COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Japan
TMT

Contributor

Nagashima Ohno & Tsunematsu

Keiji Tonomura

Partner | keiji_tonomura@noandt.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Japan.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

JAPAN
TMT

1. What is the regulatory regime for technology?

In Japan, there is no single regulatory regime for technology in general. Rather, technology and related data are protected and regulated by various laws and regulations, including industry-specific regulations and standards set by the competent authority for technology used in each industry.

2. Are communications networks or services regulated?

Yes. Communications networks or services are regulated by the Telecommunication Business Act (the Telecom Act), the Wire Telecommunications Act, and the Radio Act. Broadcasting is separately regulated by the Broadcasting Act.

3. If so, what activities are covered and what licences or authorisations are required?

Telecommunications services (including businesses that provide telecommunications services) are regulated by the Telecom Act, which came into effect in 1985 when the telecommunications market of Japan was liberalised. The Wire Telecommunications Act and the Radio Act also regulate the establishment and operation of telecommunications facilities. Broadcasting is separately regulated by the Broadcasting Act.

Telecommunications services are defined as certain services that intermediate communications of third parties through the use of telecommunications facilities or that otherwise provide telecommunications facilities for the use of communications by third parties. Telecommunications facilities are broadly defined to include machines, equipment, wires and cables or other electrical facilities for the operation of telecommunications.

Under the Telecom Act, any person who intends to operate a telecommunications business must obtain registration from the Minister of Internal Affairs and Communications (MIC), except in cases where (i) it installs no telecommunications circuit facilities, (ii) it only installs small-scale telecommunications circuit facilities (i.e., relevant telecommunication facilities remain within certain local area), or (iii) it installs radio facilities of radio stations which separately require a license under the Radio Act. In these exceptional cases, such person must file a notification with the MIC (instead of obtaining registration from the MIC).

4. Is there any specific regulator for the provisions of communications-related services?

Telecommunication services are administered by the MIC.

5. Are they independent of the government control?

The MIC is a government regulatory body and as such is not independent of government control.

6. Are platform providers (social media, content sharing, information search engines) regulated?

On February 1, 2021, the Act on Improving Transparency and Fairness of Specified Digital Platforms came into force. According to the Act, the Minister of the Ministry of Economy, Trade and Industry (METI) will designate the specified digital platform operators (“Specified DPOs”) among digital platform operators that meet the thresholds of business size such as total sales, number of users and other elements specified for each business category. It seems that, for the time being, only large-scale online malls and app stores will be designated as Specified DPOs. Currently, only five digital platform operators are designated as the Specified DPOs: (i) Amazon Japan G.K. (Amazon. co. jp), Rakuten Group, Inc.

(Rakuten Ichiba) and Yahoo Japan Corporation (Yahoo! Shopping), as comprehensive online shopping malls selling goods; and (ii) Apple Inc. and iTunes KK (App Store) and Google LLC (Google Pay Store), as application stores. Specified DPOs are required to: (i) disclose certain information on terms and conditions of the transactions to users, (ii) establish and maintain appropriate procedures and systems in accordance with the guidelines that will be provided by the Minister of METI, and (iii) report the business outline, the status of (i) and (ii), the status of settlement of disputes as well as a self-evaluation thereof to the Minster of METI for every fiscal year. The Minister of METI will review and evaluate the reports and disclose the evaluation results. The Minister of METI has the authority to issue a warning notice (*kankoku*) and/or make a public announcement (*kouhyou*) as well as issue Orders of Action (*sochi-meirei*). Failure to comply with such Orders of Action or the above-mentioned reporting obligations is subject to criminal fines. Digital platform operators that meet the thresholds of business size, but are not designated as the Specified DPOs will also be required to notify certain matters regarding their digital platform businesses to the Minister of METI.

Also, the Act for the Protection of Consumers on Digital Platforms, which came into force on May 1, 2022, regulates digital platforms with online malls and auction sites, regardless of their sales amounts. In addition to requiring certain measures to protect consumers using such digital platforms, the Act requires disclosure of an overview of such measures and their implementation status.

