JAPAN

Law and Practice

Contributed by:
Yasushi Kudo, Tsubasa Watanabe and Hayato Maruta
Nagashima Ohno & Tsunematsu

Contents

Nagashima Ohno & Tsunematsu (NO&T) is one of the foremost providers of international and commercial legal services, based in Tokyo, with over 550 lawyers, including nearly 50 experienced foreign lawyers from various jurisdictions. The firm's overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, and collaborative relationships with prominent local law firms throughout Asia, Europe, North and South America, and other regions. NO&T provides comprehensive assistance in the development of cybersecurity systems, including the establishment of internal governance systems and vendor management. The firm also has extensive experience in crisis management in the event of a security incident. In collaboration with IT system experts, NO&T also provides one-stop support for the entire process, from the initial response, including fact-finding and evidence preservation, to dealing with the authorities, information disclosure and the mass media, handling victims, root cause analysis, and recurrence prevention measures.

Authors

Yasushi Kudo is a partner at Nagashima Ohno & Tsunematsu. He mainly focuses on crisis management, including dealings with domestic and international authorities, regulatory compliance, cybersecurity/data privacy, and advice on compliance systems and corporate governance, leveraging his expertise and experience gained from secondment to the Financial Services Agency and the Securities and Exchange Surveillance Commission. Recently, his focus has been on legal issues raised by cybersecurity incidents such as ransomware attacks, data compromise and business email compromise, as well as the development of internal control systems so as to mitigate cybersecurity risks such as supply chain risk.

Tsubasa Watanabe is an associate at Nagashima Ohno & Tsunematsu. He focuses his practice on white-collar crime, regulatory, and investigation matters involving allegations of fraud, accounting irregularities, misleading representation, bribery and corruption, and violations of labour law and competition law. Specifically, he has significant experience addressing quality issues (data falsification, improper testing, etc) in respect of numerous manufacturing companies, leading investigations while designing comprehensive remedial measures and advising on responses to regulatory agencies. He has also helped guide companies to successfully adapt their businesses to the rapidly changing regulations, globally, relating to cybersecurity, AI, and data privacy regulations.

Hayato Maruta is an associate at Nagashima Ohno & Tsunematsu. He mainly focuses on crisis management, including dealings with domestic and international authorities, regulatory compliance, cybersecurity/data privacy, cartel and advice on compliance systems and corporate governance. He is also registered as a cybersecurity specialist and has extensive knowledge of cybersecurity. He is also highly knowledgeable about AI regulations in Japan. As a government committee member, he helped compile the AI Business Operator Guidelines, which form the foundation of AI regulations in Japan, and has experience proposing AI regulatory bills to the ruling party.

Nagashima Ohno & Tsunematsu

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo, 100-7036
Japan

Tel: 81-3-6889-7396
Fax: 81-3-6889-8396
Email: yasushi_kudo@noandt.com
Web: www.noandt.com/en/lawyers/yasushi_kudo

NAGASHIMA OHNO & TSUNEMATSU

1. Data Privacy Regulations

1.1 Data Privacy and Cloud Computing

The primary laws concerning data privacy in Japan are the Act on the Protection of Personal Information (APPI) and the Telecommunications Business Act. The APPI, defines (i) personal data as personal information that can identify a particular individual and that forms part of a personal information database; and (ii) sensitive personal information as personal information that requires special handling to prevent unfair discrimination, prejudice, or other detriment.

The APPI does not contain specific regulations regarding the handling of personal data in the cloud. In principle, when a user company stores personal data in the cloud, that is considered a provision to a third party, which, under the APPI, requires the consent of the individual whose personal data is being processed. However, the Personal Information Protection Committee (PCC) has indicated that if the cloud service vendor is not deemed to handle personal data, the vendor's involvement does not constitute third-party provision. As a result, under the "cloud exception", no consent of the individual's is required. Situations where the cloud service vendor is not deemed to handle personal data include cases where the contract explicitly stipulates that the cloud service vendor shall not handle personal data stored on the server, and where appropriate access controls are implemented.

The following are the factors considered in deeming that the cloud service vendors handle personal data: (i) the vendor's terms of service allow the use of the user company's personal data under certain circumstances, and (ii) the cloud service vendor possesses a maintenance ID and has access to the user company's personal data, and there is no implementation of technical access controls to restrict such access.

1.2 Data Privacy and Cross-Border Transfers

When transferring personal data overseas, in principle the APPI's cross-border transfer regulations apply. However, there are no regulations that apply specifically to cloud usage. Under the APPI, when providing personal data to individuals or entities in countries that do not have a recognised personal information protection system equivalent to that of Japan, or that do not have a system that meets the specified standards, the consent of the individual identified by such personal data is required.

