The Reform of the Japanese Act on Protection of Personal Information

From the Practitioner's Perspective

Ulrich Kirchhoff / Tobias Schiebe[*]

In times of constant collection and exchange of information, data have become one of the most important assets of companies. When it comes to the handling of data, the world is, however, widely divided on the applicable legal standards, reaching from almost no protection on one side to constitutional-like protection of personal data on the other.

In an effort to cope with rapid technological developments as well as to be recognized as a country with a safe data environment by foreign markets, such as the European Union, Japan has recently reformed its data protection law. The reformed Japanese Data Protection Act ("Act on Protec-

---

* Ulrich Kirchhoff, LL.M. (Boston University) and Dr. Tobias Schiebe, LL.M. (Victoria University of Wellington) are German attorneys at law registered as foreign law (German law) attorneys in Japan; they work for ARQIS Foreign Law Office, a Foreign Law Joint Enterprise with TMI Associates in Tokyo. The authors would like to thank Mr. Takashi Yoneyama, LL.M. (University of Southern California), Japanese attorney at law and partner at TMI Associates in Tokyo specializing in data protection and commercial law, for his contributions and advice with regard to this article.

tion of Personal Information"[1] – "APPI") became effective on 30 May 2017 and constitutes a major amendment ("Amendment") of the APPI subsequent to its initial enactment in 2005.

This article summarizes the main changes to the APPI and provides an overview of practical measures business operators in Japan need to consider in light of the amendments.

I. Scope of Application of the APPI

The only statutory law on the protection of personal information in Japan is the APPI. The APPI establishes rules concerning the handling of personal information, including the acquisition, use and transfer of such personal information. As to the interpretation of these rules, non-binding guidelines featuring suggestions on the proper interpretation of the APPI have been adopted by a number of ministries and agencies, e.g. the "Financial Services Agency of Japan Guidelines" ("FSA Guidelines"), the "Ministry of Economy, Trade and Industry of Japan Guidelines" ("METI Guidelines"), and the "Ministry of Health, Labor and Welfare Guidelines" ("MHLW Employment Guidelines").

1. Application to any Business Operator

With the Amendment, the scope of the APPI's application has been extended. In its pre-amended version, the APPI was not applicable to business operators that did not have more than 5,000 identifiable individuals in their database on at least one (1) day during the past six (6) months. For a large number of companies, in particular small and medium-sized subsidiaries of foreign companies, the APPI therefore did not apply. Absent other regulations on the handling of personal information, such businesses were in principle legally free to decide at their own discretion how they treated collected personal information.[2]

This practice has changed with the Amendment. Due to the extension of the scope, also business operators handling a smaller amount of data, so-called "Small-Size Database Operators", are now covered and need to comply with the requirements of the APPI. In principle, subsequent to the

1 *Kojin jōhō no hogo ni kansuru hōritsu* [Act on Protection of Personal Information] Act No. 57/2003.

2 Notably, the so-called "My Number Act" *(Gyō-sei tetsuzuki ni okeru tokutei no kojin o shikibetsu suru tame no bangō no riyō-tō ni kansuru hōritsu)* enacted in May 2013 assigns a specific governmental identification number to citizens residing in Japan and sets forth certain regulations on how to obtain and handle such "My Number" information.

Amendment the collection of personal information for even one individual for business purposes will be sufficient to result in application of the APPI.

Business operators handling personal information[3] are defined as any operator of a business, independent of its organizational form, including corporate entities and individuals, using a database consisting of personal information for business purposes. Any business operator employing at least one individual in Japan will normally collect personal information and will therefore become subject to the application of the APPI. Even for business operators not employing any personnel in Japan, the use of a customer database for business purposes can be the trigger for the application of the APPI. This result will not change if the customer base consists of mainly corporate entities because the information of the contact person at the corporate entity usually relates to a specific individual.

