DATA PROTECTION LAWS OF THE WORLD

Japan

DLA PIPER

JAPAN

Last modified 1 January 2023

LAW

The Act on the Protection of Personal Information ("**APPI**") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("**PPC**"), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted in 2003 but was amended and the amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI ("**Amended APPI**"). The Amended APPI will came into force on April 1, 2022. Also, there was a separate data protection law for public sector. However, the data protection law for public sector was integrated into the APPI and became effective on April 1, 2022 (the data protection law for local governments will be effective after April 1, 2023).

DEFINITIONS

Definition of Personal Information

Personal Information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information. According to the guidelines issued by the PPC, "easy reference to other information" means that a business operator can easily reference other information by a method taken in the ordinary course of business. If a business operator needs to make an inquiry of another business operator to obtain the "other information" and it is difficult for the business operator to do so, such a situation would not be considered an "easy reference to other information".

Personal Information includes any "Personal Identifier Code". A Personal Identifier Code refers to certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual. Typical examples of such code would be passport numbers or driver's license numbers.

Definition of Sensitive Personal Information

Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for third party transfer for sensitive information-prior consent is basically required from the data subject to transfer the sensitive information to a third party.

Definition of Anonymously Processed Information

"Anonymously Processed Information" refers to any information about individuals from which all personal information (i.e. the

information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restored by taking appropriate measures specified in the enforcement rules and the relevant PPC guidelines. As noted above, Personal Information includes personal identifier codes, so these must also be removed before information is considered anonymized.

If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use notified to the data subjects or disclosed to third parties without requiring the consent of the data subjects. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of Personal Information. Additionally, before disclosing the Anonymously Processed Information to a third party, a business operator must publicly state (likely in its privacy policy) the items of information (for example, gender, birth year and purchase history) included among the Anonymously Processed Information, and the means by which it shares the Anonymously Processed Information.

Definition of Pseudonymously Processed Information

Given the high hurdle of utilizing Anonymously Processed Information, such information has been less utilized than originally expected. The Amended APPI introduces the concept of "Pseudonymously Processed Information", which is the information that is processed so that such information is (i) not able to be used to identify a specific individual; but (ii) is able to be de-crypted by referencing other information. For example, Pseudonymously Processed Information is information in which names, addresses, and other similar such information are replaced with a random string of characters. Unlike normal Personal Information, a business operator can change the utilization purpose of Pseudonymously Processed Information at its own discretion (i.e. a business operator does not need to obtain consents from data subjects to change the utilization purpose). It is expected that business operators may utilize Pseudonymously Processed Information for internal data analytics purposes.

Definition of Personally Referable Information

The Amended APPI defines information which is related to personal matters, but that does not fall under the definition of Personal Information as "Personally Referable Information". The definition of Personally Referable Information is quite vague, but based on the guidelines issued by the PPC, it includes, among other things, a web browsing history collected through the terminal identifier such as cookie information, a person's age, gender or family makeup that are linked to his / her email address, a person's purchase history of goods and / or services, a person's location data, or a person's area of interest. The handling of Personally Referable Information is not regulated as Personal Information, but prior consent from data subjects would be required to transfer Personally Referable Information in certain circumstances as discussed below.

NATIONAL DATA PROTECTION AUTHORITY

The PPC has been tasked with providing many of the details necessary to interpret and enforce the APPI. The PPC issues guidelines for general rules for handling Personal Information, offshore transfer, confirmation and record requirements upon provision of Personal Information to third parties and creation and handling Anonymously or Pseudonymously Processed Information. The PPC is neutral and independent, and it has the power to enforce the APPI. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines and criminal penalties.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower
32nd Floor
3-2-1 Kasumigaseki
Chiyoda-ku Tokyo 100-0013
Japan

Tel: +81-(0)3-6457-9680

www.ppc.go.jp

REGISTRATION

Japan does not have a central registration system.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific directors or employees should be assigned to control Personal Information (e.g. Chief Privacy Officer).

COLLECTION & PROCESSING

Specifying the Purpose of Use

When handling Personal Information, a business operator must specify to the fullest extent possible the purpose of use of the Personal Information ("Purpose of Use"). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling Personal Information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the data subjects when Personal Information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When Personal Information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognizable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must 'publicly announce or 'expressly show the Purpose of Use in a reasonable and appropriate way. According to the guidelines issued by the PPC, the appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage so that the data subject can easily find the Purpose of Use before submitting the Personal Information.

TRANSFER

Disclosing / Sharing Personal Information

Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the Personal Information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger / business transfer or entrusting the handling of Personal Information to third party service providers.

Even disclosing the Personal Information within group companies is considered disclosing the Personal Information to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose Personal Information to third parties, unless individuals opt out of allowing the business operator to do so. The Amended APPI stipulates that Personal Information that has been transferred from others through the opt out measure or that has obtained by illegal manners, and Sensitive Personal Information cannot be transferred through the opt out measure. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out.

