Atsumi & Sakai

A GUIDE TO DATA PROTECTION IN JAPAN

ATSUMI & SAKAI
TOKYO | LONDON | FRANKFURT
www.aplaw.jp/en

September 2020

September 2020

Wide-ranging amendments to Japan's Act on Protection of Personal Information ('**APPI**') were passed by the Diet on 3rd September 2015 and came fully into force on 30th May 2017. The amendments had a significant impact on companies holding personal information in Japan and have expanded the extraterritorial application of the APPI.

On 5th June 2020 Japan's Diet passed a bill to revise the APPI ('**2020 Amendments'**); the bill was promulgated on 12th June 2020 and will come into force within two years of promulgation, the exact date to be fixed by Cabinet Order. The main revisions are noted in italics below. [1]

This note provides a general guide to the amended APPI and the material 2020 Amendments.

CONTENTS

[1] The act (in Japanese) is available here with the official English translation here.

1. KEY DEFINITIONS & BASIC CONCEPTS

Anonymised Information: In summary, information regarding an individual which has been processed by deleting any information (or replacing it with information which does not enable reversion to the original information) so that it cannot be used to identify the individual.

Anonymised Information Controller: (The verbatim English translation is "a business operator handling anonymised information") means a PIC using for its business a database (whether electronic or not) that allows easy retrieval of specific Anonymised Information contained in it.

Data Subject: The individual that is the subject of Personal Information.

Opt-Out: A system whereby a Data Subject is notified of the proposed transfer of its Personal Data to a third party and given the opportunity to object to that transfer.

Personal Data: Personal information contained in a database (whether electronic or not) that enables easy retrieval of Personal Information contained in it ('**Personal Information Database'**).

Personal Information: Information about a living individual from which the identity of the individual can be ascertained (including information which enables identification by easy reference to, or combination with other information). 'Personal Information' includes 'Personal Identifier Codes' which include items such as characters, numbers, symbols and/or other codes for computer use which represent certain specified personal physical characteristics (such as DNA sequences, facial appearance, finger and palm prints) and which are sufficient to identify a specific individual, as well as certain identifier numbers, such as those on passports, driver's licenses and resident's cards, and the 'My Number' individual social security ID numbers.

Personal Information Controller ('PIC'): (The verbatim English translation is 'business operator handling Personal Information') a business operator using a Personal Information Database for its business.

Personal Information/Data Processor: Is not defined by the APPI but for the purpose of this note and for ease of reference for readers who are familiar with the concept in other jurisdictions, is an entity which a PIC entrusts the handling of Personal Data in whole or in part within the scope necessary for the achievement of the purpose of utilisation' (e.g. entrusting Personal Data to a service provider such as a cloud computing service provider or a mailing service provider for the purpose of having them provide the PIC with the services).

Personal Number (**'My Number'**): a number processed from an individual's resident registry code number and a code corresponding to and used in lieu of such number.

Purpose(s) of Utilisation: The purpose(s) of use of Personal Information as specified by a PIC to the Data Subject whose Personal Data is to be used by the PIC.

Sensitive Information: (The verbatim English translation is "personal information requiring consideration") includes Personal Information relating to matters such as race, creed, religion, physical or mental disabilities, medical records, medical and pharmacological treatment, and arrest, detention or criminal proceedings (whether as an adult or a juvenile) or criminal victimisation. (Industry-sector guidelines may apply additional categories of Sensitive Information).

Specific Personal Information: Personal information which contains a Personal Number.

*[**2020 Amendments – New definitions:***

Person-related Information: *Information which is not Personal Information for the transferor as it cannot identify the Data Subject from the information (even by easy reference to, or combination with, other information) but may be for a transferee as it may be able to identify the Data Subject by reference to other information held by the transferee.*

Pseudonymously Processed Information: *Information which has been processed from Personal Information in a manner that the Data Subject can no longer be identified solely from the data.*
(Whilst the PPC has not published draft guidelines or commentaries that clarify how Pseudonymously Processed Information and Anonymised Information are different, the current understanding in practice is that Pseudonymously Processed Information is information that would still enable identification of the Data Subject if other information was also referenced to or combined together, and as such still constitutes Personal Information, whilst Anonymised Information is not.)

Pseudonymously Processed Information Controller: *a business operator using a Pseudonymously Processed Information database for its business.]*

2. THE LAW

2.1. Key acts, regulator

- The Act on Protection of Personal Information. (Unless stated otherwise, the discussion below relates to the APPI)
- The Personal Information Protection Commission ('**PPC**') – the principal data protection regulator[2] - issued various guidelines and Q&As
- The Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures ('**My Number Act**').
- The Act to amend the Act on Protection of Personal Information, etc*. (the '**2020 Amendments Act**')*.

2.2. Guidelines

Key guidelines provided by the PPC and relevant ministers are listed below; some of these guidelines are subject to 'Q&As' or 'Commentaries' which supplement the guidelines with practical guidance. The APPI delegates the power to require reports from PICs to the minister regulating each business sector or a designated minister, etc. As such, each ministry provides, jointly with the PPC or individually, guideline(s) and Q&As and Commentaries with regard to the relevant business sector.

Guidelines and Q&As issued by the PPC include the followings (only in Japanese):

- General guidelines on the APPI (available here) ('**General Guidelines**');
- Guidelines on the APPI (for transfers to third parties in foreign countries) (available here);
- Guidelines on the APPI (for checking and recording on transfers to third parties) (available here);
- Guidelines on the APPI (for Anonymised Information) (available here);
- Guidelines on the APPI (for data leakages) (available here) ('**Data Loss Guidelines**');
- Q&As on the General Guidelines and Data Loss Guidelines (available here)

[2] See section 4. Below.

The guidelines provide detailed guidance on the scope and meaning of the provisions of, and certain terms used in the APPI, and examples of their application, though the examples do not expand or limit the scope of the APPI. The guidelines also make it clear that a breach of the guidelines which is expressed as an obligation, rather than a recommendation, would be deemed a breach of the APPI. The general guidelines listed above are not comprehensive and additional guidelines (only in Japanese) have been issued for businesses and industries where there is a need for more stringent protection of Personal Information.

For credit card businesses and businesses which use genetic information, the Ministry of Economy, Trade and Industry ('**METI**') has issued the following guidance:

- for Personal Information protection in the credit industry (available here); and
- for protection of Personal Information in the industry using genetic information of individuals in the economic and industrial sectors (available here).

For the financial sector (except the credit card industry, which is regulated by METI), the Financial Services Agency ('**FSA**') has issued the following guidance:

- for Personal Information protection in the financial industries (available here) ('**Financial Sector Guidelines**'); and
- practical guidelines for security policies regarding Personal Information protection in the financial industry (available here).

For the medical sector, the Ministry of Health, Labour and Welfare ('**MHLW**') has issued the following guidance:

- for appropriate handling of Personal Information by medical or care-related service providers (available here);
- concerning safety management of medical information systems (available here);
- ethical guidelines concerning medical research targeting humans (available here);
- ethical guidelines concerning analysis and research of the human genome and genes (available here);
- concerning gene therapy clinical research (available here); and
- ethical guidelines concerning research of assisted reproduction technologies that produce fertilised embryos (available here).