Further, depending on the nature of their services and roles, platform provider might be subject to certain industry-specific laws and other regulations. For instance, social media platform providers might be regulated by the Act on the Protection of Personal Information (APPI) with respect to their handling of personal data and/or the Telecom Act as for the privacy of communications between users on their platform. Also, under the Private Lodging Business Act in 2017, platform providers are regulated as private lodging agents serving as brokers for private lodging services between guests and private lodging business operators (typically, landlords and lessees). Furthermore, on December 17, 2019, the Japan Fair Trade Commission released the “Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.” to ensure transparency and predictability for digital platform operators by clarifying the concepts of the regulation on abuse of a superior bargaining position under the Antimonopoly Act with respect to acquiring or using personal information, etc. between digital platform operators and consumers that provide the same.

7. If so, does the reach of the regulator extend outside your jurisdiction?

It depends on laws and regulations that are applicable to platform providers, but there are some laws and regulations containing a provision of extraterritorial application, which enables the regulator to enforce such laws and regulations against platform providers located outside of Japan (e.g., the Act on Improving Transparency and Fairness of Specified Digital Platforms, the Private Lodging Business Act, and the APPI), but generally speaking, enforcement actions via-a-vis such platform providers located outside of Japan have not been so active.

Notably, the Telecom Act was recently amended (which came into force as of April 1, 2021) to, among others, strengthen the effectiveness of enforcement measures vis-à-vis foreign telecommunication business operators domiciled in foreign. Such foreign operators are subject to the same obligations as those imposed on domestic operators under the Act (including the registration with the MIC or submission of a notification to the MIC) and also required to appoint their representative or agent in Japan.

8. Does a telecoms operator need to be domiciled in the country?

Under the Telecom Act, there are no regulations that require a telecommunications carrier (i.e., any person who has obtained registration or has filed a notification to operate a telecommunications business under the Telecom Act) to be domiciled in Japan.

9. Are there any restrictions on foreign ownership of telecoms operators?

Under the Act on Nippon Telegraph and Telephone Corporation, Etc., one-third or more of the total number of the issued shares of Nippon Telegraph and Telephone Corporation (NTT Corporation) must be held by the Japanese government, and the aggregate voting rights of shares in NTT Corporation held directly or indirectly by (i) any person who does not have Japanese nationality, (ii) any foreign government or its representative or (iii) any foreign juridical person or entity (subject to the calculation method of indirectly held voting rights under the Act) may not exceed one-third of the total voting rights of the issued shares of NTT Corporation. There are also certain restrictions on foreign ownership under the

Radio Act and the Broadcasting Act.

Furthermore, certain direct inward investments into Japan (e.g., acquisition of 10% or more of a listed company in Japan or any shares of an unlisted company in Japan) by foreign investors in the area of telecommunications business are subject to a prior filing requirement under the Foreign Exchange and Foreign Trade Act and could be subject to order of the Japanese government to change or stop the transaction (although such order has never been reported in the area of telecommunication business in the past).

10. Are there any regulations covering interconnection between operators?

Yes. Under Article 32 of the Telecom Act, all telecommunications carriers must accept a request from another telecommunications carrier to interconnect the facilities of the requesting carrier with the circuit facilities that the requested carrier installs, with certain exceptions (see question 11).

11. If so are these different for operators with market power?

Under Article 32 of the Telecom Act, all telecommunications carriers must accept a request from another telecommunications carrier to interconnect the facilities of the requesting carrier with the circuit facilities that the requested carrier installs, except where (i) the interconnection is likely to hinder telecommunications services from being smoothly provided, (ii) the interconnection is likely to unreasonably harm the interests of the requested carrier, or (iii) there are justifiable grounds specified by an Ordinance of the MIC.