- the name, address and representative person of the business operator;
- the fact that the purpose of use includes the provision of such information to third parties;
- the nature of the Personal Information being provided to third parties;
- the method by which Personal Information has been obtained;

- the method by which Personal Information will be provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject;
- the method for an individual to submit an opt out request to the business operator;
- the method to update Personal Information which has been provided to their parties; and
- the schedule date of provision of Personal Information.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Information. Generally, written consent should be obtained whenever possible. When obtaining consents, it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Information will be disclosed, the contents of the Personal Information and how the third party will use the provided Personal Information.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Information from the data subject:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject;
- receipt of a consent email from data subjects;
- the data subject's check of the confirmation box concerning the consent;
- the data subject's click of a button on the website concerning the consent; and
- the data subject's audio input, or touch of a touch panel concerning the consents.

If Personal Information is to be used jointly, the business operator could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Information will be used jointly;
- the item of the Personal Information to be disclosed;
- the scope of the joint users;
- the purpose for which the Personal Information will be used by them; and
- the name, address and representative person of the business operator responsible for the management of the Personal Information.

Transfer of Personally Referable Information

The Amended APPI stipulates that prior consent from data subjects is necessary if Personally Referable Information is transferred to a third party and the receiving party can identify a specific individual by way of referencing such Personally Referable Information with any information that the receiving party already has in its possession. In general, such consents are to be obtained by the receiving party and therefore, the transferor needs to, in advance to transferring Personally Referable Information to a third party, confirm if the receiving party has already obtained consents. That being said, it is possible that the transferor collects data subjects' consents on behalf of the receiving party.

Cross-border Transfer

Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the enforcement rules of the APPI or the third party receiving Personal Information has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, UK and EU countries are specified as white-listed countries based on the adequacy decision on January 23, 2019.

According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Information are at least equal with the requirements for protection of Personal Information under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Information.

According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. With regard to data subject's consents to transfer their Personal Information to foreign countries, the Amended APPI stipulates that the business operator shall provide the following information to the data subject when obtaining consents therefrom: (i) name of the country where the receiving party resides, (ii) data protection law system in the country and (iii) the data protection measures that the receiving party implements. In addition, the business operator needs to take necessary measures to ensure that the receiving party of such Personal Information continuously takes proper measures to process the Personal Information in a manners equivalent to the requirements of the APPI.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Information. The APPI does not set forth specific steps that must be taken. The PPC guidelines suggest recommended steps that business operators should take to ensure that Personal Information is secure. These necessary and appropriate measures generally include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures".

Guidelines often contain several specific steps or examples that entities subject to the guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to Personal Information, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

Under the Amended APPI, business operators shall report data breach incidents to the PPC and affected data subjects if the data breach incidents could harm the rights and interests of individuals. The PPC set the concrete threshold for reporting obligations and in the case of any of the below (i)-(iv), the business operator needs to report it to the PPC and notify the affected individuals: (i) Sensitive Personal Information is or likely to have been leaked, (ii) Personal Information that would cause financial damage by unauthorized use is or likely to have been leaked, (iii) data leakage by wrongful purpose is or likely to have been occurred, and (iv) data leakage incident that involves more than 1,000 data subjects is or likely to have been occurred.

In addition, the PPC guidelines suggest that business operators (i) make necessary investigations and take any necessary preventive measures, and / or (ii) make public the nature of the breach and steps taken to rectify the problem, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Information which has been disclosed was immediately collected before being seen by any third party or not actually disclosed, (such as the case where the company has encrypted the data or otherwise secured the data in such a way that it has become useless to third parties being in possession of such data), the notice to the PPC or any other relevant authority is not necessary.

ENFORCEMENT

If the PPC finds any violation or potential violation of the APPI, the PPC may request the business operator to submit a report, conduct on-site inspection and request or order the business operator to take remedial actions. If a business operator does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 500,000.

If a business operator does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 1,000,000. If the party that fails to follow such order is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

An unauthorized disclosure of Personal Information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000. If the party that discloses Personal Information is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ("ASCT") and the Act on the Regulation of Transmission of Specified Electronic Mail ("Anti-Spam Act") regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (i.e. an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email or fax advertisements for 3 years for email advertisements and 1 year for fax advertisements after the last transmission date of an email or fax advertisement to the consumer.

If a seller has breached any of these obligations regarding email advertisements, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (e.g. an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient;
- for-profit entities or individuals engaged in business sending any email to advertise their own or another's business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (e.g. there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act;
- an email is required to include a sender's email address or a URL so that recipients can send opt-out notices to the sender; and
- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 1,000,000 if an officer or an employee of the entity commits the violation mentioned above.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies, but it is generally considered that cookies fall under the definition of the Personally Referable Information and thus the transfer of such data would be regulated by the APPI in certain circumstances. In addition, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (e.g. member registration) and it is utilized (e.g. for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the **APPI**.

KEY CONTACTS

Tomomi Fujikouge
Of Counsel
T +81 3 4550 2817
tomomi.fujikouge@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.