For employment and welfare areas, the MHLW has issued the following guidance:

- notice regarding handling of health information in employment management (available here);
- for appropriate handling of Personal Information at health insurance societies, etc. (available here);
- for appropriate handling of Personal Information at national health insurance societies (available here);
- technical security measures regarding Personal Information in the private pension area (available here);
- for appropriate dealing by employment placement service providers, worker recruiters, worker recruitment agents or worker suppliers with equal treatment, statement of working terms, handling of Personal Information of job seekers, duties of employment placement service providers, correct statement of terms of recruitment, etc. (available here);
- concerning measures which staffing service providers are required to take (available here); and
- for appropriate dealing by supervising organisations with statement of working terms, handling of Personal Information of implementers of intern training supervised by organisations or technical intern trainees at training supervised by organisations, etc. (available here).

For the telecommunication sector, the Ministry of Internal Affairs and Comminutions ('**MIC**') has issued the following guidance:

- concerning protection of Personal Information by telecommunication businesses (available here) ('**Telecommunications Sector Guidelines**');
- commentaries on the Telecommunications Sector Guidelines (available here) ('**Telecommunications Sector Guidelines Commentaries**');
- concerning protection of Personal Information of broadcast receivers (available here);
- concerning the protection of Personal Information in postal businesses (available here); and
- concerning protection of Personal Information in correspondence delivery businesses (available here).

The Ministry of Justice has issued guidance concerning protection of Personal Information in the debt collection service industry (available here).

Regarding the My Number Act, the PPC has issued the following guidance:

- concerning appropriate handling of Specific Personal Information (main body and separate volume: security measures concerning Specific Personal Information) (available here); and
- concerning appropriate handling of Specific Personal Information in financial businesses (available here).

3. SCOPE OF APPLICATION

3.1. Who do the laws/regulations apply to?

The APPI applies to every PIC in Japan, whether a person or entity; the exemption for a person or entity which has not handled Personal Information of more than 5,000 individuals in certain cases was abolished when the APPI was revised in 2017, though the General Guidelines relax the standards of security measures for "Small or Mid-sized Business Operators" (see Section 6.4 below).

The APPI only applies to persons or entities that handle Personal Information in the course of their business. For this purpose, a 'business' means activities which can be conducted repeatedly for a particular purpose and are regarded as a business under social conventions; a business can be for profit or not. A broadcasting institution, newspaper publisher or other press organisation, professional writer, university or other academic organisation, religious body, or political party are exempted from the obligations under the APPI in connection with such press, professional writing, academic, and political activities respectively.

3.2 Extraterritorial application

The APPI applies extraterritorially when an overseas PIC which has obtained Personal Information of a Data Subject in Japan in relation to its provision of goods or services to the Data Subject in Japan and handles that Personal Information, or any Anonymised Information created from it, in a foreign country. The obligations which apply exterritorialy include:

- to specify and notify or publicise the Purposes of Utilisation, and to use it within that purpose;
- to keep Personal Data accurate and up-to-date, and to make efforts to delete it when no longer required;
- to take measures to protect the data against leakage, etc.;
- to supervise employees handling Personal Information and any service provider entrusted with the handling of Personal Data;
- the rules governing disclosure to a third party;

- to publicise privacy policies;
- the rights of a Data Subject to access, correct, and stop the illegal use of Personal Data; and
- certain rules regarding Anonymised Information.

Whilst the PPC can only render 'advice' to a PIC based overseas, it may provide information to foreign regulatory authorities for their own regulatory enforcement purposes.

*[**2020 Amendments**: Under the current APPI, the act applies exterritorialy only when an overseas PIC has obtained Personal Information of a Data Subject in Japan in relation to its provision of goods or services "to the Data Subject"; this does not cover situations where the Data Subject is different from the customer of the goods or services (e.g., an offshore PIC provides a corporate body customer in Japan with its goods or services, and in relation to the provision of the goods or services, collects Personal Information a director or employee of the corporates). Under the 2020 Amendments, the APPI will also apply extraterritorially to such cases as long as both of the corporate body customer and the Data Subject individual are located in Japan.]*

3.3. What types of processing are covered/exempted?

The APPI applies to "handling" of Personal Information by a PIC. "Handling" is not defined in the APPI or the General Guidelines, but was explained in the published discussions made at the government's committee which provided the outline of the original APPI in 2000, to mean the collection (acquisition), retention, use, transfer and any other acts of handling Personal Information. "Processing" was also explained at the discussions to include any such acts. The terms are understood in practice to be given such meanings.

For other scope of applications of the law, see section 3.1 above.

4. DATA PROTECTION REGULATORY AUTHORITY

4.1. Main regulator for data protection

The PPC is the primary regulator under the APPI and the My Number Act.

4.2. Main powers, duties and responsibilities

The PPC:

- has the task of ensuring the appropriate handling of Personal Information and Specific Personal Information so as to protect individuals' rights and interests;
- has the primary investigatory, advisory and enforcement powers under the APPI and the My Number Act, including the power to investigate the activities of a PIC, an Anonymised Information Controller and a person handling Specific Personal Information, and in certain instances to render advice to and make orders against them, if the infringement of an individual's material rights or interests is imminent;
- (in connection with protection of Personal Information under the APPI) may delegate its investigatory powers and the authority to receive data breach reports from affected PICs to the relevant minister, etc., but not its advisory or enforcement powers. The PPC has made and published the delegations (the lists (only in Japanese) are available here (investigatory powers) and here (breach report receiving authorities)). For example, the Chief of the FSA has received the delegation with regard to PICs which are private sector financial institutions under the

agency's regulations, and the Minister of Internal Affairs and Comminutions (the chief of the MIC) has received the delegation with regard to PICs which are telecommunications careers, broadcasters and certain other business operators under the ministry's regulations. For PICs in the medical and care-service sector, the Minister of Health, Labour and Welfare (the chief of the MHLW) has not been given the delegation; the PPC still exercises the power and authority by itself; and

- can provide information to foreign data protection regulators and in limited circumstances may allow information to be used for criminal investigations overseas.

