GETTING THE DEAL THROUGH

Data Protection & Privacy

in 26 jurisdictions worldwide

2014

Contributing editor: Rosemary P Jay

Published by
Getting the Deal Through
in association with:

Adams & Adams

Arzinger

Coelho Ribeiro e Associados

Com advokatbyrå

Drew & Napier LLC

ELIG, Attorneys-at-Law

Gilbert + Tobin

Heenan Blaikie LLP

Hoffmann Liebs Fritsch & Partner

Hunton & Williams LLP

Ichay & Mullenex Avocats

Iriarte & Asociados

Jayaram & Jayaram

Laux Lawyers, Attorneys-at-Law

Lee and Li, Attorneys-at-Law

Lexing Spain

Lorenz International Lawyers

Matheson

MNKS

Nagashima Ohno & Tsunematsu

Olivares & Cia

Panetta & Associati Studio Legale

Pinheiro Neto Advogados

Preslmayr Rechtsanwälte OG

Yoon & Yang LLC

GETTING THE DEAL THROUGH

Data Protection & Privacy 2014

Contributing editor
Rosemary P Jay
Hunton & Williams

Publisher
Gideon Roberton

Business development managers
Alan Lee
George Ingledew
Dan White

Account manager
Megan Friedman

Trainee account managers
Cady Atkinson, Joseph Rush, Dominique Destrée and Emma Chowdhury

Media coordinator
Parween Bains

Administrative coordinator
Sophie Hickey

Trainee research coordinator
Robin Synnot

Marketing manager (subscriptions)
Rachel Nurse
subscriptions@gettingthedealthrough.com

Head of editorial production
Adam Myers

Production coordinator
Lydia Gerges

Senior production editor
Jonathan Cowie

Subeditor
Davet Hyland

Director
Callum Campbell

Managing director
Richard Davey

Data Protection & Privacy 2014
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Second edition

ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Law Business Research

CONTENTS

Japan

Akemi Suzuki
Nagashima Ohno & Tsunematsu

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The Act on the Protection of Personal Information of 2005 (APPI) sits at the centre of Japan's regime for the protection of PII. The APPI is comprised of two parts – one that sets forth basic policies of the government concerning the protection of PII in Japan, and the other that regulates use of PII by private businesses. Use of PII by the public sector is regulated by separate statutes or local ordinances providing for rules for protection of PII held by governmental authorities.

Serving as a comprehensive, cross-sectoral framework, the APPI regulates private businesses using databases of PII and is generally considered to embody the eight basic principles under the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The APPI is implemented by a number of industry- or sector-specific administrative guidelines compiled by governmental ministries. As of March 2012, as many as 40 administrative guidelines covering 27 sectors exist. Numerous self-regulatory organisations and industry associations have also adopted their own policies or guidelines for the protection of PII.

While the right to privacy is not codified in any statute in Japan, the courts have consistently recognised the notion of a right to privacy derived from the constitutional right to pursue happiness. The privacy right is generally conceptualised by the courts as the right for a person's private life not to be disclosed except for a legitimate reason, and among academics as the right to control his or her personal information for themselves. Due to the lack of a statutory definition, a person's right to privacy could be interpreted to reach beyond the protection afforded to PII under the APPI. Therefore, owners of personal data in Japan should ensure not only compliance with the APPI, but also non-infringement of individuals' privacy rights, when handling personal data, including PII.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

There is no cross-sectoral governmental body that administers the APPI, and different governmental ministries enforce the APPI in the respective sectors and industries that they supervise. Among those ministries, the Ministry of Internal Affairs and Communication and Ministry of Economy, Trade and Industry (METI) tend to take active roles in setting the direction as to the proper utilisation personal data.

Governmental ministries have the following powers under the APPI:

- to require reports from PII data users (as defined in question 9) for their businesses over which the respective ministries have jurisdiction;
- to give advice to PII data users;
- upon breach of certain obligations of any PII data users or PII data owners (as defined in question 9), to 'recommend' cessation or other measures necessary to rectify the violation; and
- if recommended measures are not implemented and the governmental ministry deems imminent danger to an individual's material rights, to 'order' such measures.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Under the APPI, criminal penalties may be imposed if a person:

- fails to comply with any order issued by the competent governmental ministry (subject to penal servitude of six months or less or criminal fine of 300,000 yen or less); or
- fails to submit reports, or submits untrue reports, as required by the competent governmental ministry (subject to criminal fine of 300,000 yen or less).

In addition, if these offences are committed by an officer or employee of a PII data user which is a judicial entity, then the entity itself may also be held liable for a criminal fine.

At the time of writing, however, no criminal penalties have been actually charged pursuant to the APPI since its introduction.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The APPI contains notable exemptions as follows.