Entities such as state organs, local governments and incorporated administrative agencies as well as local independent administrative institutions are exempted from the application of the APPI.[4] For these organs separate specific regulations apply.

2. Scope of Information Covered

a) Personal Information

The APPI regulates the processing of "personal information" *(kojin jōhō),* or, if personal information is collected in a database, also so-called "personal data" *(kojin data)*. Personal information[5] is defined as any information that may identify a specific individual, such as name, date of birth, postal address, email address, telephone number, picture, finger print, iris pattern data or facial recognition data. Personal information is also any information which, together with other available data, will enable the identification of a specific individual even though the information used by itself does not constitute personal information.

With the Amendment it has been clarified that information including only numeric references, such as passport numbers, basic pension numbers, driver's license numbers or GPS location data sent by a vehicle, also constitutes personal information if such information may identify a specific individual, e.g. the registered owner of the vehicle in the latter case. This clarification is of high practical relevance, e.g. for the automobile industry, given Japan's aim to become a leader in the world in the area of connected cars and autonomous driving.

---

3 Art. 1 para. 3 Act on Protection of Personal Information.
4 Art. 2 para. 3 Act on Protection of Personal Information.
5 Art. 2 para. 1 Act on Protection of Personal Information.

b) Sensitive Personal Information

In addition to "personal information", the Amendment introduces "sensitive personal information".[6] This new category of information includes any information on a specific individual that may be the basis for discrimination or prejudice, such as information on race, religious beliefs, social status, criminal records, labor union membership, family status and medical history. This amendment is basically a concession to the European Data Protection Regulation in order to establish a personal information environment in Japan, thereby ensuring an equally safe protection of personal information. In particular personal medical information and information on race are of practical relevance, the latter given the Japanese history with Japanese persons having Chinese or Korean roots. Notably, names which indicate such a Chinese or Korean heritage or nationality are by themselves not considered as "sensitive personal information".

Due to the risk to specific individuals in relation to sensitive personal information, the processing of such information by a business operator is restricted and always requires the prior consent of the individual concerned. To this end, an "opt-out" procedure for transferring data to third parties (as described under II.2.c) is not permitted for sensitive personal information. Further, several guidelines (such as of the FSA) include additional provisions concerning the handling of sensitive personal information.

c) Anonymized Data

The amendment further introduces "de-identified information", also called "anonymized data", as a new information category. "Anonymized data" are defined[7] as personal information that no longer includes information that might identify a specific individual because the personal information has been made undiscoverable by technical means. The purpose is to ease the business use of information for statistical analysis (in the public media widely described as "Big Data") if no personal information is any longer included in the processed information.

As the original personal information has been excluded, the legal requirements for processing "anonymized data" have been reduced compared to personal information. For example, the transfer does not require the prior consent of the person whose personal information was excised from the information to be transferred, provided that the transfer is publically announced and it is clarified to the receiving third party that the data to be transferred have been anonymized.

---

6 Art. 2 para. 3 Act on Protection of Personal Information.

7 Art. 2 para. 9 Act on Protection of Personal Information.

3. Territorial Scope

While the APPI, as Japanese law, applies within the territory of Japan, an extraterritorial application[8] has also been regulated for the first time. If business operators who offer goods or services in Japan – but are located outside of Japan – process the personal information of specific individuals in Japan, the APPI will apply to them. This regulation mirrors the planned extraterritorial application under the European Data Protection Regulation that will become effective in May 2018. Although compliance with the APPI may not be directly enforced by the Japanese authorities against business operators located outside of Japan, the Japanese authorities plan to establish an information exchange with foreign authorities for enforcement purposes pursuant to the extraterritorial application of the APPI.

II. DATA PROCESSING (COLLECTION, USE AND TRANSFER)

1. Purpose of Use

Under the APPI, personal information may only be used within the scope of the "purpose of use"[9] (of the collected personal information), which needs to be disclosed directly to the person whose information is to be used (the "data subject") at the time the personal information is collected. The "purpose of use" is defined by the business operator collecting personal information.