*[**2020 Amendments**:*

- *The PPC will set out the details of forms for its demand (in its exercise of its investigatory power) for a PIC to provide a report or documents, advice, order, etc.*
- *The rules of Japan's Code of Civil Procedure regarding service of process will apply mutatis mutandis to the PPC's delivery to a PIC (including an offshore PIC) of such demands referred to above.*
- *The PPC can effect constructive service by publication if:*
  - *(i) the address of a PIC is not available;*
  - *(ii) delivery of its communications to an offshore PIC pursuant to the rules of the Code of Civil Procedure (i.e., the procedure for delivery via the foreign country's relevant authority or agency, or the Japanese embassy or council in the foreign country) is not available; or*
  - *(iii) the PPC does not receive a certificate of delivery within 6 months after requesting the foreign country's authority or agency to serve the notice.*
- *The PPC can effect constructive service by posting a notice at a specified location in the PPC's office, and the constructive service will be effective upon the expiry of 2 weeks (in the case of a PIC in Japan) or 6 weeks (in the case of an offshore PIC) from the date of posting.*
- *The PPC may publish a PIC's failure to comply with a PPC order.]*

5. NOTIFICATION & REGISTRATION

There is no general requirement that a PIC be registered under the APPI or related regulations, or for any registration under the My Number Act. A PIC which wishes to use an Opt-Out for disclosure of Personal Data to a third party has to file the opt-out provision prescribed in the order described below in section 6 under 'transfers pursuant to an Opt-Out' (but not the rest of its privacy policies) with the PPC. The PPC will then review the provision to ensure it is appropriate in accordance with the requirements of the APPI and make it available to the public. If the opt-out is not sufficient in terms of clarity, easy-readability and formality the PPC may require it to be improved and re-filed.

6. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

6.1 Collection & use of Personal Information

A PIC must:

- not collect Personal Information by fraudulent or other unlawful means;
- notify the Data Subject of the Purposes of Utilisation prior to the collection of the Personal Information unless it has published the Purposes of Utilisation in advance in a manner readily accessible by the Data Subject; and
- obtain the Data Subject's consent before acquiring Sensitive Information of the Data Subject unless one of the exceptions listed in Section 13.2 below "Transfers permitted by law" applies to the acquisition.

6.2 Public announcements

A PIC must make the following items readily accessible to each Data Subject:

- name of the PIC;
- Purposes of Utilisation of Personal Information retained;
- the procedure for the Data Subject to require correction, etc. of their Personal Data; and
- where to complain about the PIC's handling of Personal Data.

(‘**Public Announcements’**)

6.3 Use of Personal Information

A PIC must use Personal Information only to the extent necessary to achieve the Purposes of Utilisation specified to the Data Subject and must make efforts to delete the Personal Data when it is no longer needed for the Purposes of Utilisation.

*[**2020 Amendments**: A PIC must not use Personal Information in a manner which may facilitate or prompt an illegal or inappropriate act.]*

6.4 Personal Data Management & Security

A PIC must:

- take reasonable steps to keep Personal Data as accurate and up-to-date as is necessary to achieve its Purposes of Utilisation;
- take all necessary security measures to avoid the loss of, or unauthorised access to Personal Data; and
- exercise necessary and appropriate supervision over its employees handling the Personal Data, or any persons or entities delegated to handle Personal Data (e.g. a Personal Information/Data Processor), so as to ensure they implement and comply with such security measures.

The General Guidelines' exhibit illustrates high-level examples of security measures, which are categorised into:

- establishing basic principles;
- setting out internal rules;
- organisational security measures (e.g. appointment of a responsible person, definition of each person's responsibility, definition of scope of data handled by each staff member, data processing operation and incident reporting line, definition of responsibilities between divisions, periodical internal and/or external audit, etc.);
- staffing security measures (e.g. staff education and training, confidentiality provisions in work rules, etc.);
- physical security measures (e.g. area access control (IC card, number keys), prevention of device theft, prevention of leakage from portable devices, non-recoverable deletion of data); and
- technological security measures (e.g. system access control, access authorisation (user ID, password, IC card, etc.) control, prevention of unauthorised access (security software instalment and upgrading, encryption, access log monitoring), continuous review of system vulnerability, etc.).

The General Guidelines relax the standards for security measures for a “Small or Mid-sized Business Operator”, which is defined as a PIC with 100 or less employees but excluding (i) a PIC who has handled

Personal Data of more than 5,000 Data Subjects on at least one day in the past 6 months and (ii) a PIC who processes Personal Data on behalf of another PIC under a contract and is seen not only as processor but also as controller (i.e., PIC) with regard the data; the relaxed standards include:

- Establishing basic principles;
- setting out basic processes for collecting, using and storing Personal Data;
- for organisational security measures, clarifying who is responsible for handling Personal Data and who is not if more than one staff member handle Personal Data; such responsible person checking Personal Data is handled in accordance with the prescribed basic process; and checking the data leakage reporting process in advance;
- for physical security measures, simplified measures (e.g., password lock) are allowed; and
- for technological security measures:
  - clarifying which staff members are allowed to access devices;
  - controlling access by user account control;
  - keeping devices' operating software up-to-date and introducing security software; and
  - setting passwords for opening files when sending them by email.

Guidelines provided by the METI, FSA, etc. set out further detailed requirements for security measures and provide specific examples for certain specified industry areas.

*[**2020 Amendments: Pseudonymously Processed Information***

As Pseudonymously Processed Information is still Personal Information (as it would still enable identification of the Data Subject if other information was also referenced to or combined with it), a Pseudonymously Processed Information Controller is generally subject to the same obligations as a PIC regarding management and security of Personal Information above (and transfers to third parties) in connection with Pseudonymously Processed Information. However, its obligations are relaxed in the following aspects:

- *Allowed to change its Purposes of Utilisation beyond the scope reasonably related to the original Purposes of Utilisation even after creation or acquisition of Pseudonymously Processed Information*
- *Not subject to the general obligations to notify the PPC and the Data Subjects of a data breach*
- *Not subject to a Data Subject's right to access, correction or request to cease use (and therefore its Public Announcements (as defined above) do not need to include procedures for Data Subjects to access, correction, etc.)*

A PIC must not refer to other information to re-identify the relevant data subject of Pseudonymously Processed Information.

*A Pseudonymously Processed Information Controller may not disclose its methods for pseudonymisation of the subject's Personal Information, the data removed in the pseudonymisation process or any process used to verify the pseudonymisation ('**Removed Data etc**'). It must take security measures to prevent leakage of Pseudonymously Processed Information and Removed Data etc. and supervise and control a person contracted to process such information t may not refer to other information to re-identify the Data Subject relevant to Pseudonymously Processed Information.]*

6.5 Anonymised information

A PIC which creates Anonymised Information may not disclose its methods for anonymisation of the Personal Information underlying the Anonymised Information, the data removed in the anonymisation process or any process used to verify the anonymisation. A recipient of Anonymised Information may not seek to acquire any such information, whether from the transferor or otherwise. When a PIC processes Personal Information to Anonymised Information, it must make public in an

appropriate manner (such as via the Internet) what categories of Personal Information (e.g. ages, shopping behaviour, travel habits, etc.) are included in the Anonymised Information so Data Subjects are able to make enquiries with the PIC.

7. DATA PROCESSOR RIGHTS AND RESPONSIBILITIES

Neither the APPI nor any related regulations impose any direct obligations on Personal Information/Data Processors. However, as explained above, necessary and appropriate supervision must be exercised by a PIC over any third parties delegated by it to handle Personal Data. Such supervisory measures include execution of agreements between a PIC and a Personal Information/Data Processor providing appropriate security measures that should be taken by the Personal Information/Data Processor and the power of the PIC to instruct and investigate the Personal Information/Data Processor in connection with its handling Personal Data entrusted to it.

