governance.

An example of specific implementation procedures includes:

- "Preparation", which involves comprehensive and broad information collection and organisation, such as system development and confirmation of personal information flows, after considering whether to implement PIA.
- "Risk Identification and Evaluation", where evaluators specifically identify and assess risks related to personal information handling and identify significant risks and matters requiring action based on the preparation.
- "Risk Reduction", where designers and others formulate and execute specific measures and plans to reduce the risks identified and evaluated.

In practice, the approach varies depending on the scale, nature and content of personal information, and it is important for business operators handling personal information to consider the optimal method themselves. The results of PIA implementation should be compiled into a report, not only for reporting to the management of the business operators handling personal information but also for external publication from the perspective of accountability and transparency to stakeholders, including consumers. In such cases, it is effective to create a summary and publish it concisely and understandably, rather than detailing the implementation results.

The report may include the flow of personal information handling, the scope of PIA implementation within that flow, implementation methods, identified risks, evaluation results of those risks, and countermeasures. Although PIA is not a legal obligation in Japan, it is promoted as a voluntary initiative, and considering that some countries have made it a legal obligation, it is expected that more businesses will implement it in the future. When implementing, it is important not to do so aimlessly but to fully understand its significance and ensure appropriate effects, implementing PIA content suitable for each business.

There is no requirement to consult the data protection authority before processing if a PIA indicates high risk.

4 Records Concerning the Provision of Personal Data to Third Parties

Are organisations required to maintain internal records of their processing activities? If so, what details must be recorded and who can access them?

Yes, business operators handling personal information must create records concerning the date of provision of personal data to third parties and the name or title of the third party when providing or receiving personal data from third parties. The principle is to create records promptly each time personal data is exchanged, but there is an exception where records can be created collectively instead of individually when personal data is exchanged continuously or repeatedly with a specific business within a certain period.

Additionally, when entering into a contract for the provision of goods or services to the person and providing personal data of the contracting party to a third party in the course of fulfilling the contract, it is possible to track the distribution of personal data using the contract or other documents created at the time of provision, and these documents can serve as records.

Records must include the following items:

When providing to third parties with consent:

1. "Name or title and address of the third party, and in the case of a juridical person, the name of its representative."
2. "Name of the person identified by the personal data and other matters sufficient to specify the person."
3. "Items of the personal data."
4. "Statement of obtaining the person's consent."

When receiving with consent:

1. "Name or title and address of the third party, and in the case of a juridical person, the name of its representative."

2. "Background of the third party's acquisition of the personal data."
3. "Name of the person identified by the personal data and other matters sufficient to specify the person."
4. "Items of the personal data."
5. "Statement of obtaining the person's consent."

In certain cases, it is possible to omit record items. Regarding the recorded third-party provision records, if a disclosure request is made by the person, it is necessary to disclose the information to the requesting parties without delay. However, in the following cases, it is exceptionally permissible not to disclose all or part of the records:

1. Cases where disclosure is likely to harm the life, body, property, or other rights or interests of the person or a third party.
2. Cases where disclosure is likely to seriously impede the proper execution of the business of the business operator handling personal information.
3. Cases where disclosure violates other laws and regulations.

5 Conclusion

Above we discussed three important topics regarding data protection in Japan. First, as the PPC addresses more cases with respect to cloud computing, we expect the scope of the "cloud exception" to become clearer. However, as the MK case indicates, a provider of business systems services over the internet may be considered to have been entrusted with the handling of personal data, in which case the option of "entrustment" should also be legally positioned as a secondary solution. Thus, it may be prudent for companies to follow a two-tier approach for the time being with the "cloud exception" as the primary solution and "entrustment" as the secondary solution.

Second, in Japan, although PIA is not a legal obligation, it is encouraged as a voluntary initiative to reduce or avoid risks of infringing on privacy and other individual rights and interests. When implementing, it is important to fully understand its significance, implementing PIA content suitable for each business.

Finally, in Japan, business operators handling personal information must create records concerning the date of provision of personal data to third parties and the name or title of the third party when providing or receiving personal data from third parties. Although the principle is to create records promptly each time personal data is exchanged, there is an exception where records can be created collectively instead of individually when personal data is exchanged continuously or repeatedly with a specific business within a certain period. If the data subject requests the business operator to disclose its own personal data, in general the business operator shall disclose the personal data to the data subject. Notwithstanding this obligation, there are exceptional cases in which it is permissible not to disclose all or part of the records (e.g., likely to harm the life, body, property, or other rights or interests of the person or a third party).

Endnotes

1 We use the terms "personal data" and "personal information". To be precise, the definitions are different under the APPI, but we do not distinguish them in this chapter.

2 However, Article 28 excludes countries that are prescribed by Order of the PPC as having a personal data protection system recognised as being of a similar standard to that of Japan from the scope of "foreign countries". For example, as of the time of writing this chapter, EEA countries (EU countries, Iceland, Liechtenstein and Norway) and the UK do not fall under the category of "foreign countries".

3 See Q12-5 of *FAQs on the APPI Guidelines*. Since the location of the server is not a criterion for determination, if a U.S. company's server is located in an EU country and a Japanese business operator handling personal information stores personal data in the cloud on that server, it is deemed a transfer to a third party in the U.S. (i.e., subject to Article 28 of the APPI).

Yusaku Akasaki handles a wide range of consultations for corporate clients and has extensive (foreign and domestic) experience, particularly in corporate law, M&A, labour and employment matters, competition law and data protection law.
Leveraging his study abroad experiences in the United States and the Middle East, Yusaku frequently provides support and advice to clients on cross-border commercial transactions, data protection matters and M&A.

Chuo Sogo LPC
Osaka Dojimahama Tower 15th Floor
1-1-27 Dojimahama, Kita-ku
Osaka, 530-0004
Japan

Tel: +81 6 6676 8834
Email: akasaki_y@clo.gr.jp
LinkedIn: www.linkedin.com/in/yusaku-akasaki-856379a5

Hiroki Minekawa has completed one year of legal training, and has worked as a lawyer at Chuo Sogo LPC for two years. He particularly works on cases related to IT law and Finance law.
He offers practical advice about the Act on the Protection of Personal Information in Japan and also handles a number of general litigation cases.

Chuo Sogo LPC
Osaka Dojimahama Tower 15th Floor
1-1-27 Dojimahama, Kita-ku
Osaka, 530-0004
Japan

Tel: +81 6 6676 8834
Email: minekawa_h@clo.gr.jp
URL: www.clo.jp/english/lawyers/688

Ronald Kaloostian worked in the in-house IP department of a major Japanese innovator pharmaceutical company for over 11 years. He specialised in IP licensing, IP due diligence, joint research collaborations with US universities, strategic biopharma alliances and spin out of new companies with novel technologies and inventions. Ron joined Chuo Sogo LPC in 2023 and practises in the areas of IP, M&A, International Transactions, Data Privacy and Cybersecurity, and Global Compliance.

Chuo Sogo LPC
Hibiya Kokusai Building, 18th Floor
2-2-3 Uchisaiwaicho, Chiyoda-ku
Tokyo 100-0011
Japan

Tel: +81 3 3539 1877
Email: ronald_k@clo.gr.jp
LinkedIn: www.linkedin.com/in/ronald-kaloostian-700b627

iclg International Comparative Legal Guides

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

Data Protection 2025 features four expert analysis chapters and 27 Q&A jurisdiction chapters covering key issues, including:

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

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