Japan Newsletter
September 2016

ARQIS FOREIGN LAW OFFICE

Dusseldorf
Munich
Tokyo

Data Protection in Japan

In times of constant information exchange, data have become one of the most important company assets. When it comes to the handling of data, the world is, however, widely divided on the applicable legal standards, reaching from almost unrestricted use to the constitutional protection of data.

This newsletter provides a general overview of the presently applicable Japanese data protection regulations and describes the measures to be taken by companies when handling data in Japan.

1. Legal Framework

The only statutory law on data protection in Japan is the Act on Protection of Personal Information ("APPI") that became effective in 2005. The APPI establishes rules for the handling of "personal information", including the acquisition, use and transfer of such personal information.

At present, the regulations of the APPI only apply to business operators in Japan having in its database on at least one day, within a time period of the past 6 months, information allowing to identify an individual, such as name, postal address, email address, telephone number, picture in certain cases, etc. ("personal information"), of more than 5,000 persons. Presently, no distinction between general personal information and sensitive personal information, as it is known in Germany, exists in Japan.

Considering the importance of data handling, a reform of the APPI has been resolved by parliament in September 2015, the main body of which will become effective by September 2017. One of the major planned amendments of the APPI is the extension of the scope of application to all business operators handling data, regardless of the number of personal information in the business operator's data base.

While not legally binding, for certain industries and areas guidelines established by the competent ministries include suggestions for interpreting the APPI, 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).

2. General Legal Requirements for the Use of Personal Information

Under the APPI, personal information may only be used within the scope of the so-called "purpose of use" (of the collected personal information) which needs to be notified directly to the person whose information shall be used at the time the personal information is collected. The "purpose of use" is defined by the business operator collecting the personal information.

While not mandatory, it is recommendable to declare the "purpose of use" in writing to create evidence of its provision. The legitimate use of personal information collected mainly depends on the wording of the "purpose of use". Since there are generally no limitations and due to the process to amend a once established "purpose of use", it is recommendable to draft the "purpose of use" as broad as possible.

Contact:
ARQIS Foreign Law Office
Foreign Law Joint Enterprise with
TMI Associates
Roppongi Hills Mori Tower, 23F
6-10-1 Roppongi
Minato-ku, Tokyo 106-6123
Phone: +81 (3) 6438-2770
Fax: +81 (3) 6438-2777
Email: tokyo@arqis.com
http://www.arqis.com
twitter.com/ARQISTokyo

If companies collect personal information through different channels, e.g. in shops, at events, online, etc., it is recommendable to use the same "purpose of use" to ensure that collected personal information can be used in the same way and independently from where the information was collected.

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

- If certain rights (e.g. life, safety, property, etc.) of the person whose information shall be used or of a third person would be infringed by the notification;
- If the rights or legitimate interests of the business operator handling personal information would be infringed by the notification (e.g. if a trade secret of the business operator becomes public by the notification of the purpose of use);
- If the execution of an operation set forth by law or ordinance of a governmental institution would be harmed by the notification;
- If the "purpose of use" is obvious given the circumstances under which the personal information concerned is collected.

3. Transfer of Personal Information to Third Parties

The transfer of collected personal information to third parties by the business operator is generally feasible, if (a) the individual whose personal information shall be used has consented to the transfer, or (b) the business operator has notified the individual in advance about the possibility to object the transfer, etc. (opt-out), or (c) an exception to the afore described applies.

(a) Consent

While the consent to transfer personal information to a third party may be obtained orally, it is recommendable to obtain the consent in writing (electronic means such as 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 which the personal information shall be transferred. 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 holder at the time of the collection of data. This privacy policy may be printed on an image card, contact request form, etc. to be signed by the data holder, or shown at an online registration form to be consented to by clicking a button.

A prior consent is not required in the following cases in which the entity to which personal information shall be transferred is not considered a "third party":

- outsourced service providers (e.g. data processing companies 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 case of an isolated transfer of the database);
- joint users (e.g. use with the parent company, a subsidiary or other group companies within the scope of the purpose of use, provided that the person whose personal information shall be jointly used is informed about the joint use in advance, e.g. in the privacy policy).

Since group companies, including the parent company, are typically separate legal entities, personal information collected in Japan may not be shared with group companies, unless (i) such joint use has been notified at the time of the collection of the personal information with the "purpose of use", or (ii) the express consent of the person whose information shall be collected has been obtained. We therefore recommend confirming the "purpose of use" and, if necessary, amending it.