While not legally mandatory, in practice it is advisable for business operators to declare the "purpose of use" in writing so as to establish evidence of its provision. The legitimate use of collected personal information mainly depends on the wording of the "purpose of use". Since there are generally no limitations and it is difficult to amend a "purpose of use" once it has been established, it is advisable to draft the "purpose of use" as broadly as possible. If business operators collect personal information through different channels, e.g. in shops, at events or online, it is advisable to use the same "purpose of use" to ensure that collected personal information can be used in the same way and independently of where the information was collected.

The "purpose of use" does not constitute the consent of the data subject, instead referring only to the notification of the planned use of the collected personal information. A general consent for the use of personal information is not required if the personal information is used only by the business

8 Art. 75 Act on Protection of Personal Information.

9 Art. 15 para. 1 Act on Protection of Personal Information.

operator and is not transferred to third parties, provided that the personal information does not constitute sensitive personal information.

The "purpose of use" does not need to be disclosed to a person whose information is to be used in the following (rare) cases:

- If certain rights (e.g. the rights to life, safety or property) of the data subject or of a third person would be infringed by notification;
- If the rights or legitimate interests of the business operator handling personal information would be infringed by notification (e.g. if a trade secret of the business operator would become public by notification of the purpose of use);
- If the execution of an operation set forth by law or by ordinance of a governmental institution would be harmed by notification;
- If the "purpose of use" is clear given the circumstances under which the personal information concerned is collected (e.g. where a business card has been provided at networking event for the purpose of establishing future contact for marketing purposes).

Pursuant to the Amendment, personal information which the business operator no longer needs for business use must be deleted without undue delay. While this limitation is subject to interpretation and it needs to be seen how courts will rule on the deletion obligation, it is advisable for business operators to record the reasoning behind keeping personal information in its database.

2. Transfer of Personal Information within Japan

Besides the collection of personal information, the transfer of personal information for the purpose of sharing, for example within the same group of businesses, is one of the most important aspects of personal information processing.

The transfer of any collected personal information to third parties by a business operator is generally feasible if (a) the individual whose personal information is to be used has consented to the transfer, or (b) the business operator has notified the individual in advance about the possibility of objecting to the transfer (opt-out), or (c) if some other exception is applicable. If personal information is to be transferred to a place outside Japan, the Amendment introduces restrictions on such a transfer for the first time.

a) Consent

While the consent to transfer personal information to a third party may be obtained orally, it is advisable for companies to obtain the consent *in writing,* provided that emails are in principle sufficient. The consent needs to

include the scope of the information to be transferred as well as the details of the business operator or service provider to whom the personal information is to be transferred, such as the name and address. In practice, the consent is typically combined together with the purpose of use and included in a privacy policy that is presented to the data subject at the time of the collection of the personal information. This privacy policy may be printed on an image card, contact request form or something similar that is to be signed by the data subject, or it may be shown in connection with an online registration form to be consented to by clicking a button/checking a box.

Prior consent is not required in the following cases, in which the entity to which personal information is being transferred is not considered a "third party":

– outsourced service providers (e.g. data processing companies, payroll/accounting offices or express couriers, provided that the service provider must be supervised);
– succeeding legal entities (e.g. by merger, spin-off or transfer of business, but not in the case of an isolated transfer of the database);
– joint users (e.g. joint use with the parent company, a subsidiary or other groups of companies within the scope of the purpose of use, provided that the person whose personal information is to be jointly used is informed about the joint use in advance, e.g. in the purpose of use in the privacy policy).

