Atsumi & Sakai
TOKYO | LONDON | FRANKFURT

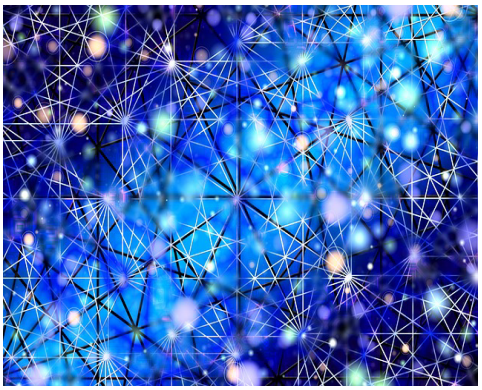
Newsletter

About us

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm. The firm operates as a foreign law joint venture, combining a comprehensive Japanese-law practice with a team of foreign partners and lawyers from major international law firms to provide its clients with the benefit of both Japanese law expertise and real international experience. 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.

REVISIONS TO JAPAN' S PERSONAL INFORMATION PROTECTION ACT

April 2015 No.A&S(Eng)_002



A bill to amend Japan' s Act on Protection of Personal Information (the "Act") (the "Bill") was submitted to the Diet on 10 March 2015; when enacted, the amendments will significantly revise the Act and modernise Japanese regulation of handling personal information.
This note sets out a brief overview of the principal amendments to the Act as set out in the Bill.

A. PRINCIPAL AMENDMENTS

1. Clarification of "Personal Information"
2. Extraterritorial Application
3. New Watchdog Committee
4. Obtaining Sensitive Information
5. Restrictions on Disclosure to Third Parties
6. New Measures for Traceability
7. "Big Data" Businesses and Anonymisatione attractive to Japanese investors, though foreign platform providers should consider the cost of compliance with these requirements (in particular the cost of due diligence, which could be substantial) when considering raising funds in Japan, and bear in mind that they are likely to be required to have a business presence in Japan in order to make an offering of securities.

B. OVERVIEW OF PRINCIPAL AMENDMENTS

1. Clarification of "Personal Information"

The Act regulates the handling of "Personal Information" (information about a living individual (a "Data Subject") from which the identity of the individual can be ascertained (including by easy reference to other information)) and the Bill clarifies the term as including biometric data and any identification code provided to an individual for the use of services or purchase of goods.
The terms "Personal Data" (Personal Information contained in a Personal Information Database), "Personal Information Database" (a database (electronic or not) that enables easy retrieval of Personal Information contained in it), and "Personal Information Controller" (a business operator using a Personal Information Database for its business) (below a "PIC") remain generally unchanged by the Bill.

2. Extraterritorial Application

The Bill clarifies that certain provisions of the Act apply 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 handles that Personal Information, or any Anonymised Information (see B.7.) created from it, in a foreign country. The obligations which will apply exterritorialy include:
- to specify and notify or publicise the purpose of use of the Personal Information, and to use it within that purpose;
- to keep Personal Data accurate and up-to-date, and to delete it when no longer required (see B.8.2.);
- to take measures to protect data against leakage, etc.;
- to supervise employees handling Personal Information and any service provider entrusted with the handling of Personal Data (see B.5.4.);
- the rules governing disclosure to a third party (see B.5.);
- 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 (see B.7.).

Whilst the Committee (see B.3.) can only render "advice" to a PIC based overseas, it may provide information to foreign regulatory authorities for their own regulatory enforcement purposes, and it would therefore be prudent for any such company to have the operation of its personal information and privacy policies reviewed in order to ensure their compliance with the revisions to the Act before they come into force.

3. New Watchdog Committee

A Personal Information Protection Committee (the "Committee") will be established with the task of ensuring the appropriate handling of Personal Information so as to protect individuals' rights and interests. The Committee members will be appointed by the Prime Minister with the consent of the Diet, though will be independent of government.

The Committee will assume the investigatory, advisory and enforcement powers which are currently exercised under the Act by responsible ministries, including the power to investigate the activities of a PIC (and an Anonymised Information Controller (see B.7.)), and in certain instances to render advice to, and make orders against, it if the infringement of an individual' s material rights or interests is imminent. Failure to cooperate with any investigation or to comply with an order may render the PIC and any responsible director or employee liable to criminal penalties. The Committee may delegate its investigatory powers to the relevant minister, etc. in limited circumstances, but not its advisory or enforcement powers. The supervisory practices of the Committee and relevant ministers, etc. will be clarified by Cabinet Order in due course.

The Committee will be able to provide information to foreign data protection regulators and in limited circumstances may allow information to be used for criminal investigations overseas.

4. Obtaining Sensitive Information

Currently a PIC may acquire Personal Information by any means except "deception or other wrongful means" ; this basic freedom will remain, but the Bill will prohibit obtaining "Sensitive Information" without the Data Subject' s consent, unless, e.g. necessary for protection of life, body or property of the Data Subject and obtaining its prior consent is difficult. "Sensitive Information" is defined in the Bill as Personal Information containing matters such as a description of the race, beliefs, social status, medical history, or criminal history of the Data Subject; the scope of the term may be revised by Cabinet Order.

5. Disclosure to Third Parties

5.1. Opt-out system

At present a PIC may disclose Personal Data to a third party without the consent of the Data Subject when an "opt-out" provision containing information specified in the Act has been notified or made readily accessible to the Data Subject. In practice opt-out provisions are usually included in privacy policies which PICs make available to the public. The Bill retains the opt-out system, but adds restrictions on its use.