8. DATA CONTROLLER AND PROCESSOR AGREEMENTS

See section 7. above with regard to the requirement for a PIC to implement supervisory measures over any third parties delegated to handle Personal Data, which include execution of agreements between a PIC and the Personal Information/Data Processor providing appropriate security measures.

9. DATA SUBJECTS' RIGHTS

If requested by a Data Subject, a PIC must disclose in writing and without delay to the Data Subject, the Data Subject's Personal Data held by it, unless the Data Subject has agreed to receiving it by other means (e.g. as electronic data). Access can be refused if it would result in:

- injury to the life or bodily safety, property or other rights and interest of the Data Subject or any third party;
- a material interference with the PIC's business operations; or
- a violation of other Japanese laws prohibiting disclosure.

Data Subjects also have the right to revise, correct, amend or delete their Personal Data, and to request cessation of use of their Personal Data if this is used for a purpose other than the one originally stated, or if it was acquired by fraudulent or other unlawful means. If a Data Subject requests a PIC to cease using their Personal Data, the PIC must do so unless the request is unreasonable, or the cessation would be costly or would otherwise be difficult (e.g. the recall of books already distributed). In this case, the PIC must take alternative measures to protect the rights and interests of the Data Subject. The PIC must notify the Data Subject without delay of whether the requested action has been taken, and, if not taken, must endeavour to explain the reasons why. A Data Subject can enforce its rights to require revision, etc. of its Personal Data by civil action if such a request is not complied with within two weeks of being made.

Data Subjects do not have any of the rights above if:

- the Personal Data will be deleted within six months of collection; or
- if the Data Subject or other person comes to know that there is such Personal Data held by the PIC it might result in:
    - injury to the life or bodily safety, property or other rights and interest of the Data Subject or any third party;
    - encouraging illegal or unjust acts;

- endangering national security, damage to a trusted relationship with a foreign country or international organisation, or the country's disadvantage on negotiation with a foreign country or international organisation; or
- obstacles to prevention, suppression or investigation of crimes or otherwise impairing public safety and order.

*[**2020 Amendments:***

- *A Data Subject will be given a right to access to a PIC's record of data transfers to third parties.*
- *Personal Data which the PIC will delete in 6 months will no longer be exempted from the Data Subjects' right to access.*
- *The Data Subject will have the right to require the PIC to cease using Personal Data or to cease transferring Personal Data to third parties if the PIC no longer needs to use the data, a data breach has occurred or there is a likelihood of infringement of the Data Subject's rights or lawful interests due to the PIC's handling of the Personal Data.*
- *Pseudonymously Processed Information is not subject to the data subject's right to access or cessation of use.]*

10. DATA PROTECTION OFFICERS

The APPI does not specifically require a PIC to appoint a data protection or similar officer. However, the General Guidelines provide that a PIC must take security measures for the handling of Personal Information, an example of such a security measure being 'appointment of a person in charge of the handling of Personal Information and the definition of the responsibilities of the person' (see section 6.4 above). The guidelines state that whether measures are mandatory depends on the materiality of the damage which may be suffered by Data Subjects in the event of a data leakage, the size and nature of the business, and the general nature of the data handling (including the nature and volume of data handled). Some industry-sector guidelines also provide such requirements.

Certain private organisations or associations have created qualifications as 'data protection officer' or equivalent, and issue them to persons who have passed examinations set by them (e.g. Japan Consumer Credit Association issues a Personal Information Handling Officer qualification, and the Information-Technology Promotion Agency issues an Information Systems Security Administrator qualification). These qualifications are not acknowledged, supported or required by law, but are industry-driven efforts to enhance data privacy.

11. DATA BREACH NOTIFICATION

11.1. General obligation

The Data Loss Guidelines are limited to setting out certain principles for handling leakages, leaving PICs to decide what specific action should be taken with regard to the facts of each case.

11.2 Action following a data loss

The Data Loss Guidelines state that in the event of the leakage, destruction or damage of Personal Information or the likelihood of any of them:

- it is 'desirable' that the affected PIC takes the following steps:
  - reporting of the incident within the PIC;

  - taking measures to prevent expansion/aggravation of any damage (to Data Subjects or third parties affected by the incident) due to the incident;
  - investigation of relevant facts and the cause of the incident;
  - identification of the affected areas within the servers/systems of the PIC and of the Data Subjects whose data was affected;
  - promptly planning and implementing measures to prevent the recurrence of the incident or further incidents that may otherwise occur due to the security vulnerability which allowed the occurrence of the incident in question;
  - unless the leaked data is encrypted at a high level, 'promptly' notify the Data Subjects potentially affected or make the facts of the leakage easily available to those Data Subjects (depending on the facts of each case) for the purpose of preventing the Data Subjects or third parties incurring further damage (e.g. to give the Data Subjects opportunities to take actions to avoid or mitigate harms by third parties' use of the leaked information); and
  - publicly announce the relevant facts and measures to be taken to prevent a recurrence of the incident (depending on the facts of each case).
- the PIC must make efforts to promptly notify to the PPC of a breach unless:
  - the leaked data is encrypted at a high level;
  - all the leaked data has been collected by the PIC prior to being seen by third parties;
  - there is no risk of any specific individual being identified from, or the affected Data Subjects being harmed by use of, the leaked data;
  - the data loss was obviously only internal and not an external leakage; or
  - the leakage is obviously insignificant (e.g. a mis-delivery of parcel where the Personal Information is only on the delivery address label on it).

A data breach notification to the PPC is done by completing a web-based form online here. If a PIC has a security policy which does not allow access from its system to external systems online or has trouble in completing an online submission, other methods of submission, e.g. by fax or post, are still available.

Where a PIC has entrusted Personal Data to a Personal Information/Data Processor and the Personal Information/Data Processor was subject to the data loss the obligations above fall on the PIC.

11.3 Terminology

Leaked data is encrypted at a high level when (i) the encryption system is on the list of ISO/IEC 18033 or the Japanese government has confirmed the encryption system as being sufficiently secure, and (ii) the decryption key is remotely controlled or not usable by a third party, or the leaked data or decryption key can be remotely deleted.

'Desirable', 'promptly' and 'make efforts' are not defined or explained in the Data Loss Guidelines and their meaning will need to be determined by reference to their common definition, regulatory and best practice, and the facts of each case, in particular the risk of an innocent party suffering any loss.

It is not uncommon for obligations under Japanese laws and regulations to be expressed as being ‘desirable’ or similar, and in the absence of factors which would dictate otherwise, best practice would be to comply with the obligation unless there is a good reason not to. In addition, the greater the harm non-compliance may cause, the more advisable compliance becomes.

Although 'promptly' is not defined, the nuance of the original Japanese term '*sumiyakani*' would

suggest four or five days in many cases, though this is subject to the facts of each case, and in particular how seriously the affected Data Subjects may be affected and accordingly how urgently they should be notified.