In addition, there are specific regulations on telecommunications carriers who install basic and important telecommunications facilities as designated by the MIC. Such designated carriers are obligated to establish interconnection tariffs concerning the amount of money that a carrier will receive and the technical conditions required at the points of interconnection with other carriers' facilities. Such interconnection tariffs must be authorised by the MIC (in the case of fixed line facilities) or must be submitted to the MIC prior to implementation of the interconnection tariffs (in the case of mobile facilities).

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

The Telecom Act provides certain consumer protection regulations, which include:

i. review of tariffs by the MIC;
ii. obligation of the carrier to explain terms and conditions;
iii. obligation of the carrier to deliver certain explanatory documents;
iv. consumer's right to terminate the contract;
v. certain prohibited conducts of the carrier (e.g., intentional failure to disclose or misrepresentation of material information about the contract, or continuous solicitation to already rejected users); and
vi. obligations of the carrier to make proper guidance to sales intermediaries.

13. What legal protections are offered in relation to the creators of computer software?

Under Japanese law, computer software may be legally protected by patents and copyrights.

Under the Patent Act, a computer program, including any information that is to be processed by a computer and equivalent to a computer program, can be protected where the software program fulfils the requirements of an invention, which is defined as a highly advanced creation of technical ideas utilizing the laws of nature.

While patents protect the ideas of computer software, copyrights protect the expression of those ideas. Copyrights provide the copyright owners of certain works (including computer programming works) with certain exclusive rights, including the right to reproduce, distribute, transfer and create derivative works of the software. Registration is not required to secure copyrights or exercise copyrights against third parties, but registration is required to assert the transfer of copyrights against third parties, although conducting such registration is uncommon in practice.

14. Do you recognise specific intellectual property rights in respect of data/databases?

In Japan, there are no unique intellectual property rights that protect data itself; but certain kinds of data may be protected under patents, copyrights, or trade secrets under limited circumstances. For instance, data may be

protected by patents when data exist as a form of a computer program (see question 13) or by copyrights when copyrightable works are expressed in a data format.

Also, data may be protected as "trade secrets" or "data for limited provision" (Protected Data) under the Unfair Competition Prevention Act or by tort claim under the Civil Code. Under the Unfair Competition Prevention Act, injunctions can be issued and monetary damages can be awarded by a court in respect of data infringements. However, unlike trade secrets, criminal sanctions will not apply with respect to Protected Data.

While there are no special rights for databases, such as database sui generis rights recognised in the EU, a database that constitutes a creation in light of its selection or systematic construction of information contained therein may be protected under the Copyright Act. In addition, databases may, in certain circumstances, be protected under the Patent Act, under the Unfair Competition Prevention Act, or by tort claim under the Civil Code.

15. What key protections exist for personal data?

The Act on the Protection of Personal Information (the APPI) is a comprehensive, cross-sectorial framework for the protection of personal information, which regulates private businesses using personal information as well as use of personal information by the public sector. The APPI is implemented by cross-sectoral administrative guidelines prepared by the Personal Information Protection Commission (the PPC). With respect to certain sectors, such as medical, financial and telecommunications, sector-specific guidance and guidelines are published by the relevant governmental ministries jointly with the PPC given the highly sensitive nature of personal information handled in those sectors. Self-regulatory organisations and industry associations have also adopted their own policies or guidelines. In addition, the Act on Utilisation of Numbers to Identify a Specific Individual in Administrative Procedures provides special rules concerning the handling of "individual numbers", which are granted to each resident of Japan under the Individual Social Security and Tax Numbering System (known in Japan as the "My Number System"), and other specific personal information (i.e., personal information containing any "individual number").

The obligations of all business operators handling "personal information" include: (i) specifying and notifying the purposes for which the personal information is used and processing the personal information only to the extent necessary for achieving such specified purposes; (ii) not using deceptive or wrongful means in collecting personal information; and (iii) not using personal information in a way which might facilitate or induce illegal or wrongful actions.

