Chambers
Global Practice
Guides

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

Data Protection & Privacy 2022

Japan: Trends & Developments

Takashi Nakazaki, Kensuke Inoue,
Yuta Oishi and Shigenobu Namiki
Anderson Mori & Tomotsune

practiceguides.chambers.com

Trends and Developments

Contributed by:
Takashi Nakazaki, Kensuke Inoue, Yuta Oishi and Shigenobu Namiki
Anderson Mori & Tomotsune ***see p.8***

Trends

A notable trend in the Japanese data protection and privacy space in 2020 and 2021 has been the increasing enforcement activity of the Personal Information Protection Commission (PIPC). In addition to the incidents mentioned in the relevant sections of the Developments section of this article, the PIPC issued administrative guidance to a taxi company collecting facial recognition data for personalised advertising, on the grounds that such use was not adequately notified to the data subject upon acquisition of facial images. Although not a direct result of this incident, the PIPC established a panel of experts on facial recognition to consider rules specific to facial recognition data.

In addition to the PIPC, other regulatory authorities are also considering the introduction of further regulation to the use of personal data. For example, the Ministry of Internal Affairs and Communications is considering the introduction of an independent regulation which will require certain social networking services to disclose information on data storage locations, with the aim of revising and implementing the Telecommunications Business Act in 2022.

Developments

2020 amendments to the APPI

In 2020, the Japanese legislature introduced significant substantive amendments to the Act on the Protection of Personal Information (APPI). Drafting and adoption of enforcement rules and ordinances have continued throughout 2020 and 2021. These amendments ("2020 amendments") were made pursuant to the three-year revision schedule, which was adopted in 2017 and will come into effect from 1 April 2022. The background of the 2020 amendments and a brief outline of the main points are set out below.

Background

Since the comprehensive revision of the APPI in 2017, businesses of various sizes and in various industry sectors, including major information technology companies, have actively invested in many new and innovative uses of personal data. At the same time, media coverage and social awareness of data privacy issues have increased dramatically in Japan. The 2020 amendments seek to address various pressing issues concerning personal data that have arisen during the past three years.

Broadly speaking, the 2020 amendments either create new obligations on the use of personal data, or significantly strengthen the existing regulations. As a whole, the 2020 amendments aim to increase the level of protection of personal data on a par with other jurisdictions, while introducing some unique local aspects. This trend is likely to continue, if not accelerate further, for the foreseeable future.

Thus, all businesses handling the personal data of Japanese data subjects, whether located within Japan or abroad, are strongly advised to be well informed of the APPI and the 2020 amendments, and ensure compliance by reviewing their privacy policies, internal data handling manuals, data-outsourcing agreements, and current data-handling practices.

Introduction of mandatory reporting and notice of data breach

Before the 2020 amendments, the APPI only required businesses to "make an effort" to report a data breach to the PIPC. Similarly, notification to affected data subjects were merely "desirable" measures which were loosely related to the obligation to implement adequate security measures set forth in the APPI.

Under the 2020 amendments, businesses are required to file an initial report to the PIPC with details of the data breach incident within three to five days of their occurrence. The 2020 amendments also requires businesses to file a more detailed follow-up report within 30 to 60 days of the security incident.

The 2020 amendments requires businesses to report the following four types of data breach incidents:

- data breaches involving "special-care required personal information" (which is broadly "sensitive personal data");
- data breaches involving data which may cause financial harm to the data subject if misused;
- data breaches caused by malice or ill intent; and
- data breaches involving more than 1000 data subjects.

Businesses are required to file the data breach report via the PIPC website, which is only available in Japanese. It should be noted that in the context of a client and a service provider, the 2020 amendments impose the reporting obligations on both parties. However, if the service provider notifies the client of the data breach, the service provide is exempt (paragraph 1, Article 26).

Separate and independent from the reporting obligation to the PIPC, the 2020 amendments require businesses to notify the data subject of the details of the data breach incidents outlined above in a prompt manner. In contrast to the PIPC reporting obligations, the 2020 amendments do not set forth a strict timeline for the notification obligation. This is due to the fact that the appropriateness of notifying the data subject of the incident tends to be highly fact-specific.

Furthermore, the 2020 amendments do not require a particular method or mode for the notice. Of course, it would be prudent to consider notifying the data subject in a manner that is clear, and for which the evidence of timing can be properly recorded for proof of compliance (Article 10 of the Enforcement Regulations).