Examples of what might constitute 'making the fact of the leakage easily available to the affected Data Subjects' include:

- placing a sign in an office habitually attended by the Data Subjects; or
- adding a notice on an accessible webpage directly linked from the home page of the PIC's website.

Although what constitutes 'make effort' is not defined it would be given its normal meaning; though, as with 'promptly' and 'desirable', the greater the actual or potential harm of the data loss, the more advisable compliance with the obligation becomes.

11.4 Reporting to the PPC

Whilst the obligation to report a data leakage to the PPC is only to 'make efforts', best practice would be to submit a report unless any of the exemptions above applies (in which case a report is not required). If the PIC thinks the data loss is not serious enough to warrant a formal report but it is not exempted from reporting, it can seek informal guidance from the PPC on what action to take. If the data loss is very serious, e.g. the loss of bank account details and passwords, or the PIC is not certain what action to take the PIC should contact the PPC (and local counsel) at the earliest opportunity, and without waiting to complete the formal report to the PPC. Should a data loss not be reported, and the PPC subsequently becomes aware of it, it may require a report be submitted.

11.5 Notifying affected Data Subjects

When considering whether to notify affected Data Subjects of a data loss directly, or by a more general notice, the two major factors for a PIC to consider are the seriousness of the loss and the harm it may cause, and the effectiveness of the means of notification. If a loss may cause serious harm, the prudent course would be to make it public promptly, and then notify affected parties individually (always subject to any directions from the PPC). Where a PIC has decided to give a general notification, it will need to evaluate how effective the means of notification is likely to be; for example, if notification is given on a website, how likely is it that the affected parties will visit the website and how long it should be kept active in order to notify an appropriate proportion of affected Data Subjects. A notification, individual or general, should include a description of the loss and the actions taken by the PIC to mitigate its effects, and it would be advisable to include a phone number or email address which the affected Data Subjects can use to obtain further information on the loss.

As noted, depending on the facts of each case, it might be appropriate for the PIC to publicly announce the relevant facts of the data loss, and the measures to be taken to prevent its recurrence; there is no guidance on what form this notice should take, and although it may also be sufficient as notice to the affected Data Subjects, its effectiveness as such would need to be considered carefully.

Notifications (individual or general) should be given in Japanese, and if any affected Data Subjects may not understand Japanese, any other appropriate foreign language. Notifications should not be given only in a foreign language unless it is certain that all affected Data Subjects will understand that language.

11.6 Investigations

If a data loss has occurred and been reported to the PPC, voluntarily or at the request of the PPC, it may investigate the background to the loss, the PIC's data management procedures and the actions the PIC has taken (or not taken) to notify the affected parties (and the PPC). Where the PPC finds defects in the PIC's data management or post-loss actions, it may give guidance to the PIC on what actions to take to improve its data management, or what further steps should be taken to notify affected Data Subjects of the loss. If the defects are material, the PPC may issue advice for improvement to the PIC and publish the advice on its website. If the PIC fails to follow advice for improvement, the PPC may then escalate the matter and issue an order for improvement. (An order for improvement may be issued immediately without preceding advice for improvement in limited cases of a serious data loss.)

If a PIC has not notified the PPC or the affected Data Subjects of the data loss (or has not publicised the loss if material in either scale or subject matter) and the PPC comes to know of the loss, it might be more likely to find the PIC's attitude to compliance unsatisfactory and thus issue and publish an advice for improvement.

*[**2020 Amendments:***

A. Reporting to regulators

*Reporting to the PPC will become mandatory. However, in order to minimise the burden on industry which would arise from having to report minor breaches, the obligation will be limited to certain breaches; the threshold(s) will be set out later by PPC regulation and will likely be based on whether there is a substantial risk to individuals' rights and interest. The "Outline" of the 2020 Amendments which the PPC published in 13 December 2019 (prior to the publication of the bill for the 2020 Amendments) (the '**Outline**') proposed that the thresholds shall refer to the number of losses (though it is not clear whether the "number" is the number of affected Data Subjects) and any losses, irrespective of the number of losses, of Sensitive Information, though these criteria are not expanded upon in the 2020 Amendments Act and are to be clarified in PPC regulations which will implement the act.).*

B. Timing of reporting

*The current obligation to "*make efforts to promptly notify to the PPC of a breach" *will become an obligation to notify the PPC of certain information regarding the breach. The Outline proposed that the report should be "promptly", though this is not expanded upon in the 2020 Amendments Act and is to be clarified in PPC regulations or guidelines which will implement the act. What constitutes "promptly" will still be judged on a case-by-case basis. The PPC will then be able to require a further report within a specified period. The change will mean that PICs should establish efficient data loss reporting mechanisms rather than handle the reporting of losses on an ad-hoc basis after they have occurred.*

C. Recipient of reports

The current APPI regime enables reporting to certain accredited information protections organisations; the 2020 Amendments will centralise the reporting process so reports will only be made to the PPC or delegated government agencies.

D. Notifying Data Subjects

The current obligations to notify affected Data Subjects of a data breach are somewhat vague and leave the PIC to make a determination of what action to take (see **11.5 Notifying Affected Data Subjects** above*); under the 2020 Amendments as a general rule if a PIC is required to report a data loss to the PPC it will also be mandatory to notify the loss to any affected Data Subject. If it is not possible or practicable to notify Data Subjects directly, e.g. if the Data Subject's contact details are not known, and the PIC has taken other measures to protect the rights and interest of the Data Subjects (such as using public notices), the obligations to directly notify the Data Subjects do not apply. The Outline and the 2020 Amendments Act do not clarify the timing of notification; the act provides that a notification by a PIC to the Data Subjects shall be in a manner that is set out in the PPC's regulations. The regulations, which are yet to be published, may clarify on timing of the notification. PICs should take all reasonable steps to maintain up-to-date contact details for their Data Subjects and/or periodically review their procedures for notifying data losses through public notices and other means.]*

11.7 Sanctions

Neither the APPI nor the Data Loss Guidelines imposes any sanctions for failure to make a report or notification of a data loss, and the Data Loss Guidelines only require a PIC to 'make efforts' to report a data loss. However, it should be noted that a PIC has presumably breached its duties for data security when it failed to prevent the data loss, and it would probably further be in breach of its obligation if it did nothing following the data loss where action was obviously required. These breaches will allow the PPC to issue an advice for improvement. That said, and as noted here, it is advisable for PICs to report a data loss unless a report is clearly not required, and failure to report might be a factor the PPC would take into consideration when deciding whether to issue an advice for improvement. The PPC may publish such advice once issued. If an advice is not complied with the by PIC, the PPC may escalate to issue an order for improvement.

Failure to comply with an order for improvement would be grounds for criminal imprisonment for up to 6 months or a criminal fine of up to JPY 300,000 for an individual who is the PIC or the director or employee of the PIC entity in charge of the breach, and the same criminal fine for the PIC as an entity.