In addition, business operators handling "personal data" (i.e., personal information constituting a personal information database) are subject to certain obligations, such as: (i) endeavouring to keep the personal data accurate and up to date to the extent necessary for the purposes of use; (ii) undertaking necessary and appropriate measures to safeguard personal data; (iii) conducting necessary and appropriate supervision over its employees and its service providers who process its personal data; (iv) reporting to the PPC and notifying a data subject with regard to data breaches; (v) not providing personal data to any third party without the prior consent of the relevant individual (subject to certain exemptions); (vi) preparing and keeping records of third-party transfers of personal data; and (vii) when acquiring personal data from a third party other than data subjects (subject to certain exceptions), verifying the name of the third party and how the third party acquired such personal data.

Business operators handling "retained personal data" (i.e., personal data that a business operator has the authority to disclose, correct, add content to or delete content from, discontinue the use of, erase, and discontinue its provision to a third party) are required, among other things, to: (i) make accessible to the relevant individual certain information regarding the retained personal data; and (ii) respond to a request of the relevant individual to, e.g., provide a copy of retained personal data to such individual, correcting, adding or deleting the retained personal data, or discontinuing the use of or erasing such retained personal data.

The APPI imposes stringent rules for "sensitive personal information", which includes race, beliefs, social status, medical history, criminal records and the fact of having been a victim of a crime, and disabilities.

The APPI provides for special rules for "anonymized personal data", which must meet certain requirements under the APPI. Business operators that created or retain such anonymized personal data are subject to certain obligations (e.g., disclosure of the creation of such anonymized personal data and prohibition of re-identification) but no consent of the data subject is required for the use or provision of such anonymized personal data.

Notably, the amended APPI, which came into force on April 1, 2022, introduced new regulations, which will

have a significant impact on businesses as it includes, inter alia: (i) new regulations on “Pseudonymized Information,” (ii) new regulations on third-party transfers of “Individual Related Information” (including cookie information) where it is anticipated that the recipient may identify an individual, even if the disclosing party cannot identify an individual, (iii) the addition of matters to be disclosed by business operators, (iv) enhancement of the rights of data subjects, (v) obligation to report to the PPC and notify a data subject with regard to data breaches, (vi) stricter regulations on cross-border transfers, (vii) broadened enforcement options on entities outside of Japan, and (viii) reinforcement of criminal penalties.

16. Are there restrictions on the transfer of personal data overseas?

Under the APPI, personal data may not be transferred to a third party located outside of Japan without the prior consent of the relevant individual unless:

i. the relevant third-party transferee is located in a foreign country that the PPC considers has the same level of protection of personal information as Japan (only the 31 member countries of the EEA are officially designated as such by the PPC based on the framework for the mutual and smooth transfer of personal data between Japan and the EU that was implemented on January 23, 2019);
ii. the relevant third-party transferee has established a system to continuously ensure its undertaking of the same level of protective measures as personal data users would be required under the APPI; or
iii. the transfer falls under an enumerated exception in the APPI.

Under the amended APPI, to obtain the consent of the relevant individual, the business operator would be obliged to, prior to the data transfer, provide the individual with information on the protection of personal information in the foreign country where the third party is located, as well as the measures implemented to protect personal information by the third party and certain other similar information. In addition, in the case of Item (ii) above, the business operator would be obliged to take necessary measures to ensure the continuous implementation of the protective measures by the third party and to provide the relevant individual with information on such necessary measures upon request.

17. What is the maximum fine that can be applied for breach of data protection laws?

Under the APPI, there is no administrative fine that can be applied for breach of the APPI, but criminal penalties may be imposed on business operators handling personal information under certain circumstances. The maximum criminal fine to be imposed on corporations is \100,000,000, which may be imposed in situations where business operators violate either the prohibition against illegal theft or provision of a personal information database or a PPC order.

