Atsumi & Sakai

MAJOR REVISIONS TO JAPAN'S PERSONAL INFORMATION PROTECTION REGIME EFFECTIVE FROM 30TH MAY 2017

- Abolition of the De Minimis Exemption
- New Requirements for Cross-border Data Transfers
- Extraterritorial Application Expanded
- Additional Categories of Personal Information
- New Reporting and Filing Obligations
- Rules for Sensitive and Anonymised Information

January 2017

SUMMARY

Amendments to Japan's Act on Protection of Personal Information ("APPI") ("Amendments") were passed by the Diet on 3rd September 2015; some provisions, mainly those establishing and governing the Personal Information Protection Commission ("Commission"), are in force, and it has now been announced that the remaining provisions will be implemented on 30th May 2017 ("Implementation Date"), though regulations and guidelines setting out the precise scope of some of the revisions have yet to be issued by the Commission. The Amendments are likely to have a significant impact on companies holding personal information in Japan[1],[2], and expand the extraterritorial application of the APPI.

This note provides a general guide to the Amendments to help companies which may be affected by them to plan for the new regime.

BACKGROUND

The protection of personal information[3] in Japan is regulated under the APPI and numerous subsidiary regulations and guidelines. The Amendments update and enhance the APPI regime to address recent and anticipated technological and business developments in the use and storage of personal information, and, in particular, the use of "Big Data" and data transfers.

The Amendments will be supplemented and clarified by guidelines and regulations from the Commission and relevant ministries and regulators. Guidelines already issued by the Commission 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 will not expand or limit the scope of the APPI; the guidelines also make it clear that a breach of a guideline which is expressed as an obligation, rather than a recommendation, would be deemed a breach of the APPI. The guidelines are not comprehensive, and additional guidelines may be issued for businesses and industries where there is a need for more stringent protection of personal information[4].

MAIN AREAS COVERED BY THE AMENDMENTS

1. Abolition of the "5,000 persons" Exemption
2. Expansion of the Scope of "Personal Information"
3. Acquisition and Transfer of Sensitive Personal Information
4. Due Diligence and Transfer Records
5. Transfer of Personal Information in Reliance on Opt-out Provisions
6. Transfer of Personal Information Offshore
7. Extraterritorial Application of the APPI
8. Reporting of Data Leakages
9. Creation and Use of Anonymised Information
10. Enforcement of the Correction and Deletion of Personal Information
11. Criminal Liability for Data Theft
12. Filing and Publication of Opt-out Provisions
13. Investigatory Powers
14. Data Protection Officers

---

1. Abolition of the "5,000 persons" Exemption

The most important change likely to affect foreign companies with Japanese subsidiaries or branches is the abolition of the "5,000 persons" exemption rule (sometimes referred to as the "small enterprise rule") which, put broadly, exempts data controllers[5] which hold the personal information of not more than 5,000 individuals ("data subjects") from the application of the APPI; the abolition of the rule is

---

[1] *The Amendments do not affect the separate, and more stringent, data protection regime applicable to the use and storage of "My Number" personal identification numbers (used for tax, social security and similar matters) which applies to all holders of such numbers, without exception.*

[2] *Industry-based regulatory guidelines on data protection (e.g. guidelines issued jointly by the Commission and the Financial Services Agency) may also apply in certain cases.*

[3] *Put broadly, "personal information" means information which can identify an individual on its own, or in combination with, or by reference to other information.*

[4] *Draft industry-sector regulatory guidelines published to date do not materially deviate from those already in force.*

[5] *A business operator, whether an individual or an entity, using a database (electronic or otherwise) of personal information in its business.*

expected to bring a significant number of companies (both domestic companies and foreign companies with branches, or operating a business, in Japan) into the scope of the APPI regime. Although regulations published by the Commission to date do not include alternative exemptions for those holding small amounts of personal information, they do provide examples of security measures feasible for "small size data controllers"[6] and which they would be expected to adopt as appropriate in their circumstances for the protection of personal data they hold; such "feasible measures" include:

a) establishing basic rules on data collection, use, storage, etc.;
b) distinguishing between persons who have data handling, use, etc. responsibilities and those who do not;
c) appointment of a person responsible for checking the status of data handling, etc.;
d) any feasible measures to prevent unauthorised access to data;
e) keeping computer operating systems up-to-date and installing security software; and
f) establishing staff rules for reporting data leakages to those responsible for handling them.