*[**2020 Amendments**: Failure to comply with an order for improvement would be grounds for criminal imprisonment for up to 1 year or a criminal fine of up to JPY 1,000,000 for an individual who is the PIC or the director or employee of the PIC entity in charge of the breach, and the same criminal fine for the PIC as an entity.]*

11.8 Compensation

To date, PICs which have suffered a data loss have often voluntarily offered compensation to affected parties both to forestall any proceedings, and to maintain good public relations. Compensation payments to Data Subjects (per person) have ranged from JPY 500 of e-money or gift vouchers, through gift vouchers of JPY 10,000 (approx. €80), to cash payments of JPY 35,000 (approx. €290). If an affected party brings an action before a court against a PIC for a data loss, any judgment by the court would be likely to be an order against the PIC to pay damages on the grounds of a breach of contract or tort theory. Save for cases such as the unauthorised use of affected payment card data or the disclosure of Sensitive Information affecting the personal lives of individuals, the amount of

damages an affected party might be entitled to is frequently not large enough to warrant the commencement of proceedings once the costs of the proceedings are taken into consideration.
It should also be noted that in Japan it is often important to treat all affected parties equally. Even if a PIC does not publicise a data breach and communicates privately with each affected party individually, the widespread use of social media makes the risk of unequal treatment between affected parties being kept private increasingly unlikely, with its attendant negative impact on the PIC's reputation.

11.9. Sectoral data loss obligations

Whilst the Data Loss Guidelines only provide that it is 'desirable' for an affected PIC to take actions, including giving notice to affected parties and publicising the incident, and that it should make 'efforts' to notify to the PPC, the Financial Sector Guidelines (as on the list at 2.2. above) provide that such actions are mandatory in the financial service sector. Similarly, the Telecommunications Sector Guidelines Commentaries (as on the list at 2.2. above) provide that a breach of secrecy of communications must be reported to the MIC.

12. SANCTIONS

See sections 11.7.

In addition, many sector-specific regulations authorise the relevant regulators to enforce the regulations by rendering business improvement orders, or business suspension orders in the worst cases, against providers of services which require licences from the regulator, “where necessary for ensuring the appropriate operation of the business”. “Appropriate operation of the business” may include the management of security of customers’ data. For example, the FSA may order a business improvement order against a bank pursuant to the Banking Act, or against an investment manager pursuant to the Financial Instruments and Exchange Act, if the service provider failed to manage the security of customers’ data in the course of operation of the licensed businesses.

13. DATA TRANSFERS AND OUTSOURCING

13.1 General rule

Transferring Personal Data to third parties, including affiliated entities of the PIC, without the prior consent of the Data Subject is prohibited unless an exception applies. The primary exceptions are listed below.

13.2 Transfers permitted by law

The prior consent of the Data Subject to a transfer of its Personal Data (including Sensitive Information) is not required if the transfer:

- is specifically required or authorised by any laws or regulations of Japan;
- is necessary for protecting the life, health or property of an individual and consent of the Data Subject is difficult to obtain;
- is necessary for improving public health and sanitation, or promoting the sound upbringing of children, and the consent of the Data Subject is difficult to obtain; or
- is required by public authorities or persons commissioned by public authorities to perform their duties and obtaining the prior consent of the Data Subject carries the risk of hindering the

performance of those duties (e.g. the disclosure is required by police investigating an unlawful act).

13.3 Transfer pursuant to an Opt-Out

Personal Data (other than Sensitive Information) can be transferred after the PIC has notified the Data Subject or made readily available to the Data Subject, and filed with the PPC, all of the following information, and a period necessary for the Data Subject to exercise its opt-out right has expired:

- that the transfer is within the scope of the originally stated Purpose of Utilisation;
- the specific Personal Data to be transferred;
- the means with which the Personal Data will be transferred;
- the fact that the transfer of the Personal Data is subject to an opt-out; and
- where to provide such opt-out exercise notice.

The General Guidelines only say that how long the 'period necessary for the Data Subject to exercise its opt-out right' varies depending on factors such as the nature of business, how close the relationship between the Data Subject and the PIC is, the nature of the Personal Data to be transferred, and how quickly the PIC can handle the Data Subject's exercise of its opt-out rights.

*[**2020 Amendments**:*

It has been clarified that transfers pursuant to the Opt-Out rule will not be available for Personal Information which has been obtained (i) by fraudulent or other unlawful means or (ii) from a preceding transferor pursuant to the Opt-Out rule. This revision is based on the PPC's finding that Personal Data has often been traded or shared between name-list brokers or peer business operators under the Opt-Out rules.
The following information will also be required to be filed with the PPC:

- *the name of person who is the representative of the transferor PIC if the PIC is a corporate body, in addition to the name of the transferor PIC itself;*
- *how the transferor PIC has obtained the Personal Data which it will transfer pursuant to the Opt-Out rule; and*
- *other matters which the PPC will set out in regulations.]*

13.4 Transfer of Sensitive Information

A transfer of Sensitive Information to a third party requires the consent of the Data Subject unless an exception as listed above applies; such consent cannot be given through use of an Opt-Out.

13.5 Transfer of Anonymised Information

Anonymised information may be transferred to a third party without the consent of the original Data Subject (it no longer constitutes 'Personal Information'), provided that the transferor makes public both the fact of the transfer and what types of Personal Information are included in it and notifies the recipient that the information is Anonymised Information.

*[**2020 Amendments:***

Transfer of Pseudonymously Processed Information

As Pseudonymously Processed Information is still Personal Information, the requirements and exceptions applicable to the transfer of Personal Information as described in this Section 13. also apply to the transfer of Pseudonymously Processed Information.

Transfer of Person-related Information

Although Person-related Information is not Personal Information for a transferor, it is for a transferee as the relevant Data Subject is identifiable by reference to other information held by the transferee, and the 2020 Amendments set out the general requirement for prior consent of the Data Subject for a transfer of its Person-related Information to a third party transferee (where the consent must be based on the Data Subject's understanding that the information will be person-identifiable at the transferee). Transfers permitted by law (e.g., a transfer required or authorised by Japanese laws or regulations) also apply. Transfers under an Opt-Out is not permitted. The terms of the 2020 Amendments Act do not provide that the entities listed in the "Scope of third parties" section (Section 13.6) below are not third parties for the purpose of transfers of Person-related Information; that being so it is currently understood that transfers to such entities will still generally require the Data Subject's consent, subject to a future clarification by the PPC in guidelines, etc. The revision of rules, under the 2020 Amendments, on a transfer of Personal Information to a third party in a foreign country (as described below) also applies to a transfer of Person-related Information. Transfer due diligence and records will also apply.