However, the "cloud exception" may also apply in such cases, meaning that the transfer may not be classified as a "provision" and therefore might not require the individual's consent.

1.3 Penalties for Non-compliance With Data Privacy Regulations

There are no penalties or sanctions that apply specifically to the use or provision of cloud services.

2. Data Security Measures

2.1 Data Security and the Cloud

Japan has no laws and regulations that apply specifically to data stored in the cloud, regardless of where the data is stored; however, in accordance with the APPI, "[a] business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data" (Article 23). Such measures "shall be necessary and appropriate ones in light of the scale and nature

of the business, the status of handling of personal data (including the nature and volume of personal data), and the risks arising from the nature of the media on which the personal data is stored, taking into account the seriousness of the infringement of the rights and interests of the individual in the event of leakage of personal data, etc." (Guidelines for the Protection of Personal Information (General Rules) (the "APPI Guidelines"), Section 3-4-2, p 53). Section 10 of the APPI Guidelines also sets out the measures that should be implemented (eg, formulation of a key principle in respect of protection of personal information; establishment of rules for handling personal data; organisational and personnel security control measures, as well as physical and technical security control measures; and monitoring of the external environment). The specific measures are left to the discretion of the business operator.

In addition, the Information Security Guidelines for Cloud Service Provision (3rd Edition) (Ministry of Internal Affairs and Communications (MIC), 2021), although they are not legally enforced (the guidelines are, however, referred to in practice), set forth the security and organisational requirements relating to cloud services and their providers, such as (i) the development of relevant regulations and response procedures, and of organisational measures, including employee training; and (ii) technical and physical measures, including access management, encryption and authentication, change history management, implementation of failure monitoring, and measures for physical security of data centres and the like.

In addition to the above Information Security Guidelines for Cloud Service Provision (3rd Edition), the Information Security Management Guidelines for the Use of Cloud Services (Ministry of Economy, Trade and Industry (METI), 2013) and the ISMAP (Information System Security Management and Assessment Program) Management Standards (ISMAP Steering Committee, revised 2024) also stipulate general security requirements that apply to cloud services. Furthermore, some guidelines apply additionally to the handling of data in specific business fields. For example, in the medical and financial sectors, certain additional guidelines apply to the use of cloud services:

- in the medical sector, the Guidelines for the Safe Management of Medical Information Systems, 6.0 Edition (Ministry of Health, Labour and Welfare, 2023) and the Guidelines for the Safe Management of Information Systems and Services that Handle Medical Information, 1.1 Edition (METI and MIC, 2023); and
- in the financial sector, Safety Measures Standards and Commentary for Computer Systems at Financial Institutions (12th Edition) (The Center for Financial Industry Information Systems, 2024).

Regardless of where the data is stored, unauthorised access is prohibited by the Act on Prohibition of Unauthorised Computer Access and is subject to punishment (Article 3):

- "Any person who has violated the provisions of Article 3 is punished by imprisonment with work for not more than three years or a fine of not more than 1 million yen." (Article 11).

Therefore, if there is unauthorised access to data on the cloud, the investigative authorities will conduct an investigation or prosecution as far as they have jurisdiction.

In the event of a security incident, regardless of whether on the cloud or not, under certain circumstances the business operator is obliged to report the incident to the government or other body. For example, if there is a leak of personal data due to a security incident, a business operator handling that data is obligated to report it to the PPC (Article 26, Paragraph 1 of APPI; see **5 Data Breach Notification** for details). Depending on the nature of the business, the business operator may also be obligated to report the incident to the relevant government agency under the law regulating the said business (eg, Telecommunications Business Act, Article 28). Even if reporting is not legally required, it is recommended that security incidents be reported to the relevant authorities and the Information-technology Promotion Agency (IPA) based on the guidelines above.

3. Data Ownership and Control

3.1 Data Ownership in Cloud Agreements

Although Japan has no laws and regulations that apply specifically to data stored in the cloud, the APPI applies to personal data regardless of where the data is stored. In accordance with the APPI, the data subject of personal data is entitled to request notification of the purpose of utilisation (Article 32, Paragraph 2), disclosure (Article 33), and correction (Article 34) of the personal data held by the business operator handling personal information. In addition, if the said business operator violates laws and regulations in its utilisation of the personal data or no longer needs to use the data, the said data subject can request that the said business operator discontinue use of, or erase, the personal data (Article 35). Likewise, regarding personal data held by government agencies and other public bodies, regardless of whether the data is stored in the cloud or not, the data subject is entitled to request disclosure, correction, discontinuance of use, or erasure or the like of the personal data under certain circumstances (Articles 76, 90, 98).