5.2. Filing of Opt-out Provisions

The Bill requires a PIC which wishes to use the opt-out system for disclosure of Personal Data to a third party to file the opt-out provision (but not the rest of its privacy policies) with the Committee, which will then review the provision to ensure it is appropriate in accordance with the requirements of the Act and make it available to the public. If the opt-out is not sufficient in terms of clarity, easy-readability and formality the Committee may require it to be improved and re-filed.
The Bill prohibits the use of the opt-out system for disclosure of "Sensitive Information" (see B.4.), so the Data Subject' s consent will Sgenerally be required for disclosure of such information to a third party.

5.3. Transfers overseas

The Act currently does not have any rules specifically addressing the transfer of Personal Data to a person or entity (whether related to the transferor or not) in a foreign country, though the general restrictions, etc. on the transfer of Personal Data to third parties still apply.
The revisions in the Bill will prohibit use of the opt-out system, reliance on the ability to entrust the handling of Personal Data to a third party (see B.5.4.), and the "joint use" of Personal Data (see B.5.4.) for disclosure of Personal Data to a third party in a foreign country (so the Data Subject' s consent will be generally required for such disclosure) unless:

(i) the foreign country is on a list of countries issued from time-to-time by the Committee which it has confirmed as having a data protection regime with a level of protection equivalent to that of Japan; or
(ii) the third party has a system of data protection which meets the standards required for a PIC under the Act, as to be specified by the Committee.

The cross-border transfer of Personal Data between offices or data centers within the same legal entity will not be subject to these rules, but the various parts of the legal entity from and to which Personal Data is transferred must have safety measures in place for the protection of Personal Information as generally required by the Act.

Following the revisions, the transfer of Personal Data overseas between different legal persons within the same corporate group, which is now generally possible without the Data Subject' s consent by using the "joint use" exemption, will need the Data Subject' s consent unless the requirements at either (i) or (ii) are met.

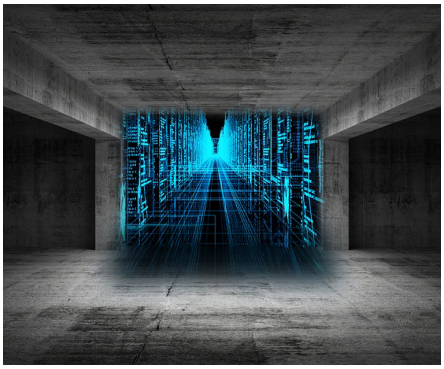
5.4. Permitted disclosures not changed by the Bill

Except as noted in B.5.3., the disclosure of Personal Data to a third party without the Data Subject' s consent in certain circumstances, including the cases below, as currently permitted by the Act, will not be changed by the Bill:
- disclosure required or authorised by law;
- disclosure necessary for the protection of life, body or property of a Data Subject where obtaining it' s prior consent is difficult;
- entrusting Personal Data to a service provider (e.g., a cloud computing service provider or a mailing service provider, and providing the Personal Data for that purpose); and
- "joint use" of Personal Data within a group of companies, or between companies providing integrated or affiliated services in each case by including certain related statements in the privacy policy.

6. Traceability Regime

The Bill introduces new requirements for the traceability of Personal Information, in particular a PIC receiving Personal Data from a third party must make enquiries to ascertain the third party' s name and address, the identity of its representative, and how it obtained the Personal Data; a record of the enquiries and the answers received must be kept. When disclosing Personal Data to a third party a PIC must create and keep a record of the date of disclosure, the third party' s name and certain other matters to be specified by the Committee.

7. "Big Data" Businesses and Anonymisation



The Bill expands the overall purpose of the Act so as to provide guidance for the sound development of anonymised data analysis and its utilisation in business (so-called "big data"), the aim being to provide a regime that will both protect the rights and interests of Data Subjects, and promote the sound development of the big data business. To this end the Bill also introduces 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 using for its business a database (electronic or not) that allows easy retrieval of specific Anonymised Information contained in it), and requirements for handling Anonymised Information by a PIC or an Anonymised Information Controller during and after its creation, and for its transfer to third parties so as to prevent reversion to the original information and identification of the Data Subject, promote transparency and ensure any transferee is aware that the information is anonymised; more detailed standards will be provided in due course by the Committee.

8. Other Noteworthy Amendments

8.1. Changes to the "5,000 individuals" rule

A person or entity which has not handled Personal Information of more than 5,000 individuals at any time in the past six months is currently effectively exempted from the requirements of the Act. The Bill removes this exemption, but enables exemptions to be provided by Cabinet Order where the risk of infringement of individuals' rights and interests is limited.

8.2. Deletion of Redundant Personal Data

The amendments will require the deletion of Personal Data when it is no longer needed for its specified purpose.

8.3. Criminal theft of data

The Bill creates a new criminal offence where an individual who is, or used to be, a director, employee or manager of a PIC provides to a third party or steals a Personal Information Database which she/he handled in relation to the PIC' s business (including a duplicate or modified database) "for the purpose of unjust profit of herself/himself or a third party" .

C. ENACTMENT

It is expected that the Bill will be enacted this year, and then come into force on a date to be specified by Cabinet Order.
More details of the new regime will be set out in Cabinet Order(s), regulatory guidelines, and standards and procedures to be set out by the Committee after its creation.

It is not expected that the Bill will be subject to material revisions, so businesses handling Personal Information should review their data handling practices to see whether any changes are necessary or advisable in light of the revisions set out in the Bill, as described above.

| Author(s)

Ryuichi Nozaki > *View Profile*
Director, Atsumi & Sakai Europe Limted
info_uk@aplaw.jp

Daniel C. Hounslow > *View Profile*
UK Consultant to Atsumi & Sakai, Tokyo
daniel.hounslow@aplaw.jp

| General enquiries:
info@aplaw.jp