It is vital that any company which is currently outside of the scope of the APPI regime through the application of the 5,000 persons exemption promptly take steps to ensure it will comply with the requirements of the regime from the Implementation Date.

2. Expansion of the Scope of "Personal Information"

The scope of what constitutes personal information subject to the APPI regime has been expanded to include:

"Personal Identifier Codes", which include:

a) characters, numbers, symbols and/or other codes for computer use which represent certain specified personal physical characteristics (such as DNA sequences, facial appearance, iris patterns[7], vocalisations[8], posture and walking movements, finger and palm prints, and vein patterns) and which are sufficient to identify a specific individual;
b) certain identifier numbers[9], such as those on passports, driver's licenses and resident's cards, and the 'My Number' individual social security ID numbers;
c) certain unique characters, numbers, symbols and other codes that are assigned to, and stated on, health and care insurance cards; and
d) any characters, numbers, symbols and other codes from time-to-time designated by the Commission as being equivalent to any of the items above; and

"Sensitive Personal Information"[10], which includes personal information relating to matters such as race[11], creed, religion, physical or mental disabilities, medical records[12], medical and pharmacological treatment[13], and arrest, detention or criminal proceedings (whether as an adult or a juvenile)[14] or criminal victimisation.

3. Acquisition and Transfer of Sensitive Personal Information

A data controller must obtain the prior consent[15] of a data subject before acquiring sensitive personal information of the data subject unless one of the exceptions to the consent requirement ("General Exceptions")[16] applies.

---

[6] A data controller with not more than 100 long-term employees, excluding data controllers (i) which have held personal information of more than 5,000 individuals on any date during the 6-month period ending on the date of the determination, or (ii) contracted by a third-party data controller to perform data-handling services.

[7] A retina scan is not currently a "Personal Identifier Code".

[8] These must be physical characteristics, such as vibration of the vocal cords, or a change of shape of the vocal tract. A voice recording is not a "Personal Identifier Code", though would be if it could be used in combination with other information to identify a specific individual.

[9] Phone numbers, email addresses and credit card numbers are not "Personal Identifier Codes", though would be "Personal Information" if they can be used in combination with other information to identify a specific individual. Credit card numbers are subject to separate protection under financial regulations on credit card businesses.

[10] A data controller may also be subject to industry-based regulatory guidelines which separately define and regulate the use of "sensitive information" in that industry (e.g. guidelines issued jointly by the Commission and the Financial Services Agency); unless varied by the relevant regulator, these requirements will continue to apply after the Implementation Date and to the extent they are more restrictive than those introduced by the Amendments.

[11] Nationality is not "Sensitive Personal Information".

[12] Any result of a medical check, even that a person is "normal" or "healthy", or observed data supporting the result, is "Sensitive Personal Information".

[13] Elderly care is not "Sensitive Personal Information" because it may need to be shared in local communities.

[14] The fact that a person is a member of so-called anti-social forces, such as criminal groups, is not "Sensitive Personal Information", though any criminal proceedings against such a person is.

[15] A consent required by the APPI may be in any manner "which is regarded reasonable and appropriate as a means necessary for the data subject to decide to provide the consent"; examples include (i) oral expression, (ii) in writing, (iii) email, (iv) check a box, (v) click a button on a webpage, and (vi) touch a panel, push button or switch. Industry-sector guidelines may have more stringent requirements.

[16] The principal exceptions are when (i) the acquisition is required or authorised by Japanese law, (ii) the acquisition is necessary to protect a person's life, body or property, and obtaining the consent is difficult, and (iii) the information in question has been made public by the data subject, the government or certain

A transfer of sensitive personal information will require the consent of the data subject unless a General Exception applies or it is to a person or entity which is not regarded as a third party for the purpose of transfers of personal information[17] ("Related Party Exception"); although a data controller may, in certain circumstances, transfer personal information without the data subject's consent by relying on an "opt-out" provision[18] ("Opt-out Exception"), it may not do so for a transfer of sensitive personal information.