- In respect of fundamental constitutional rights, media outlets, universities and other academic institutions, religious groups and political parties are exempt from the APPI to the extent of the processing of personal data for purposes of journalism, academic research and religious and academic activities, respectively.
- Private businesses that have owned PII of less than 5,000 individuals in their electronic or manual database at any time in the past six months are also exempt (small business exception).
- Use of PII for personal purposes is outside the scope of the APPI.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Secrecy of communications from the government's intrusion is a constitutional right. Interception of electronic communication by private persons is regulated by the Telecommunications Business Act of 1984 and the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders of 2001. Marketing e-mails are restricted under the Act on Regulation of Transmission of Specified Electronic Mail of 2002 and the Act on Specified Commercial Transactions of 1976.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Use of personal information by governmental sectors are regulated by the Act on the Protection of Personal Information Held by Administrative Organs of 2003, the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies of 2003 and various local ordinances providing rules for the protection of PII held by local governments. In addition, the Act on Utilization of Numbers to Identify Specific Individuals in Administrative Process, which was approved by the Diet in May 2013, provides rules concerning the use of personal information acquired through the use of the proposed social security and tax numbering system.

7 PII formats

What forms of PII are covered by the law?

In terms of forms of PII, the use of 'database, etc' of PII (PII database) is covered by the APPI. PII database includes not only electronic databases but also manual filing systems that are structured by reference to certain classification criteria so that information on specific individuals is easily searchable.

For purposes of the APPI, PII is defined as information related to a living individual which can identify the specific individual by name, date of birth or other description contained in such information. Information that, by itself, is not personally identifiable but may be easily linked to other information and thereby can be used to identify a specific individual is also regarded as PII. PII comprising a PII database is called PII data.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

Yes, it is widely considered that the APPI does not have extraterritorial application. Separately, PII of individuals residing outside of Japan is considered to be protected under the APPI, as long as such PII is held by private business operators established or operating in Japan.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The APPI distinguishes (i) obligations imposed on all private business operators using PII database (for the purposes of this chapter, called PII data users); and (ii) obligations imposed only on those PII data users who control the relevant PII data (for the purposes of this chapter, called PII data owners). Generally, service providers are subject to the obligations of PII data users but not subject to the obligations of PII data owners.

The obligations of all PII data users mentioned in (i) above include:

- to specify the purposes for which the PII is used and to process the PII only to the extent necessary for achieving such specified purposes (see question 10);
- to notify the relevant individual of, or publicise, the purposes of use (see question 12);
- to not use deceptive or wrongful means in collecting PII (see question 10);
- to undertake necessary and appropriate measures to safeguard the PII data it holds (see question 19);
- to conduct necessary and appropriate supervision over its employees and its service providers who process its PII data (see question 19); and
- to not disclose the PII data to any third party without the consent of the individual (subject to certain exemptions) (see question 29).

In comparison, the obligations of PII data owners mentioned in (ii) above are more stringent, and are imposed only with respect to such PII data for which a PII data user has the right to provide a copy of, modify (correct, add or delete), discontinue using, erase or discontinue disclosure to third parties (retained PII data).

- to make accessible to the relevant individual certain information regarding the retained PII data (see question 12);
- to provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (see question 34):
- to correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon the request of the relevant individual (see question 14);
- to discontinue the use of or erase such retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI (see question 14); and
- to discontinue disclosure of retained PII data to third parties upon the request of the relevant individual if such disclosure is or was made in violation of the APPI (see question 14).

The following are excluded from the retained PII data and therefore do not trigger the above-mentioned obligations of PII data owners:

- any PII data where the existence or absence of such PII data would harm the life, body and property of the relevant individual or a third party; encourage or solicit illegal or unjust acts; jeopardise the safety of Japan and harm the trust or negotiations with other countries or international organisations; or would impede the crime investigations or public safety; and
- any PII data which is to be erased from PII database within six months after it became part of the PII database.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent? Give details.

The APPI does not contain an equivalent set of specific criteria for legitimate data processing as contained in the EU Data Protection Directive. The APPI does, however, prohibit the collection of PII by deceptive or wrongful means, and requires that the purposes of use must be identified as specifically as possible, and must generally be notified or made available to the relevant individual in advance. Processing of PII beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

The APPI does not have special rules for specific types of personal data. Some of the administrative guidelines for the APPI adopted by governmental ministries, however, impose stringent restrictions on the collection, use and disclosure to third parties of certain sensitive data. While there is no formal definition of sensitive data, it is generally considered to encompass political views, religious or similar beliefs, race or ethnic origin, labour union membership, physical and mental health, sex life, criminal records and other discriminatory information.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

There are several notification requirements under the APPI.