18. What additional protections have been implemented, over and above the GDPR requirements?

As European Commission issued its adequacy decision on Japan, Japan is deemed to offer an adequate level of data protection from the GDPR perspective. However, since the regulatory framework and basic concepts under the APPI are different from those under the GDPR in many aspects, it is not easy to compare the APPI with the GDPR in terms of the protections implemented thereunder. Generally speaking, however, more protections are implemented under the GDPR than under the APPI with limited exceptions (e.g., while the anonymized data is not subject to the regulations under the GDPR, the anonymously processed data is still subject to the regulations under the APPI which are different from and less strict than those applicable to the personal data). It has been debated whether to implement additional protections and regulations by reference to those under the GDPR; however, the right to data portability and the right not to be subject to a decision based solely on automated processing (including profiling) were not introduced, while the obligations to report to the PPC and notify a data subject with regard to data breaches were added by the amended APPI.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

In Japan, there are no specific laws that directly prohibit, restrict or otherwise govern cloud-based services. Where the data being placed in the cloud is personal information/data, use of cloud-based services may be considered as constituting the provision of personal data to third-parties under the APPI, which requires the prior consent of the relevant individual (subject to certain exemptions depending on whether such third-parties are located in or outside of Japan) (see questions 15 and 16).

However, the guidelines published by the PPC provide that the use of cloud services to store personal data does not constitute the provision of personal data to cloud service providers under the APPI as long as it is ensured by contract or otherwise that the cloud service providers are properly restricted from accessing the personal data stored in the cloud.

Aside from the personal data protection regulations, provision or use of cloud-based services may be subject to other restrictions depending on the nature of the services or the stored data, including consumer protection regulations and sector-specific guidelines in medical and financial sectors. The Information Security Management Guidelines for the Use of Cloud Services (2013), published by the METI in March 2014, provides advice for the selection and implementation of appropriate controls from the ISO Q 27002 (code of practice) and guidance for optimal implementation in order to address risks associated with the use of cloud services. Also, the Information Security Measures Guidelines for the Provision of Cloud Services (3rd edition, 2021) published by the MIC in September 2021, provides advice for cloud service businesses to address risks associated with the provision of IoT or cloud services.

20. Are there specific requirements for the validity of an electronic signature?

There are no specific requirements for the validity of an electronic signature, except for certain limited types of agreements. As for a handwritten signature, if a document is signed or sealed by the principal or his or her agent, such document will be presumed to be authentically created under the Code of Civil Procedure. Likewise, in order for a digital record with an electronic signature by the principal to be presumed to be created authentically, such electronic signature must meet the requirements set forth under the Act on Electronic Signatures and Certification Business (the E-Signature Act). Partly because of such requirements for an electronic signature and the long-lasting custom of using seals (*hanko*) in Japan, electronic signatures had not been so commonly used in Japan until the COVID-19 pandemic; however, due to the COVID-19 pandemic, the use of electronic signatures has been getting popular rapidly. To clear some uncertainties on application of the E-Signature Act on cloud-based electronic signatures, the METI released Q&As in July and September 2000, in which they indicated that cloud-based electronic signatures, such as DocuSign, Adobe Sign, and Cloud Sign, could be considered electronic signatures under the E-Signature Act, as long as certain conditions were met.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

No transfer of employees, assets or third party contracts would occur automatically in the context of outsourcing IT services. A transfer will occur only if the parties agree to such a transfer. In the case that the parties agree to transfer a certain business (including employees, assets, third-party contracts and liabilities), and not merely an outsourcing of IT services, by way of a company split (*kaisha-bunkatsu*), however, employees who are primarily engaged in the transferred business but who will not be transferred, and employees who are not primarily engaged in the transferred business but who will be transferred, are entitled to certain opt-out rights concerning their non-transfer or transfer, respectively, under the Act on the Succession to Labor Contracts upon Company Split.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

In Japan, there is no clear rule on the liability for malfunctions of a software program that purports to be a form of A.I. Theoretically, such liability may be found based on (i) strict liability under the Product Liability Act, (ii) tort under the Civil Code, or (iii) breach of contract or defective product under the Civil Code. If such software program is incorporated into certain equipment or other product and such product is found to be defective, the manufacturer of such product may be liable under the Product Liability Act. If such malfunctions were foreseeable by a party (e.g., a manufacturer or user of the software program) and the negligence (or intent) of such party is established, such party may be liable for damages flowing from a causal relationship under a tort claim, but it would heavily depend on the nature of the A.I. and the malfunctions or other circumstances whether such malfunctions were foreseeable.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

The key laws imposing obligations on companies to maintain cybersecurity include the Basic Cybersecurity Act and the APPI. More generally, an internal control system required under the Companies Act and the Financial Instruments and Exchange Act may, but is not

necessarily required to, include the measures to maintain cybersecurity.