*Cookies and website browsing/web form entry history data associated with the cookies ('**Cookies, etc.**') are not Personal Information unless the relevant Data Subject can be identified by easy reference to or combination with other information. However, even if Cookies, etc. are not Personal Information for a transferor in this sense, if the Cookies, etc. is transferred to a third party transferee and would be Personal Information for the transferee as it holds other information and the individual related to the Cookies, etc. can be identified by reference to such other information (e.g., the Cookies, etc. are a history of website browsing that suggests the individual's activity behaviour, preference of goods or services, or otherwise usable for profiling, and the transferee would use the Cookies, etc. for targeted advertising, or assessment of application for job position or financial services, etc.), this will be a transfer of Person-related Information under the 2020 Amendments and will thus be subject to the general requirement for the prior consent of the Data Subject.]*

13.6 Scope of third parties

Under the APPI, the following entities are deemed not to be third parties (meaning that the transfer of Personal Data (including Sensitive Information) to such parties does not require the Data Subject's consent):

a. a Personal Information/Data Processor;
b. a company that enters into a merger, a company split or a business transfer with the PIC. (Disclosure in the process of negotiations for mergers and acquisitions is permissible if made upon execution of a non-disclosure agreement which requires the company to which the data is disclosed to implement appropriate safety measures); or
c. a company designated to jointly use the Personal Data with the PIC. In this case, the PIC must notify, or make readily accessible to the Data Subject:
    a) the fact of such joint use of the Personal Data;
    b) the scope of the Personal Data to be jointly used;
    c) the scope of the parties who will jointly use the Personal Data;
    d) the purpose of the joint use; and
    e) the name of a party among the joint users responsible for dealing with enquiries from or exercise of rights by Data Subjects.

Such joint use is available by group companies or business partners or affiliates which provide integrated services to common customers.

Where a transfer of Personal Data is to a person or entity which is not a third party, further transfer of the Personal Data by that person or entity would be subject to the consent rules and exceptions applicable to such transfers, as described in this note.

13.7 Transfers to branches

Though not a specified exception to the general consent requirement, a transfer of Personal Data between a Japanese company and its Japanese branch, or between a foreign company and its Japanese branch is not a transfer of Personal Data to a third party as in each case the branch and the company are the same legal entity.

In the case of a foreign company with a Japanese branch:

a. If the Japanese branch first collects and handles Personal Information and subsequently transfers the Personal Data to its offshore parent (including any other presence (e.g., data server) of the offshore parent or of an affiliate entity of the offshore parent acting as a Personal Information/Data Processor contracted by the parent/branch in a foreign country ("**offshore presence**")):
   (i) The offshore parent is subject to the application of the APPI as a PIC in connection with handling of Personal Information at the Japanese branch.
   (ii) The transfer of the Personal Data from the Japanese branch to the offshore parent or to an offshore presence is not subject to the restriction on transfers under the APPI (as described above).
   (iii) Regarding the offshore parent's handling of Personal Data itself or through an offshore presence upon the transfer from the Japanese branch, the General Guidelines state that the rules of extraterritorial application of the APPI to an overseas PIC (i.e., that the APPI only applies when the overseas PIC has obtained Personal Information of a Data Subject in Japan in relation to its provision or goods or services to the Data Subject) (see Section 3.2 above) applies to a foreign company (offshore parent) with a Japanese branch handling Personal Information at the offshore parent (or by extension an offshore presence). However, it would be prudent to take the view that the offshore parent may be subject to the APPI in connection with the handling of Personal Data at the offshore parent or foreign presence even if the Personal Data is not obtained in relation to the provision of goods or services to the Data Subject by the offshore parent because (x) multinational companies often operate data management systems on a globally integrated basis where a Japanese branch can share the data on the system and (y) in practice the PPC may not accept the view that the offshore parent can evade the security and other requirements under the APPI merely by transferring Personal Data from the Japanese branch to a foreign presence within the offshore parent.

b. If the offshore parent operates a globally integrated data management system (with a data server in a foreign country) and Personal Information obtained by activities of the Japanese branch is provided from the Data Subject or other source directly to the integrated data system offshore, the discussion at a. (i) and (iii) is likely to equally apply.

c. If the Japanese branch does not collect and handle Personal Information, and the offshore parent collects Personal Information of a Data Subject in Japan without involving the Japanese

branch, or it is provided to a foreign presence without involving the Japanese branch, the rules of extraterritorial application of the APPI to an overseas PIC (see a. iii above) applies. If the Personal Information in question relates to the business of the Japanese branch it would be prudent to treat it as "obtained by activities of the Japanese branch" under b. above.

Whether a Japanese company and its foreign branch are a single legal entity would be determined in accordance with the laws of the jurisdiction under which the branch was formed.

13.8 Transfer of Personal Data to a third party in a foreign country

The transfer by a PIC of Personal Data to a third party (including a party which is deemed not to be a third party (see Section 13.6 above)) in a foreign country (other than in reliance on one of the exceptions listed above under 'transfers permitted by law') is subject to the following requirements in addition to those generally applicable to transfers of Personal Data:

- where consent to the transfer is given by the Data Subject, it must be clear it covers the transfer to a third party in a foreign country and the Data Subject must be provided, when giving the consent, with information necessary for judging whether to provide the consent (e.g. the foreign country is identified or identifiable or the circumstances where such data transfer will be made have been clarified); or
- in the absence of such consent, if the transferor wishes to rely on an Opt-Out or the fact that the transferee is not to a third party as an exception to the requirement to obtain the Data Subject's consent to the transfer, it is also necessary that the transferee:
    - is in a country on a list of countries issued by the PPC as having a data protection regime equivalent to that under the APPI; or
    - implements data protection standards equivalent to those which PICs subject to the APPI must follow.

At the date of this note only the UK and countries in the European Union (including the EEA) are on the list of countries issued by the PPC as having equivalent data protection. If the country of the transferee is not such a country, a transferor PIC would have to rely on the transferee implementing equivalent standards to the APPI in order to effect a transfer of Personal Information offshore without the Data Subject's consent or in reliance on an exception listed above in transfers permitted by law. The requirement for equivalent standards to the APPI can be satisfied:

- if the transferee is accredited under APEC's CBPR system; or
- by the transferor and the transferee:
    - entering into a contract; or
    - if they are in the same corporate group, both being subject to binding standards of the group for the handling of Personal Data; pursuant to which the transferee is subject to all the obligations imposed by the APPI on PICs who are subject to it, and which must include certain specified matters, such as purpose of use, record-keeping and details of security measures.

[2020 Amendments:

When transferring Personal Data to a third party offshore:

- *If the transfer is on the ground of the Data Subject's consent to the cross-border transfer, the transferor must provide the Data Subject with certain information regarding the protection levels of the data protection law of the foreign country; the information required will be set out in more detail in regulations to be issued by the PPC.*

- *If the transfer is allowed without the Data Subject's consent because the transferee has established a level of protection of Personal Data equivalent to that under the APPI, the transferor must (a) continue ensuring the transferee maintains that protection level and (b) provide the Data Subject with information of such protection level if requested by the Data Subject.]*

13.9 Transfer due diligence and records

A transfer of Personal Data now requires that the transferor PIC and the transferee (if a PIC, or if it becomes a PIC as a result of the transfer) keep specified records and the transferee is also required to make enquiries on the source of the Personal Data transferred, unless the transfer was made in reliance on an exception listed above as a transfer permitted by law or the transferee is not a third party.