As these rights must be exercised against the business operator handling personal data, when a data subject exercises these rights concerning personal data stored in the cloud, the request must be made, using the methods specified by that business operator, to the business operator that is using the relevant cloud service and is holding the relevant personal data, rather than to the cloud service provider itself.

In addition, according to some surveys in 2022 (cf. Synergy Research Group, MMRI), the most prevalent cloud service among businesses in Japan is Amazon Web Service (AWS), and the AWS Customer Agreement (in Japan: governed by the laws of Japan) provides:

- "We will not access or use Your Content except as necessary to maintain or provide the Services, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to any government or third party or (b) move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body." (Article 1.4).

The AWS Customer Agreement provides that the service user (business operator) who uses the cloud service to handle personal data should respond to the above-mentioned request from the data subject.

3.2 Data Portability

Regardless of whether the data is stored in the cloud or not, Japan has no laws and regulations that specifically stipulate data portability as a right of the data subject; ie, as stated in **3.1 Data Ownership in Cloud Agreements** and **3.3 Data Retention and Deletion**, while the rights of data subjects are recognised under the APPI with regard to the disclosure, correction, discontinuance of use, or erasure of personal data, no comprehensive data portability rights, as stipulated in the European GDPR, are recognised in Japan, regardless of whether the data is in the cloud or not.

3.3 Data Retention and Deletion

Japan has no laws and regulations that apply specifically to data stored in the cloud, regardless of where data is stored; however, in accordance with the APPI: "A business operator handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Utilization." (Article 22).

In addition, a business operator shall respond to requests from data subjects for the disclosure, correction, discontinuance of use, or erasure, of personal data (Articles 33, 34, and 35).

Therefore, under the APPI, business operators handling personal data are required to establish procedures (policies) for the disclosure, correction, or for the discontinuance of use, or for erasure, or the like, of the personal data they hold and to disclose these procedures to the data subjects in advance (Article 32, Paragraph 1, Item 3). Specifically, it is necessary to post information regarding the procedures and policies on websites, brochures, and the like, or to set up a contact point for inquiries (APPI Guidelines (General Rules) 3-8-1, p 125).

4. Vendor Management

4.1 Due Diligence

In Japan, no legislation stipulates a legal obligation to carry out due diligence when selecting a cloud service provider; however, if the cloud service provider is deemed to be a subcontractor (processor) handling personal data (for more information on the criteria, reference should be made to "Points to note when a cloud service provider falls under the category of a business operator handling personal information under the APPI (Alert)" (PPC, 2024)), the business operator handling and storing personal data in the cloud is obliged to supervise the cloud service provider to ensure that appropriate safety management measures are taken (APPI Article 25). In relation to this obligation, the APPI Guidelines state that when selecting the said subcontractor, "business operators must confirm in advance that each item (stipulated in Section 10 (Safety Management Measures) of the APPI Guidelines) is implemented without fail in line with the content of the outsourced work" (APPI Guidelines 3-4-4(1), p 55).

In addition, in the context of information security and cybersecurity, certain guidelines (referred to in **2.1 Data Security and the Cloud**) formulated and published by the regulatory authorities in specific business fields also require that business operators use cloud services to supervise cloud service providers, as a means of outsourcing management. If, under this supervision, due diligence by the business operator is insufficient, they may be subject to administrative guidance, pursuant to the relevant business laws.

The scope and level of due diligence carried out when selecting a cloud service provider is fundamentally left to the discretion of the business operator, and various guidelines have been pub-

lished on this, including the SLA Guidelines for SaaS (METI, 2008) and the Cloud Service Level Checklist (METI, 2010). In addition, when government agencies use cloud services, they are required to select services that meet the requirements listed in 4.1 and 4.2 of the Uniform Standards for Cyber Security Measures for Government Agencies (2023) (Cyber Security Strategy Headquarters, 2023), and can select from among the compliant providers registered in the ISMAP Cloud Service List. The items in these unified standards can also be used as a reference when private sector businesses conduct due diligence when selecting a cloud service provider.

4.2 Data Protection in Cloud Service Agreements

The regulations and governmental guidelines regarding data protection that may be applicable when handling personal data in the cloud, as well as the security requirements demanded of cloud services, are as described in **2.1 Data Security and the Cloud**.