4. Due Diligence and Transfer Records

From the Implementation Date, a transfer of personal information will require that the transferor data controller and the transferee (if a data controller, or if it becomes a data controller as a result of the transfer) to keep specified records, and the transferee will also be required to make enquiries on the source of the personal information transferred, in either case unless the transfer was made in reliance on a General Exception or a Related Party Exception.

a) The transferor must keep a record of:
   i. (if the transfer was made in reliance on the Opt-out Exception) the transfer date;
   ii. 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
   iii. the data subject's consent to the transfer, or, if the consent has not been obtained and the transfer was made in reliance on the Opt-out Exception, that fact; and

b) The transferee must keep a record of:
   i. (if the transfer was made in reliance on the Opt-out Exception) the date it received the personal information;
   ii. 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;
   iii. the type(s) of data transferred;
   iv. 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 the opt-out exception, that fact; and
   v. if the Opt-out Exception has been relied on, the fact that the opt-out has been filed with, and published by, the Commission,

   and must ascertain and keep a record of how the transferor acquired the personal information transferred.

The transfer records must be kept for a period from time-to-time specified by the Commission; the retention period is currently generally three years.

5. Transfer of Personal Information in Reliance on Opt-out Provisions

Under the revised APPI there must be "a period necessary for the data subject to exercise its opt-out rights" from the time when the opt-out provision was notified to, or became readily accessible to[19] the data subject and before the start of a data transfer relying on the opt-out provision. Commission guidelines only say that how long the period should be will vary depending on factors such as the nature of business, how close the data subjects are to the data controller, the nature of the personal information to be transferred, and how quickly the data controller can handle the data subject's exercise of its opt-out rights.

---

exempted persons (such as broadcasting institutions); items (i) and (ii) are also General Exceptions to the requirement to obtain a data subject's consent to a transfer of its personal information.

[17] A transferee is deemed not to be a "third party" for the purpose of the APPI when (i) the transferee is engaged under a contract with the transferor to provide a data handling service on the transferor's behalf and personal information is transferred (entrusted) to the transferee for the purpose, (ii) personal information is provided as the result of a merger or other business succession and it is only used for its original purpose of use, or (iii) the transferor and the transferee are "joint users" of personal information; consent to such transfers is not required because the APPI generally only requires the data subject's consent for transfers to a "third party".

Though not a Related Party Exception, a transfer of personal information between a Japanese company and its Japanese branch, or between a foreign company and its Japanese branch are not transfers of personal information as in each case the branch and the company are the same legal entity; 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.

[18] The data subject has been informed by a data controller of a proposed transfer of the data subject's personal information to a third party and given the opportunity to object to the transfer but has not done so within a specified period (see section 5. below regarding timing); the data controller may then make the transfer.

[19] This could include publication on a public website or other media accessible by the public, or in terms of business provided to the data subject or publicly available. Publication of an opt-out provision by the Commission (see section 12 below) satisfies the requirement that it be "readily accessible".

6. Transfer of Personal Information Offshore

From the Implementation Date, the transfer by a data controller of personal information to a third party[20] in a foreign country (other than in reliance on a General Exception) will be subject to the following requirements in addition to those currently generally applicable to such transfers:

a) 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[21]; and
b) in the absence of such consent, if the transferor wishes to rely on the Opt-out Exception or the Related Party Exception to the requirement to obtain the data subject's consent to the transfer, it will also be necessary that the transferee:
    i. is in a country on a list of countries issued by the Commission as having a data protection regime equivalent to that under the APPI; or
    ii. implements data protection standards equivalent to those which data controllers subject to the APPI must follow.

The Commission has yet to issue the list of countries, so until it is issued, or if, when it is issued, the country of the transferee is not on it, a transferor data controller would have to rely on b) ii. in order to effect a transfer of personal information offshore without the data subject's consent or in reliance on a General Exception Commission guidelines; b) ii. can be satisfied:

c) by the transferor and the transferee:
    i. entering into a contract; or
    ii. if they are in the same corporate group, both being subject to binding standards of the group for the handling of personal information,

    pursuant to which the transferee is subject to all the obligations imposed by the APPI on data controllers who are subject to it, and which must include certain specified matters, such as purpose of use, record-keeping and details of security measures; or
d) if the transferee is accredited under APEC's CBPR system[22].