Although notification to the data subject is the general rule, the 2020 amendments do provide certain exceptions in cases where it is difficult to notify the data subjects themselves because their contact information is unknown, or alternative measures (such as publication on the corporate websites) may be taken instead (paragraph 2 of Article 26).

Under the 2020 amendments, failure to comply with violations of the PIPC reporting obligations or the obligation to notify data subjects do not automatically directly trigger formal penalties. Nonetheless, they are a clear violation of the APPI, and therefore are subject to administrative recommendations and orders from the PIPC (Article 145). Violations of orders may result in the public announcement of the violation, and ultimately, in penalties and fines (Article 173).

Expanding and strengthening the rights of data subjects

Before the 2020 amendments, the APPI granted rights to data subjects such as disclosure, correction, and deletion. However, the APPI limited

the scope to personal data that had been stored for more than six months, did not explicitly grant data subjects the right to request the suspension of the use of personal data, and the causes of action were mostly limited to violations of the APPI itself.

Under the 2020 amendments, the APPI has sought to expand and strengthen the rights of data subjects in various areas.

First, the 2020 amendments expand the scope of personal data that is subject to disclosure to personal data that is scheduled within six months (paragraph 4, Article 16).

Second, the APPI now allows data subjects to request businesses to suspend the use of personal data (Article 35). Data subjects may also request disclosure of the record of third-party transfers maintained by businesses (paragraph 5, Article 33). However, the 2020 amendments do add some flexibility by allowing business to determine the mode of disclosure of the personal data (paragraph 2, Article 33).

Furthermore, the 2020 amendments add the following as actionable causes.

- when the personal data is subject to "improper use" (as described above);
- when it is no longer necessary for the business to use the said personal data; and
- when rights and interests may be harmed by the data breach.

Introduction of information disclosure obligations related to cross-border data transfer

Before the 2020 amendments, the APPI required businesses to either obtain the consent of the data subject, or extend the level of data protection under the APPI through the execution of a data transfer agreement or other contractual documentation with the recipient for transfers of personal data to recipients located outside Japan (paragraph 1, Article 28). However, the APPI did not require businesses to provide information regarding the jurisdiction in which the data recipient was located, or the level of data protection of the jurisdiction in which the recipient was located. This aspect of the APPI became an area of focus and debate given rising awareness and concern over the issue of "national security interests" and personal data stored outside Japan.

Coinciding with this trend, in 2021, a major Japanese IT company was reported to have entrusted the personal data of Japanese data subjects to a service provider located outside of Japan, where the data security had been poorly arranged, and this personal data was accidentally made accessible beyond its intended scope. This incident drew wide-spread criticism, and demonstrated the need for an amendment to the existing APPI.

Under the 2020 amendments, businesses are required to provide data subjects with relevant information regarding the transfer of their personal data to recipients outside Japan. Some examples of the required items are the following (pursuant to paragraph 2 of the same Article and Article 17 of the Enforcement Regulations):

- the jurisdiction in which the recipient is located;
- an outline of the local data protection framework; and
- the data security measures employed by the recipient.

The timeframe in which the business will be required to provide this information will differ depending on how the business seeks to comply with cross-border data transfer regulation.

If the business seeks to comply with the cross-border data transfer regulation by obtaining the consent of the data subject, the relevant information must be provided by the time consent has been obtained. On the other hand, if the business seeks to comply with the data transfer regulation by means of executing contractual documents extending data protection under the APPI, the relevant information may be provided upon request from the data subject.

However, in the latter case, it is also necessary for businesses to periodically confirm the status of the handling of the personal data by the recipient, and to take necessary measures such as suspending the data transfer if maintenance of adequate levels of protection cannot be sustained due to changes in the local laws and regulations (paragraph 3, Article 18 of the Enforcement Regulations).

Expanding extraterritorial regulatory enforcement

Before the 2020 amendments, the PIPC could only issue administrative guidance, advice and recommendations in terms of enforcement to businesses located outside Japan.

After the 2020 amendments, the PIPC has the power to require reports and issue administrative orders to businesses located outside Japan (Article 166). Furthermore, the 2020 amendments introduced the provision of relevant information to foreign data protection enforcement authorities, in order to effectively enforce the APPI outside of Japan (Article 172).

Introduction of heavier penalties for non-compliance

Before the 2020 amendments, penalties for violation of PIPC orders were limited to up to six months in prison with forced labour, or JPY300,000.