Since groups of companies, including the parent company, are typically separate legal entities, personal information collected in Japan may not be shared with a group of companies unless (i) such joint use within Japan has been disclosed to the data subject at the time of the collection of the personal information in the "purpose of use", or (ii) the express consent of the person whose information is to be collected has been obtained. It is therefore advisable to include a joint use in the "purpose of use" by stipulating the entities that will be joint users and the personal information that will be shared. The "purpose of use" may, in principle, only be amended for the future collection of information. With regard to already collected personal information the new "purpose of use" must be disclosed to the persons whose data was already collected, and their consent to the new "purpose of use" must be obtained. Joint use was a common approach for sharing personal information in Japan without obtaining the consent of the data subject. However, the joint use exception applies only to a joint use featuring entities in Japan. If the entity with which the personal information is to be shared is located outside of Japan, the general restrictions on the transfer of personal information outside of Japan apply (please refer to item II.3. below).

In addition, if sensitive personal information is to be transferred to a third party, the prior express consent of the data subject is always necessary.[10]

b) Opt-out

If prior consent has *not* been obtained, the business operator may, alternatively, provide the person whose personal information is to be transferred to a third party within Japan with the opportunity to object to the transfer (opt-out),[11] provided that the person whose information is to be used has been informed in advance or the following is applicable:

– the "purpose of use" generally specified "transfer of personal information to third parties";
– the person has the opportunity to determine the category of personal information to be transferred, e.g. names and addresses;
– the person has the opportunity to determine the method of transferring the personal information, e.g. online or by physical transfer;
– the person has the opportunity to suspend the transfer of personal information to third parties upon request.

The persons whose personal information is concerned may be notified by postal mail, email, etc., provided that the business operator must be able to prove that the information regarding the transfer has been disclosed. For this reason, it is advisable to use various information channels. In addition to the above-described direct notification, it is advisable to publicly announce an opt-out procedure on the website of the business operator. A public announcement *only* through the business operator's website is typically insufficient.

c) Exceptions

If the transfer of personal information within Japan is in the public interest, prior consent is not necessary. Such instances include where:

– personal information is necessary for the protection of life, safety or the property of a person;
– personal information is necessary to improve public hygiene or to promote the health of children;
– personal information is necessary to facilitate cooperation with governmental institutions;
– personal information is required by law or ordinance.

10 Art. 23 para. 1 Act on Protection of Personal Information.
11 Art. 23 para. 2 Act on Protection of Personal Information.

3. Transfer of Personal Data outside of Japan

The Amendment introduces for the first time restrictions on the transfer of data outside of Japan. While prior to the Amendment provisions existed only regarding data transfer to a third party in general, the Amendment stipulates limitations under which the transfer of personal information to a place outside of Japan is permitted.

Pursuant to the Amendment data transfer is permitted only when made (i) to overseas recipients in countries which have an "adequate" level of data protection equal to Japan, (ii) to overseas recipients with whom contractual agreements have been concluded to ensure compliance with data protection standards in Japan, or (iii) to overseas recipients in cases where the data subject whose personal information is to be transferred has given prior consent to such transfer.

A special committee, established with the Amendment, is to determine which countries are deemed to have a comparable level of data protection to Japan.[12] This so-called "Personal Information Protection Commission"[13] ("Commission") consists of experts from practice and academia and operates as a first point of contact for questions regarding data protection as well as supervisory authority. The Commission's responsibilities include defining the countries which will be considered as having an adequate level of data protection from the perspective of Japan. While originally a list of countries with a comparable level of protection was supposed to be prepared by the Commission by the time of the implementation of the Amendment, the Commission opted for entering into bilateral negotiations with other nations instead and will determine the countries with an adequate level of protection of personal information incrementally over time. As a wide uncertainty about the countries with an adequate level of protection exists, the only practical options at this point of time are either to obtain the data subject's consent to a transfer of personal information outside of Japan or to conclude a data transfer agreement obligating the recipient to compliance with the regulations under the APPI. Even though the European Union has one of the strictest data protection regimes in the world, the decision on whether or not the European Union is considered as having an adequate level of protection from the perspective of the APPI has not yet been made.[14]

---

12 Art. 24 Act on Protection of Personal Information.

13 Art. 59 Act on Protection of Personal Information.

14 A decision is expected at the earliest in the first quarter of 2018 and will also depend on the recognition of Japan as a country with a sufficient personal information protection scheme from the perspective of the European Union.