7. Extraterritorial Application of the APPI

From the Implementation Date, an offshore data controller which is not already subject to the APPI regime[23] and which acquires personal information of data subjects in Japan for the purpose of it supplying goods or services to those persons will be subject to the APPI even if it does not handle any personal information in Japan.

Although the Commission cannot enforce its orders for compliance with the APPI, etc. against such an offshore data controller, it may provide information to foreign regulatory authorities for their own regulatory enforcement purposes, and it would therefore be prudent for the offshore data controller to have the operation of its personal information and privacy policies reviewed to ensure that they comply with the revised APPI regime.

If an offshore data controller is subject to the APPI, it will be required to file any opt-out provisions[24] with the Commission for review and publication[25]. When making the filing, the offshore data controller must also notify the Commission of its agent in Japan appointed and authorised to act on its behalf in respect of the filing (i.e., communicate with the Commission); a Japanese lawyer or corporation-type law firm can act as such an agent.

8. Reporting of Data Leakages

A draft of general guidelines concerning the handling of data leakages has been published by the Commission for public comment; it is not expected that the guidelines will be materially revised before being implemented. The draft states that in the event of the leakage, destruction or damage of personal information, the leakage of descriptions or personal identifier codes[26] which have been removed from

---

[20] *See the second part of footnote 17.*
[21] *For example, it refers to or can identify (from the data subject's view) the specific foreign country or specifies the situations where data is to be transferred to a third party in such a foreign country.*
[22] (http://www.cbprs.org/GeneralPages/About.aspx; *currently, only the US, Japan, Canada and Mexico have joined the framework.*
[23] *Currently, a foreign entity may fall within the scope of the APPI if it handles personal information in Japan e.g., it has a branch in Japan, or operates a business in Japan, which handles personal information in Japan.*
[24] *It is arguable that the opt-out provision need only be filed to the extent it affects data subjects in Japan, but the Commission has yet to issue guidance on the point.*
[25] *See section 12 below.*
[26] *See section 2 above.*

personal information in the process of creating Anonymised Information[27], or the likelihood of any of the foregoing, it is "desirable" that the affected data controller take the following steps[28]:

a) reporting of the incident within the data controller;
b) taking measures to prevent expansion/aggravation of any damage (to data subjects or third parties affected by the incident) due to the incident;
c) investigation of relevant facts and the cause of the incident;
d) identification of the affected areas within the servers/systems of the data controller and of the data subjects whose data was affected;
e) planning and implementation of measures to prevent the recurrence of the incident that may otherwise occur due to the cause of the incident in question;
f) notice to data subjects potentially affected (depending on the facts of each case);
g) public announcement of the relevant facts and measures to be taken to prevent recurrence of incident (depending on the facts of each case); and
h) (if required) reporting the incident to the Commission[29].

9. Creation and Use of Anonymised Information

Given the rapid expansion of the use of "big data", the Amendments introduce the concepts "Anonymised Information" (in summary, information regarding an individual which has been modified so that it cannot be used to identify the individual) and "Anonymised Information Controller" (a business operator which uses in its business a database (electronic or otherwise) of Anonymised Information that allows easy retrieval of specific Anonymised Information), and requirements for handling Anonymised Information by a data controller or an Anonymised Information Controller.

A data controller which creates Anonymised Information[30] may not disclose its methods for anonymisation of the subject personal information, the data removed in the anonymisation process or any process used to verify the anonymisation; the recipient of the Anonymised Information may not seek to acquire any such information, whether from the transferor or otherwise.

When a data controller 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 will be able to make enquiries with the data controller[31].

Anonymised Information may be transferred to a third party without the consent of the original data subject (it no longer constitutes "personal information"[32]), 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.

10. Enforcement of the Correction and Deletion of Personal Information

Although the current APPI regime gives a data subject the right to require a data controller to correct, delete or cease to use, etc. its personal information[33], it does not provide a mechanism for the data subject to enforce those rights. From the Implementation Date, a data subject may enforce these rights by civil action if such a request is not complied with within two weeks of being made.