Under the 2020 amendments, violation of PIPC orders is punishable with up to one year in prison with forced labour or JPY1 million. The maximum penalty for corporations has been dramatically increased from up to JPY300,000 to JPY100 million (Article 179). Although the 2020 amendments do not introduce an administrative monetary penalty system, this may be further considered in future amendments.

New prohibition on "improper use" (Article 19)

Before the 2020 amendments, the APPI did not contain specific regulations on businesses with regard to the purposes of the use of personal data, or the method employed in such use, insofar as the use of personal data did not exceed the purpose of use published or notified to the data subject.

In 2019, an online website named "The Bankrupts Map", began offering a form of personal-credit-information-providing service by collecting, compiling and republishing personal data of individuals who filed for bankruptcy from the official gazette. The wide dissemination of personal data involved in this endeavour, such as the address of the bankrupts layered on top of Google maps, attracted widespread attention, severe criticism and multiple privacy and defamation claims. On 29 July 2020, the PIPC found that the website violated the APPI by providing personal data to third parties without consent or any other legal exceptions, and issued its first ever formal administrative order to suspend any further publication of the personal data. This incident triggered a widespread call to introduce a substantive limit to the purpose of use for which businesses may use personal data.

Under the 2020 amendments, business are prohibited from using personal data in ways that may encourage or induce illegal or unjust behaviour. The PIPC has the power to issue an administrative recommendation or order (Article

145), which will lead to criminal punishment if the administrative order is violated (Article 173). "The Bankrupts Map" is listed as one of the examples of the "improper use" in the official guidelines scheduled to be issued with the 2020 amendments.

Introduction of "pseudonymously processed information"

Before the 2020 amendments, the APPI contained a form of anonymised personal data termed "anonymously processed information", which was exempt from certain aspects of the regulation. For example, transfer of anonymously processed information to a third party did not require the consent of the data subject. However, the formal requirements and the level of anonymisation required by the APPI to fall within the definition anonymously processed information was strict. As a result, many businesses hesitated to adopt anonymously processed information for use in their businesses.

Under the 2020 amendments, the APPI introduced a new category of information named "pseudonymously processed information" to promote the use of personal data in businesses. In essence, pseudonymously processed information is information that is processed to remove personal identifiers so that it cannot identify a living individual, unless it is combined with other identifying information (Article 2.5). In other words, if the personal data is stripped of unique personal identifiers such as names, it will likely become pseudonymously processed information.

Businesses may use pseudonymously processed information for use beyond the published purpose without obtaining the consent of the data subject. For example, medical data collected for the published purpose of treatment of patients, may be used for research purposes even if the latter had not been listed in the existing purpose of use published or notified to the data subject.

Nevertheless, in order to maintain adequate levels of protection, the APPI does require specific methods to be taken for preparing "pseudonymously processed information" (Article 31 of the Enforcement Regulations). Furthermore, "pseudonymously processed information" is only intended for internal use within the business.

Introduction of "personal related information"

Before the 2020 amendments, the text of the APPI was not clear on the regulatory scope regarding data which did not identify a data subject by the initial holder of the data, but which may become personally identifiable data once it has been transferred to a third party holding additional data. Thus, whether cookies, internet protocol addresses or browsing history were regulated by the APPI was left to interpretation.

In 2020, a major online job matching service for college graduates, was reported to have provided the data of college graduates to potential employers, in which the provided data was able to be used to identify a certain individual by the potential employers by combining the received data with their own data. As this matter concerned many large and well-known companies, and as the recruiting process of college graduates is a very significant issue in Japan, this incident highlighted the need for clear rules on this issue.

Under the 2020 amendments, the APPI introduces a new category of regulated data named "personal related information", which seeks to expand the scope of regulation to information which is related to living individuals, but does not fall within the statutory definition of "personal information".

The newly introduced personal related information is, in essence, information with which the recipient may identify a living individual by itself or in combination with other information. Personal related information includes cookies, internet protocol addresses and web browsing history.

Under the 2020 amendments, if the recipient of personal related information intends to identify a data subject with the received personal related information, the transferor of the personal related information must check whether the recipient has obtained the consent of the data subject before transferring the "Personal Related Information". For example, if a business intends to receive cookies or browser history from its corporate customers, and seeks to identify a certain individual with them, the business will be required to obtain the consent from the individual before the corporate customer can provide the cookies or browser history.