The AWS Customer Agreement (in Japan: governed by Japanese law), which is the most widely used cloud service in Japan, provides the following regarding data protection requirements in the cloud:

- AWS security: "Without limiting Section 8 or your obligations under Section 2.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure".
- Your accounts: "You will comply with the terms of this Agreement and all laws, rules and regulations applicable to your use of the Services... Except to the extent caused by our breach of this Agreement, (a) you are responsible for all activities that occur under your account, regardless of whether the activities are authorized by you or undertaken by you, your employees or a third party (including your contractors, agents or End Users), and (b) we and our affiliates are not responsible for unauthorized access to your account".
- Your security and back-up: "You are responsible for properly configuring and using the Services and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content".

Due to the nature of cloud services, the cloud service provider, including AWS, is responsible for the security of the cloud service itself, and the security of web services that use the cloud service is the responsibility of the business operators who are the users of the cloud service. Further, the AWS Customer Agreement stipulates that business operators that use cloud services must comply with data privacy regulations and that the business operators themselves are responsible for any liability incurred due to their activities, including any violations of the data privacy regulations. Thus, AWS (the cloud service provider) has designed its services such that business operators that use the cloud service take measures to comply with the regulations themselves.

Such design, encompassing the responsibility of service users with regard to compliance with security and privacy legislation, is used not only in the AWS Customer Agreement but also in the model contract for cloud services used in Japan (JISA Cloud Service Model Terms of Use and

Application Form (JISA, 2021), Articles 29 and 38).

4.3 Data Processing Agreements and the Cloud

Although the APPI does not have as detailed provisions as the GDPR regarding data processing agreements that are concluded when a business operator outsources the processing of personal data, it stipulates: "When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data." (Article 25). This requires business operators handling personal data to "supervise subcontractors to ensure that they take the same-level safety management measures as stipulated in Article 23 of the Act" through the conclusion of subcontracting agreements and the like (APPI Guidelines (General Rules) 3-4-4, p 54). As this provision applies regardless of whether personal data is stored in the cloud or not, in relation to managing the subcontractor (processor), the business operator will need to, even when handling personal data in a cloud environment, conclude a subcontracting agreement.

With regard to the content of the safety management measures to be stipulated in the subcontracting agreement, the APPI Guidelines require that the subcontractor (processor) must not subcontract handling of the personal data to a third party without the approval of the business operator which initially handled the personal data, and that the safety management measures listed in Section 10 of the APPI Guidelines (see **2.1 Data Security and the Cloud** for details) that are agreed upon between the business operator handling personal data and the subcontractor should be stipulated (APPI Guidelines (General Rules) 3-4-4(2), p 55).

4.4 Exit Strategies and Data Migration

The AWS Customer Agreement, the most widely used cloud service in Japan (in Japan: governed by the law of Japanese), provides: "You may terminate this Agreement for any reason by providing us notice and closing your account for all Services for which we provide an account closing mechanism. We may terminate this Agreement for any reason by providing you at least 30 days' advance notice." (Article 5.2(a)).

In either case, as long as there are no unpaid dues, the data on the cloud will remain available for 30 days after cancellation without being deleted (Article 5.3(b)).

The mechanism whereby users may cancel cloud services at their discretion is also adopted in the model contract for cloud services used in Japan (Article 15 of "JISA Cloud Service Model Terms of Use and Application Form" (JISA, 2021)).

As stated in **3.2 Data Portability**, Japan has no regulations regarding data portability, nor a system that allows data to be transferred from one cloud service provider to another after the contract with a particular cloud provider has ended. Therefore, users should take the necessary steps themselves if they want to transfer data from one cloud provider to another.

5. Data Breach Notification

5.1 Requirements to Report Data Breaches

The APPI provides for the general obligation to report personal information breaches and for penalties for non-compliance; however, there

are no obligations or penalties that apply specifically to breaches arising from the use of cloud services.

5.2 Investigating and Remedying Data Breaches

In general, regardless of whether data breaches involve the cloud, investigations and measures to prevent recurrence of data breaches are implemented in relation to information leakage incidents. However, there are certain particularities in relation to incidents involving the leakage of personal data stored in the cloud. Specifically, the cause of the leakage may not be limited to the user company but could also involve the cloud service vendor. Therefore, it is advisable for the user company not only to conduct its own investigation but also to request an investigation from the cloud service vendor or to ensure, through pre-established contractual terms, that the user company has the ability to conduct such an investigation.