In addition, when personal information is no longer needed for its specified purpose, the data controller must make efforts to delete it.

11. Criminal Liability for Data Theft

Improperly using or disclosing personal information for gain will constitute a crime, and the current or former directors or employees of a data controller who disclose all or part of a personal information

---

[27] *See section 9 below.*
[28] *Some industry-based guidelines (e.g. in the financial services sector) provide more detailed, and more stringent procedures for handling data leakages.*
[29] *Reporting is not necessary in certain limited circumstances (such as when the leaked data has been strongly encrypted, all leaked data has been recovered before being seen by any third parties, the data leakage is minor, etc.). The reporting of data leakages may also be subject to industry-based regulation which may impose stricter requirements (e.g. in the financial services sector).*
[30] *It is not clear from the legislation whether the anonymisation of personal information requires the consent of the data subject if it is not within the scope of use of the information which the data subject has consented to; the prudent view is to seek the data subject's consent in such a case.*
[31] *The legislation does not expand on the nature of the enquiries or their possible consequences.*
[32] *See footnote 2.*
[33] *The data controller may refuse the request in certain circumstances, e.g. if unreasonable or costly to implement.*

database, etc. (including a copy or a processed version) which they handled in the course of their duties for improper gain of any person or entity, or steals all or part of such a database (whether for gain or not), is liable to imprisonment for up to one year or to a fine of not more than JPY500,000; if the person committed the crime in the course of the business of a corporate entity (whether the data controller or a third party), the entity may also be liable to a fine of not more than JPY500,000, even if not at fault.

12. Filing and Publication of Opt-out Provisions

A data controller which wishes to use the Opt-out Exception[34] for disclosure of personal information to a third party must file the opt-out provision (but not the rest of its privacy policies) with the Commission[35], which will publish it on the Commission's website[36]. An opt-out provision will not be effective until filed with the Commission, though it is likely that the Commission will only regard an opt-out provision as having been filed when it is satisfied that all relevant information has been provided.

The Commission will start accepting the filing of opt-out provisions from 1st March 2017.

13. Investigatory Powers

The Commission will have powers to investigate data compliance and practices, including on-site inspections and the right to require the production of documents; it may also delegate certain of its investigatory powers to competent ministers (who may sub-delegate in some cases, e.g. to regulators). The extent to which the Commission will use or delegate its authority is not yet clear, though it is possible that in practice ministers (and regulators, etc. to whom they delegate) will continue to exercise authority over the protection of personal information in their respective industries in much the same manner as they do now.

14. Data Protection Officers

Neither the current APPI nor the Amendments specifically require a data controller to appoint a data protection or similar officer[37]. However, guidelines issued by the Commission and which apply to all data controllers provide that a data controller "must" take security measures for the handling of personal information; examples of such a security measure in the guidelines include "appointment of a person in charge of the handling of personal information and the definition of the responsibilities of the person". The guidelines state that whether "examples" 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 nature and volume of data handled). Data controllers who do not have a data protection or similar officer should therefore evaluate their data protection management to consider whether to appoint one, and take advice where not certain.

For further information on these matters, please contact:

Daniel C. Hounslow
Solicitor, England & Wales
Consultant (UK) to Atsumi & Sakai, Tokyo
E: daniel.hounslow@aplaw.jp

Bonnie Dixon
Attorney, New York
Partner, Atsumi & Sakai
E: bonnie.dixon@aplaw.jp

---

[34] *See section 3 above and footnote 17.*
[35] *The Commission has published a form for the filing (in Japanese) - Pages 11 to 13 (exhibit form No.1) of the Ordinance for Enforcement of the APPI: http://www.ppc.go.jp/files/pdf/290530_personal_commissionrules.pdf*
[36] *https://www.ppc.go.jp/*
[37] *A data controller may also be subject to industry-based regulatory guidelines which impose obligations regarding the appointment of a data protection or similar officer.*

This memorandum was prepared by Japanese lawyers (Bengoshi) at Atsumi & Sakai and is provided as a general guide only; it does not constitute, and should not be relied on as constituting legal advice. Please see notice 2. below regarding any subsequent Japanese law advice.

Atsumi & Sakai
www.aplaw.jp

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

January 2017