As this is practically difficult, the corporate customer is expected to obtain consent from the individual before providing cookies or other information.

2021 amendments to the APPI

In 2021, the Japanese legislature introduced amendments to the APPI with the aim to establish a unitary legal framework under the APPI ("2021 amendments"). As the scope and importance is limited in comparison to the 2020 amendments, this article will only briefly outline the main points.

First, the 2021 amendments integrated existing data protection laws and regulations targeting government entities into the APPI. Regulations on national administrative organs and independent administrative agencies, which had been separate laws, were integrated into the APPI. Local governments have also established common rules, although only individual ordinances have been enacted as to date. Research institutions, such as national and public hospitals and universities, were also subject to a different legal framework from the APPI, which was an obstacle for smooth data distribution between the private sector and these entities. As a result of the amendment, these entities, will be subject to the same rules as the private sector.

Separately, academic research institutions, which were uniformly exempt from the APPI, were not included in the scope of the adequacy recognition under the GDPR qualification. The 2021 amendments adjusted the statutory exemption with the aim of extending the effect of the adequacy recognition of the GDPR to academic institutions in Japan.

Contributed by: *Takashi Nakazaki, Kensuke Inoue, Yuta Oishi and Shigenobu Namiki,*
Anderson Mori & Tomotsune

Anderson Mori & Tomotsune (AMT) is a leading full-service law firm with over 500 licensed professionals. AMT has broad experience in intellectual property, life sciences and information technology. The practice boasts over 30 attorneys-at-law and patent and trade mark attorneys. It provides clients with professional and comprehensive advice and counsel services that suit their respective circumstances and objectives in relation to international and domestic disputes, transactions, regulatory filings and other matters. AMT is headquartered in Tokyo, with branch offices in Osaka and Nagoya. Outside Japan, the firm has offices in Beijing, Shanghai, Singapore, Ho Chi Minh City and Bangkok. It also has associated firms in Hong Kong, Jakarta and Singapore. Tokyo, Osaka and Nagoya are the key office locations for the IP, life sciences and IT practice.

AUTHORS

Takashi Nakazaki is a special counsel at Anderson Mori & Tomotsune, and has been engaged in an extensive range of TMT matters, including telecoms regulations, computers, software development, e-commerce, platform services, domain name disputes and digital forensics. His experience also includes legal advice in several fields of intellectual property and licensing, including traditional copyright, digital copyright, trade marks, open source, cross border licensing and biochemicals. Mr Nakazaki has also assisted many start-up clients with general corporate advice. He is the co-founder of the Japan chapter of the International Association of Privacy Professionals (IAPP).

Kensuke Inoue is a special counsel at Anderson Mori & Tomotsune with expertise in the areas of Japanese and international data protection law and information technology law. He also has broad experience in advising on intellectual property matters, M&A transactions, and general corporate law. He regularly handles both transactions and dispute resolution, including cross-border matters. He is a member of the International Association of Privacy Professionals (IAPP). He holds an LLM from the University of California, Berkeley School of Law (Certificate in Law and Technology), and is admitted to practise law both in Japan and California.

Yuta Oishi is a senior associate at Anderson Mori & Tomotsune with expertise in the areas of Japanese and international data protection law. He also has broad experience in advising on intellectual property matters, TMT matters and various corporate matters. He regularly handles both transactions and dispute resolution, including cross-border matters. He is a member of the International Association of Privacy Professionals (IAPP). He holds an LLM from the University of California, Berkeley School of Law (Certificate in Law and Technology), and is admitted to practise law both in Japan and New York State.

Shigenobu Namiki is a senior associate at Anderson Mori & Tomotsune with expertise in the areas of Japanese and international data protection law. He also has broad experience in advising on intellectual property matters, M&A transactions, and general corporate law. He regularly handles both transactions and dispute resolution, including cross-border matters. He is a member of the International Association of Privacy Professionals (IAPP). He holds an LLM from the University of California, Berkeley School of Law (Certificate in Law and Technology), and is admitted to practise both in Japan and New York State.

Anderson Mori & Tomotsune

Otemachi Park Building
1-1-1 Otemachi Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1086
Fax: +81 3 6775 2086
Email: takashi.nakazaki@amt-law.com
Web: www.amt-law.com

ANDERSON MŌRI & TOMOTSUNE