The Basic Cybersecurity Act provides that, in accordance with the basic principles set forth under the Act, cyberspace-related business entities (referring to those engaged in business regarding the maintenance of the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies, or those involved in business related to cybersecurity) and other business entities must make a voluntary and proactive effort to ensure cybersecurity in their businesses and to cooperate with the measures on cybersecurity taken by the national or local governments.

The APPI does not directly set forth obligations to maintain cybersecurity, but the APPI and sector-specific guidelines provide rules for information security concerning personal information. For instance, under the APPI, a business operator handling personal information is required to take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security of the personal data.

The Penal Code and the Unauthorised Computer Access Prohibition Act cover the criminality of hacking/DDOS attacks. Also, the acquisition of a trade secret or a specially designated secret through an unauthorised access or the like may be subject to criminal penalty under the Unfair Competition Prevention Act or the Specially Designated Secret Protection Act, respectively.

24. What technology development will create the most legal change in your jurisdiction?

While it is expected that Internet of Things (IoT), artificial intelligence (AI) and robotic process automation (RPA) will continue to cause substantial changes in the legal arena, blockchain or distributed ledger technologies have the potential to make a significant impact on various transactions (such as payment transactions and financial instruments) and will most likely create a new legal system (such as smart contracts, fungible or non-fungible token (NFT), IP rights management and property title registrations). Such “web 3” movement will entail substantial changes in laws and regulatory bodies.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

One of the greatest impediments to economic development and commerce is vertically segmented legal and regulatory systems. Although cross-sectoral, innovative businesses and services are expected to develop, the current legal and regulatory systems are still sector-oriented and rigid, which tends to create grey areas of law and inefficiency of compliance and regulations. The government initiated a study group to consider the possibility of reframing the legal and regulatory systems to address such issues. Also, the Digital Agency of Japan was established in September 2021, which will examine and implement digital and regulatory reform and comprehensively address cross-cutting administrative reform issues based on a set of “digital principles”.

26. Do you believe your legal system specifically encourages or hinders digital services?

While there exist certain issues in the legal system that could hinder digital services to some extent (see question 25), the Japanese government has adopted, and continues to consider, various measures to change the legal system to encourage digital services. For instance, the Regulatory Sandbox was introduced as one of the measures under the Act on Special Measures for Productivity Improvement for the purpose of allowing businesses to conduct demonstration tests and pilot projects quickly and collect data that may contribute to regulatory reforms. Furthermore, the Copyright Act was amended, effective January 1, 2019, to introduce more flexible exemptions whereby copyrighted works can be used without a license from copyright owners in order to enhance the development of digital/communication technologies such as machine learning for artificial intelligence (AI).

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

As mentioned above (see question 16), the current legal system can solve the legal issues associated with artificial intelligence (AI) to some extent, but there is no legislation that specifically deals with AI. Thus there remain many uncertainties related to the legal issues associated with AI (such as civil and criminal responsibilities concerning malfunctions of AI and protections of AI software and AI deliverables).

To address such uncertainties, in June 2018, METI published the “Contract Guidelines on Utilization of AI and Data”, which consists of two sections: Data and AI

(the METI Guidelines). The AI section explains a fundamental approach to be taken in relation to contracts that concern the development and utilization of AI-based software from the perspective of promoting the development and utilization of software using AI technology. The METI Guidelines also provide sample provisions for development contracts for AI-based software.

Contributors

Keiji Tonomura
Partner

keiji_tonomura@noandt.com