The transferor must keep a record of:

- (if the transfer was made in reliance on an Opt-Out) the transfer date;
- the name or other identifier of the transferee and the Data Subject, and the type(s) of data transferred (e.g. name, age, gender); and
- the Data Subject's consent to the transfer, or, if the consent has not been obtained and the transfer was made in reliance on an Opt-Out, that fact.

The transferee must keep a record of:

- (if the transfer was made in reliance on an opt-out) the date it received the Personal Data;
- the name or other identifier of the transferor and its address (and the name of its representative if the transferor is a legal entity), and the name of the Data Subject;
- the type(s) of data transferred;
- the Data Subject's consent to the transfer, or, if the consent has not been obtained and if the transfer was made in reliance on an Opt-Out, that fact;
- if an Opt-Out has been relied on, the fact that the Opt-Out has been filed with, and published by, the PPC; and
- must ascertain and keep a record of how the transferor acquired the Personal Information transferred.

14. EMPLOYMENT

An employer is required by the Industrial Safety and Health Act to engage a medical professional to conduct certain medical check-ups of their employees. It is generally understood that the medical professional is a PIC, rather than a Personal Information/Data Processor for the employer as PIC, in connection with the diagnosis information they obtain from the medical check-up; in most cases the medical professional should share with the employer the legally mandatory medical check-up information of the employees, and the sharing is generally permitted without the employees' consent as an exception to the general rule that the Data Subject's consent is required for the transfer and acquisition of Sensitive Information as it is required by law. The MHLW's guidelines require an employer not to handle such diagnosis information beyond the scope necessary for the purpose of ensuring the employees' health.

15. MY NUMBER ACT - SOCIAL SECURITY NUMBERS

15.1 Background

The My Number Act introduced a national social security ID number system for all individuals resident in Japan (whether Japanese or foreign) under which they are allocated a unique individual number (**'Personal Number'** also known as **'My Number'**). An individual's Specific Personal Information (Personal Information containing a My Number) is regarded as their confidential private information and its handling is subject to stringent regulation under the My Number Act. The My Number Act regime is entirely separate from the APPI.

My Numbers are used, amongst other things, to track income, social security, taxes, welfare and benefits, and will be required by public bodies when dealing with annual tasks, such as tax filings, as specified by the My Number Act and related guidelines (together **'Specified Purposes'**).

All employers will need to collect their employees' Specific Personal Information (which may, in relation to filing of certain social security documents, need to include those of employees' dependents), as they will be used in documentation when the employer files certain tax/social security documents for their employees with administrative offices, such as tax and pension offices.

15.2 Transfers and outsourcing

The rules and exceptions that permit disclosure and transfer of an individual's Personal Data under the APPI do not apply to disclosure of Specific Personal Information.

The My Number Act and related guidelines require an employer to:

- not share an employee's Specific Personal Information with any other person or entity, including any affiliate of the employer, even with the employee's consent (with certain limited exceptions), except a third party engaged by the employer to provide services for Specified Purposes (e.g. tax accountants, data managing service providers) (a **'Contracted Third Party'**); and
- establish appropriate supervision over any Contracted Third Party.

In practical terms an employer should:

- if it provides employee information to a third party other than a Contracted Third Party, ensure that the information transferred does not include My Numbers; and
- if Specific Personal Information is transferred to a Contracted Third Party, ensure that the transferee has appropriate systems in place for protection of the confidentiality of the Specific Personal Information and that the Specific Personal Information is only used for a Specified Purpose.

15.3 Use

According to the My Number Act and related guidelines an employer must:

- not obtain, store or use an employee's Specific Personal Information for any purpose other than a Specified Purpose; and
- conduct identity verification of each employee (e.g. checking the employee's My Number card) as required by the My Number Act when obtaining the employee's Specific Personal Information.

In practical terms the employer should:

- make sure the purpose of use of Specific Personal Information as notified or made available to employees is limited to Specified Purposes, in particular if the employer provides a broader scope of purpose of utilisation of Personal Information in its existing privacy policy; and
- establish specific rules for the collection of Specific Personal Information, including an identification process.

Banks, securities firms and insurance companies may also request their customers to provide Specific Personal Information. The regulations under the My Number Act described above equally apply to such financial institutions' handling Specific Personal Information.

15.4 Storage & security

The My Number Act and related guidelines require an employer to establish appropriate systems for the secure storage and handling of Specific Personal Information.
In practical terms the employer should:

- draft/amend internal rules on data protection to ensure the handling of Specific Personal Information in accordance with the My Number Act;
- ensure employees handling Specific Personal Information are aware of the restrictions on their use and the scope of the related data protection regime, in particular the areas where the obligations are stricter than those currently generally implemented by the employer for data protection; and
- ensure its data protection systems are adequate to comply with the obligations under the My Number Act as they are likely to be stricter than under the employer's other data protection obligations (whether under the APPI or otherwise).

15.5 Reporting of losses

Any loss of any Specific Personal Information must be reported to the PPC, though there is no specified deadline for giving the notification; the form of the report is slightly different from that for other data losses. The system for escalation of remedial orders by the PPC is the same as that for losses of other Personal Information, though failure to comply with an order for improvement could lead to more serious criminal sanctions against both the data controller and any of its officers responsible for the loss. Notification to the affected Data Subjects is still only desirable.

For further information please contact:

(Mr) Ryuichi Nozaki
Partner*
E: ryuichi.nozakai@aplaw.jp

Daniel C. Hounslow
Consultant**
E: daniel.hounslow@aplaw.jp

* Attorney (Bengoshi), Japan
** Mr. Hounslow is not registered in Japan as gaikokuho-jimu-bengoshi and neither practices law nor acts as an intermediary of legal matters on any laws in Japan; he does not practice law or advise on English or any other law in the UK or elsewhere. Neither Atsumi & Sakai LPC nor Atsumi & Sakai Europe Limited is regulated by the Solicitors Regulation Authority for England and Wales.

September 2020

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm with a dynamic and innovative approach to legal practice; it has been responsible for a number of ground-breaking financial deal structures and was the first Japanese law firm to create a foreign law joint venture and so admit foreign lawyers as full partners. Expanding from its highly regarded finance practice, the firm now acts for a wide range of international and domestic companies, banks, financial institutions and other businesses, offering a comprehensive range of legal expertise.

Atsumi & Sakai has an outward-looking approach to its international practice, and has several foreign partners and other lawyers with extensive experience from leading international law firms, so providing its clients with the benefit of both Japanese law expertise and real international experience. As the only independent Japanese law firm with a London office, it can also provide real-time advice on Japanese law to its clients in Europe, the Middle East and Africa, as well as providing a more convenient service to its clients in the Americas.

Atsumi & Sakai

www.aplaw.jp/en/

Tokyo Office: Fukoku Seimei Bldg., 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan

London Office: 4th Floor, 50 Mark Lane, London EC3R 7QR, United Kingdom

Frankfurt Affiliate Office: OpernTurm (13F) Bockenheimer Landstraße 2-4, 60306 Frankfurt am Main, Germany

---