4. Rights of Data Subjects

Under the APPI, a data subject has the following rights:

- Disclosure[15] of stored personal information concerning:
  - Name of the business operator handling personal information;
  - Purpose of use;
  - Procedure for gaining access to, correction of and suspension of the personal information;
  - Contact information for complaints concerning the handling of personal information.
- Correction or deletion of incorrect personal information;
- Suspension of use or deletion of personal information if (i) personal information was used in excess of the purpose of use or transferred without prior consent or (ii) personal information was acquired by fraud or other unfair means.

Under the APPI, a data subject has been granted a statutory right to sue the business operator processing personal information so as to enforce his/her rights if the business operator fails to comply with the above-described requests within two (2) weeks.

III. LEGAL COMPLIANCE OBLIGATIONS OF THE BUSINESS OPERATOR

Since the Amendment not only extends the scope of application to all business operators processing personal information but also restricts the transfer of personal information to places outside Japan, it is important for business operators to take measures to comply with the changed legal environment.

1. General

From a practical perspective, the first steps for a business operator to confirm compliance with the APPI are as follows:

- Confirm whether personal information is processed in an internal data due diligence and whether or not a privacy policy on the processing has been enacted.
- If personal information is processed and a privacy policy has not yet been implemented, confirm if a privacy policy stipulating the "purpose of use" of the collected information has been established.

15 The business operator is allowed to charge for disclosure expenses.

– Confirm if structures, processes and responsibilities have been set up to allow for the timely handling of data subjects' requests regarding the protection of their rights and confirm if technical ("cyber-security") and physical safeguards are in place.

2. International Transfer

If the business operator transfers personal information from Japan to a place outside of Japan, the following measures must be taken:

– If possible, obtain the express consent of the data subject concerned because the countries with an adequate level of data protection similar to Japan have not yet been determined;
– Alternatively, if obtaining consent of the data subject is practically difficult, conclude a contractual agreement with the recipient to ensure compliance with Japanese data protection standards.

3. Outsourcing

Business operators may outsource the handling of personal information at their sole discretion. External service providers – such as payroll service providers for employees and data administration service providers – who process personal information on behalf of the business operator and within the scope of the "purpose of use" for which the personal information has been collected do not constitute "third parties"; this allows for a transfer of collected personal information to the service provider if the service provider is located in Japan, as otherwise the restrictions on transfer to a place outside of Japan would apply.

If the handling of personal information has been outsourced to external service providers, the handling of personal information by the service provider needs to be supervised because the business operator remains liable for the acts of the service provider as far as the processing of personal information is concerned. In addition to the careful selection and monitoring of the external service provider, it is therefore advisable to conclude a written service agreement, including at least:

– a sufficient confidentiality obligation, possibly including a contractual penalty in the event of a breach by the service provider;
– a limitation of the use of the personal information to the purpose for which the information has been obtained;
– a limit on the number of employees having access to the personal information;
– an obligation to return or delete the personal information after the end of the contractual relationship;

– a right of the business operator to supervise and audit the service provider with regard to the processing of personal information;
– a prohibition against the sub-contracting or sub-transferring of personal information; and
– an indemnification obligation of the service provider in the event of a leakage of personal and/or other information.

Even as regards other service providers that do not handle personal information but may obtain access thereto, such as office cleaning service companies, it is advisable to conclude confidentiality agreements and to ensure that physically stored personal information, such as employee information, is locked and not visible in the office.