5.3 Notifying Data Breaches

Under the APPI, if there is a case of, or the risk of, loss, damage, or leakage ("Leakage, etc"), there is an obligation to submit an initial report to the PCC within three to five days from the date of awareness of such Leakage, etc. Further, a detailed report must be submitted within 30 days from the date of the awareness. Furthermore, the individual whose personal information was subject to such Leakage, etc must be promptly notified. Both the initial and detailed reports must include the details of the Leakage, etc and the categories of personal data that were affected.

If a cloud service vendor is deemed to handle personal information stored in the cloud and the aforementioned "cloud exception" does not apply, the cloud service vendor may be deemed to be a subcontractor handling personal data. In this case, the cloud service vendor also has the obligation to report and notify the Leakage, etc. However, if the cloud service vendor notifies the user company, the vendor is not required to directly notify the PCC or the individuals affected. Instead, the principal (user company) is responsible for making the necessary reports and notifications.

6. International Data Transfers

6.1 Cross-Border Transfer Regulation

As noted in **1.2 Data Privacy and Cross-Border Transfers**, the cross-border transfer regulations under the APPI apply when providing personal data to third parties located abroad. Additionally, the guidelines established by the PCC require that, even in cases where the "cloud exception" applies, if personal data is stored on servers located in foreign countries, the user company itself is considered to be handling personal data abroad. Therefore, the user company must understand the personal information protection systems of the respective foreign countries and take necessary and appropriate measures to ensure security (known as "the obligation to understand external environments").

Furthermore, following the 2022 amendment to the APPI, it is now required that measures taken to ensure the security management of retained personal data be made known to the individual. This means that, among other necessary actions, companies must disclose the name of the foreign country where the cloud service vendor is located and the name of the foreign country where the server storing the personal data is located.

6.2 Data Localisation

In Japan, aside from cross-border transfer regulations, there are no specific data localisation requirements.

6.3 Conflicts of Law

In cases where legal regulations apply that are different from those of Japan, such as requirements in respect of government access or domestic storage requirements, the rights and interests of individuals are potentially harmed. Or, when using foreign cloud service vendors that utilise servers outside Japan, it is possible that data cannot be repatriated to Japan upon contract termination due to the data localisation regulations of the foreign country. To address such scenarios, the APPI and the guidelines thereto establish the obligation to understand external environments and take necessary safety management measures, as mentioned in **6.1 Cross-Border Transfer Regulation**.

Furthermore, the requirement to obtain the individual's consent when providing personal data to entities in countries that do not have a personal information protection system recognised as equivalent to Japan's, or that have not established compliant frameworks, also helps to mitigate risks arising from differences between foreign legal systems and Japanese law.

7. Compliance and Audits

7.1 Cloud Computing and Compliance/Audits

In Japan, there is no legislation that stipulates a direct legal obligation to conduct compliance audits of cloud service providers. As a result, no legislation stipulates procedures for compliance audits of cloud environments, mechanisms for ensuring effectiveness, penalties, etc.

However, if a cloud service provider falls into the category of a subcontractor handling personal data, the business operator which initially handled the personal data is obligated to supervise the said cloud service provider to ensure that appropriate safety management measures are taken (Article 25 of the Act), and is therefore required to check that personal data is being handled appropriately by "conducting regular audits", etc. (APPI Guidelines 3-4-4(3), p 55).

In addition, in the context of information security and cybersecurity, certain guidelines (referred to in **2.1 Data Security and the Cloud**) formulated and published by the regulatory authorities in specific business fields also require that business operators use cloud services to supervise cloud service providers, as a means of outsourcing management. If this supervision is insufficient, administrative guidance, pursuant to the relevant business laws, may be given to business operators using cloud services.

The content of compliance audits of cloud service providers carried out by business operators that use cloud services is fundamentally left to the discretion of the business operators, and there are various methods, such as: (i) sending a self-checklist to the cloud service provider and asking them to respond; or (ii) if a security audit of the cloud service provider is carried out by an external auditing firm or the like, requesting and checking the audit report. However, (i) could be insufficient to accurately gain a grasp of the risks, and (ii) is unusable if the cloud service provider does not agree to the external audit (and it is also impossible to require the provider to undergo the audit). Therefore, there are many difficulties in conducting compliance audits of cloud service providers.

Meanwhile, there are several certification systems, such as the ISMS Cloud Security Certification System, the Cloud Security Mark System, and the ISMAP System, which certify that cloud providers have appropriate security and organisational systems in place. In order to maintain these certifications, cloud service providers must undergo regular audits by certification organisations; therefore, confirming that these certifications are being maintained on an ongoing basis is a possible method by which cloud service users (business operators) could conduct compliance auditing of cloud service providers.