First, the APPI requires all PII data users to notify individuals of, or make available to individuals, the purposes for which their PII data is used, promptly after the collection of the PII, unless such purposes was publicised prior to the collection of the PII. Alternatively, such purposes must be expressly stated in writing if collecting PPI provided in writing by the individual directly.

Second, the APPI requires each PII data owner to keep certain information accessible to those individuals whose retained PII data is held. Such information includes: name of the PII data owner; all purposes for which retained PII data held by the PII data owner is used generally; and procedures for submitting a request or filing complaints to the PII data owner. If, based on such information, an individual requests to know the specific purposes of use of his or her retained PII data, the PII data owner is required to notify, without delay, the individual of such purposes.

13 Exemption from notification

When is notice not required (for example, where to give notice would be disproportionate or would undermine another public interest)?

There is an exception to the first notice requirement mentioned in question 12 where, among other circumstances, (i) such notice would harm the interest of the individual or a third party; (ii) such notice would harm the legitimate interest of the PII data user; and (iii) the purposes of use are evident from the context of the acquisition of the relevant PII data.

The exceptions from the second notice requirement mentioned in question 12 are applicable where, in addition to the circumstances mentioned in (i), (ii) and (iii) above, the purposes of use are evident from the information made available to the individual by the PII data owner.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Upon request from an individual, a PII data owner must:

- provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (see question 34);
- correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon request from the relevant individual;
- discontinue the use of or erase the retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI; and
- discontinue disclosure to third parties of retained PII data upon the request of the relevant individual if such disclosure is or was made in violation of the APPI.

An exemption from the third and fourth obligations mentioned above is available where the discontinuance or erasure costs significantly or otherwise imposes hardships and one or more alternative measures to protect the individual's interests are taken.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The APPI requires all PII data users to endeavour to keep the PII data it holds accurate and up-to-date to the extent necessary for the purposes for which the PII data is to be used.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

No. PII data may be held as long as is necessary for the purposes for which it is used.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

PII can generally be used only to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual in a manner mentioned in question 12 above. Use beyond such extent or for any other purpose must, in principle, be legitimised by the consent of the relevant individual.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be reasonably related to the previous purposes. PII may be used for such amended purposes, provided that the amended purposes are notified or made available to the affected individuals.

Exemptions from the purposes for use requirement are applicable to, for instance, the use of PII pursuant to laws, and where use beyond specified purposes is needed to protect life, body and property of an individual and it is difficult to obtain consent of the affected individual.

Security obligations

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The APPI provides that all PII data users must have in place 'necessary and appropriate' measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the PII data they hold or process; and conduct necessary and appropriate supervision over their employees and service providers who process such PII data. What constitute 'necessary and appropriate' security measures are elaborated in many of the administrative guidelines for the APPI. For instance, the administrative guidelines prepared by the METI (METI Guidelines) set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical measures.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

The APPI does not include obligations to notify the regulators or affected individuals of any breaches of security. However, upon the occurrence of any such breach, notification to both the regulator and affected individuals whose data is compromised is generally required or recommended under most administrative guidelines for the APPI. In addition, such guidelines generally recommend or require public announcement of security breach incidents.

Exceptions to such requirement or recommendation vary depending on individual guidelines – the METI Guidelines, for instance, provide that neither notification to the affected individuals nor public announcement is necessary if the lost or disclosed data was protected by advanced encryption or other security enhancing measures and the risk of violation of privacy or other rights of the relevant individuals are nil or very low.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No, there is no legal requirement to appoint a data protection officer. However, the appointment of a 'chief privacy officer' is generally recommended under the METI Guidelines and a number of other administrative guidelines on the APPI. The METI Guidelines do not provide for qualifications, roles or responsibilities of a chief privacy officer.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

PII data users are generally required under applicable administrative guidelines on the APPI to establish internal rules to safeguard the PII data.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

There is no such registration requirement in Japan.

24 Formalities

What are the formalities for registration?

Not applicable.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Not applicable.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

27 Public access

Is the register publicly available? How can it be accessed?

Not applicable.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The APPI prohibits disclosure of PII data to third parties without the relevant individual's consent. As an exception to such prohibition, the transfer of all or part of PII data to persons that provide outsourced processing services is permitted to the extent such services are necessary for achieving the permitted purposes of use. PII data users are required to engage in 'necessary and appropriate' supervision over such service providers in order to safeguard the transferred PII data. Necessary and appropriate supervision by PII data users is generally considered to include proper selection of service providers; entering into a written contract setting forth necessary and appropriate security measures; and collecting necessary reports and information from the service providers.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The APPI provides for important exceptions to the general prohibition on disclosure of PII to a third party without the individual's consent, including:

- disclosure under the 'opt-out' mechanism. A PII data user may disclose PII data to third parties without the individual's consent, provided that it is prepared to cease such disclosure upon request from the individual; and certain information regarding such disclosure is notified, or made easily accessible, to the individual prior to such disclosure;
- transfer in M&A transactions. PII data may be transferred without the consent of the individual in connection with the transfer of business as a result of a merger or other transactions; and
- disclosure for joint use. A PII data user may disclose PII data it holds to a third party for joint use, provided that certain information regarding such joint use is notified, or made easily accessible, to the individual prior to such disclosure. Such disclosure is most typically made when sharing customer information among group companies in order to provide seamless services within the permitted purposes of use. Information required to be notified or made available includes items of PII data to be jointly used, the scope of third parties who would jointly use the PII data, the purpose of use by such third parties, and the name of a party responsible for the control of the PII data in question.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

At present, there are no general restrictions on the ability of a data owner to transfer PII outside Japan.

Update and trends

In May 2013, the Act on Utilisation of Numbers to Identify Specific Individuals in Administrative Process, otherwise known as the My Number Act, passed the Diet. Under this new Act, a unique 12-digit social security and tax number (My Number) will be assigned to each resident in Japan (including non-Japanese citizens) in 2015, and will be available for use from January 2016 onwards.

This Act has met with strong concern regarding the potential mistreatment of personal information gained through My Numbers and the possible invasion of privacy. In light of such concerns, the scope of the permitted use of My Numbers is quite limited under the current Act. As an initial step, My Numbers will be available for use for the purposes of social security, tax and disaster relief operations only. Use of My Numbers in relation to medical, nursing and other industries that deal with sensitive information is set to be reviewed three years after the introduction of the Act.

Further, in order to ensure adequate protection of personal information and privacy, an independent governmental committee will be established to supervise proper handling of personal information gained through My Numbers.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

No, there is no requirement to notify the transfer of PII under the APPI.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Not applicable.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

The APPI does not grant inspection rights to individuals but imposes on PII data owners obligations to respond to individuals' requests for access to their PII data. Specifically, upon request from individuals, PII data owners are obligated to provide, without delay, a copy of retained PII data to the individuals. Such disclosure, however, is exempted as a whole or in part if such disclosure would:

- prejudice life, body, property or other interest of the individual or any third party;
- cause material impedance to proper conduct of the business of the PII owners; or
- result in a violation of other laws.

35 Other rights

Do individuals have other substantive rights?

In addition to the obligations set forth in question 14, PII data owners are subject to an obligation to cease disclosure of PII data to third parties if the relevant individual 'opts out' the third party disclosure.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The APPI does not provide for individuals' right to receive compensation or the PII data users' obligation to compensate individuals upon a breach of the APPI. However, pursuant to the Civil Code of Japan, an individual may bring a tort claim based on the violation of his or her privacy right. Breaches of the APPI by a PII data owner will be a key factor as to whether or not a tortious act existed. If a tort claim is granted, not only actual damages but also emotional distress may be compensated.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals' right to monetary compensation (mentioned in question 36) is enforced through the judicial system. With regard to violations by PII data owners of the obligations described in questions 34 and 35, individuals do not have any statutory right to demand enforcement by the competent governmental ministry. The ministry may, however, recommend PII data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for protection of individuals' rights.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Not applicable.

NAGASHIMA OHNO & TSUNEMATSU

Akemi Suzuki **akemi_suzuki@noandt.com**

Kioicho Building
3-12, Kioicho, Chiyoda-ku
Tokyo 102-0094
Japan

Tel: +81 3 3511 6225
Fax: +81 3 5213 2325
www.noandt.com/en/index.html

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Administrative law in Japan usually provides for an appeal of a governmental ministry's decision to a court with proper jurisdiction. Therefore, if the relevant supervising ministry takes administrative actions against a PII data user, the PII data user will generally be able to challenge the actions judicially.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

See question 3.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

There are no binding rules applicable to the use of 'cookies' or equivalent technology. Any data collected through the use of 'cookies' is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and thereby can identify a specific individual, then the data will constitute personal data subject to the APPI.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Unsolicited marketing by e-mail is regulated principally by the Act on Regulation of Transmission of Specified Electronic Mail. Pursuant to the Act, marketing e-mails can be sent only to a recipient who has 'opted in' to receive them; who has provided the sender with his or her e-mail address in writing (for instance, by providing a business card); who has a business relationship with the sender; or who makes his or her e-mail address available on the internet for business purposes. In addition, the Act requires the senders to allow the recipients to 'opt out.' Marketing e-mails sent from overseas will be subject to this Act as long as they are received in Japan.

Unsolicited telephone marketing is also regulated by different statutes. It is generally prohibited to make marketing calls to a recipient who has previously notified the caller that he or she does not wish to receive such calls.