IV. Legal Consequences of Data Breaches

1. Administrative Action

The APPI is an essential part of the Japanese public law regime and constitutes the basis for public enforcement and compliance with the Japanese data protection standards. Unlike the European approach, the Japanese supervision authority[16] rarely immediately issues administrative orders, following instead an escalation and – as typical in Japan – soft-landing approach. Prior to issuing an official administration order, the supervision authority usually directly contacts the business operator if it becomes aware of a violation and informally requests that the operator immediately rectify the violation. The authority monitors the compliance of the business operator with the informal request, and only if the business operator does not meet this obligation will administrative orders be issued in the following sequence:

– Administrative order to submit a report *(hōkoku);*
– Administrative advice *(shidō* and *jogen);*
– Administrative recommendation *(kankoku);*
– Administrative order *(meirei).*

2. Direct Action by the Data Subject

If personal information is leaked due to negligent or intentional misconduct of the business operator, including but not limited to a violation of the APPI, the business operator may also be subject to damage compensation claims raised by the data subject in a tort action under the Japanese Civil

16 Personal Information Protection Commission

Code.[17] While there are no court precedents under the Amendment yet and only a few precedents based on tort exist, the available court decisions indicate a rather small amount of damages being granted to data subjects for a business operator's violation of the APPI, these ranging from approximately JPY 500 to JPY 35,000.[18] The economic impact on the business operator may nevertheless be severe as typically a high number of individuals are concerned in the event of a data breach violating the APPI. In the most prominent case of a data breach in Japan, known as the "Benesse Case",[19] approximately 48.6 million data subjects were involved and thousands of compensation claims have been filed. While the matter was settled as regards several data subjects in return for a payment of only JPY 500, some claimants have asked for significantly higher amounts and their cases have not yet been settled.

3. Penalties

In the event of the violation of an authority's administrative order to correct the business operator's management of personal information, penal sanctions, including monetary fines of up to JPY 500,000 or imprisonment of up to one (1) year, may be imposed. Yet due to the above described escalation and soft-landing approach, penal sanctions are rarely imposed. The greatest risk of a business operator in Japan in the event of a violation of the APPI and other laws remains the potential loss of reputation if the public becomes aware of a data leakage or a violation of the APPI.

SUMMARY

The reformed Japanese Data Protection Act ("Act on Protection of Personal Information" – "APPI") has come into effect on 30 May 2017 and sets new conditions for handling data in order to align with international practices and new technologies. This article summarizes the main changes to the APPI and shall provide an overview of practical measures business operators in Japan need to consider in light of the amendments. This concerns the scope of application of the APPI, data processing (in particular the transfer of personal

17 *Minpō* [Japanese Civil Code] Art. 709.

18 Ōsaka High Court, 25 December 2011, Hanrei Chihō Jichi 256, 11; Tōkyō High Court, 28 August 2007, Hanrei Taimuzu 1264, 299; Ōsaka District Court, 19 May 2006, Hanrei Jihō 1984, 122.

19 A leak of personal information occurred at Benesse Corporation, Japan's largest provider of foreign language education for children. The leak of personal information was apparently caused by a sub-contractor who had been employed to manage Benesse's customer database.

data to recipients outside of Japan), legal compliance obligations as well as legal consequences of data breaches.

ZUSAMMENFASSUNG

Das reformierte japanische Datenschutzgesetz, welches am 30. Mai 2017 in Kraft getreten ist, stellt neue Vorgaben für den Umgang mit Daten auf, um dem internationalen Datentransfer und neuen Technologien gerecht zu werden. Der vorliegende Artikel fasst die wichtigsten Änderungen zusammen und soll einen Überblick über die vor dem Hintergrund der Änderung des Datenschutzgesetzes zu ergreifenden Maßnahmen geben. Betroffen von der Gesetzesänderung sind insbesondere der Anwendungsbereich des Datenschutzgesetzes, das Verarbeiten von Daten (im Speziellen der Transfer von persönlichen Daten zu Empfängern außerhalb Japans) im Zusammenhang mit den nach dem Datenschutzgesetz bestehenden Compliance-Pflichten und die rechtlichen Konsequenzen im Falle einer Datenschutzverletzung.