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 informed to the persons whose data have already been collected and their consent for the new "purpose of use" be obtained.

Please note that under the reformed APPI a category of special sensitive personal information will be introduced, such as information related to race, religious beliefs, social status, criminal records, and medical history or any other information that may lead to a discrimination or prejudice, which may only be transferred upon prior express consent of the individual whose information is concerned.

(b) Opt-out

If a prior consent has not been obtained, the business operator may, alternatively, provide the person whose personal information shall be transferred to a third party the opportunity to object the transfer (opt-out), provided that the person, whose information shall be used, has been informed in advance or has the opportunity to access the following information:

- the "purpose of use" generally specified "transfer of personal information to third parties";
- the category of personal information to be transferred, e.g. names, addresses, etc.;
- the method of transferring the personal information, e.g. by online or physical transfer, etc.;
- suspension of the transfer of personal information to third parties upon request.

The person 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 of the transfer has been notified. For this reason, it is recommendable to use various information channels. In addition to the afore described direct notification, it is recommendable 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 not sufficient.

(c) Exceptions

If the transfer of personal information is in the public interest, a prior consent is not necessary. Those cases include:

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

4. New Special Requirements for the Transfer of Personal Data outside Japan

Under the presently applicable APPI, there are no specific rules for the transfer of personal information outside Japan, except for the general requirements for the transfer to a third party as described above.

However, the reformed APPI will include, for the first time, limitations under which a transfer of personal information to a recipient outside Japan is permitted. The transfer of personal information to a place outside Japan is planned to be only permitted (i) to overseas recipients in countries which have a comparable level of data protection like Japan, (ii) to overseas recipients complying with data protection standards in Japan, for example by contractual agreement to the Japanese standards, or (iii) to overseas recipients if the concerned individual has expressly consented to the transfer.

Which countries are deemed to have a level of data protection comparable to Japan shall be determined by a special committee of experts. While this committee has already been established, the list of countries is not yet available.

If personal information is transferred to countries outside Japan, monitoring of the planned amendments of the APPI will be necessary as, depending on the country, the consent of the person whose information shall be transferred or contractual agreements to secure the compliance of the recipient with data protection standards in Japan may be required.

With regard to transfer of personal information to Germany, storing personal information of Japanese customers in Germany may result in the application of the German data protection laws, resulting in restrictions to the re-transfer to Japan.

5. Legal Consequences of Abuse or Mishandling of Personal Information

In the case of a violation of an authority's administrative order to correct the business operator's handling of personal information, penal sanctions, including monetary fines of up to JPY 300,000 or imprisonment of up to 6 months, may be imposed. If personal information is leaked due to negligent or intentional misconduct of the business operator, the business operator may also be subject to damage compensation claims by the person whose information was leaked, and/or administrative countermeasures by the authorities. In addition, the reputation of the business operator may be affected if the public becomes aware of a data leakage which is typically one of the greatest risks for business operators in Japan.

6. Out-Sourcing of Services

Business operators may outsource the handling of personal information at their sole discretion. External service providers, such as payroll service providers for employees, data administration service providers, etc., handling data 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, allowing for a transfer of collected personal information to the service provider.

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 handling of personal information is concerned. In addition to the careful selection of the external service provider, it is therefore recommendable to conclude a written service agreement, including at least:

- a sufficient confidentiality obligation, possibly with a contractual penalty in case of a breach by the service provider;
- a limitation of the use of the information to the purpose for which the information has been obtained;
- a limit of the number of employees having access to the information;
- an obligation to return or delete the 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 handling of personal information;
- a prohibition to sub-contract or sub-transfer personal information; and
- an indemnification obligation of the service provider in the event of a data leakage.

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

Our Offices:

Tokyo Office

ARQIS Foreign Law Office
Foreign Law Joint Enterprise with
TMI Associates
Roppongi Hills Mori Tower, 23rd floor
6-10-1 Roppongi, Minato-ku, Tokyo
106-6123 Japan
Phone: +81 (3) 6438-2770
Fax: +81 (3) 6438-2777
tokyo@arqis.com

Düsseldorf Office

ARQIS Rechtsanwälte
Hammer Str. 19
40219 Düsseldorf
Germany
Phone: +49 (211) 13069-000
Fax: +49 (211) 13069-099
duesseldorf@arqis.com

Munich Office

ARQIS Rechtsanwälte
Prinzregentenplatz 7
81675 Munich
Germany
Phone: +49 (89) 309055-600
Fax: +49 (89) 309055-699
munich@arqis.com