THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 16

JAPAN

Tomoki Ishiara[1]

I OVERVIEW

In Japan, the Act on the Protection of Personal Information[2] (APPI) primarily handles the protection of data privacy issues. The APPI was drastically amended in 2016 and has been in full force since 30 May 2017. Prior to the amendment, the APPI was applied solely to business operators that have used any personal information database containing details of more than 5,000 persons on any day in the past six months[3] but this requirement was eliminated by the amendment. Under the amended APPI, the Personal Information Protection Commission (PPC) was established as an independent agency whose duties include protecting the rights and interests of individuals while promoting proper and effective use of personal information. Under the amended APPI, the legal framework has been drastically changed and the PPC has primary responsibility for personal information protection policy in Japan. Prior to the amendment, as of July 2015, 39 guidelines for 27 sectors regarding personal information protection were issued by government agencies, including the Ministry of Health, Labour and Welfare,[4] the Japan Financial Services Agency,[5] and the Ministry of Economy, Trade and Industry.[6] Under the amended IPPI, however, the guidelines (the APPI Guidelines)[7] that prescribe in detail the interpretations and practices of the APPI are principally provided by the PPC, with a limited number of special guidelines provided to specific sectors (such as medical and financial ones) by the PPC and the relevant ministries.[8]

---

1 Tomoki Ishiara is counsel at Sidley Austin Nishikawa Foreign Law Joint Enterprise.

2 Act No. 57 of 30 May 2003, enacted on 30 May 2003 except for Chapters 4 to 6 and Articles 2 to 6 of the Supplementary Provisions; completely enacted on 1 April 2005 and amended by Act No. 49 of 2009 and Act No. 65 of 2015: www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

3 Article 2 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003).

4 The Guidelines on Protection of Personal Information in the Employment Management (Announcement No. 357 of 14 May 2012 by the Ministry of Health, Labour and Welfare).

5 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).

6 The Guidelines Targeting Medical and Nursing-Care Sectors Pertaining to the Act on the Protection of Personal Information (Announcement in April 2017 by the PCC and the Ministry of Health, Labour and Welfare).

7 The General Guidelines regarding the Act on the Protection of Personal Information dated November 2017 (partially amended March 2017).

8 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement in February 2017 by the PCC and the Financial Services Agency).

II THE YEAR IN REVIEW

i Background of the amendment to the APPI: Policy Outline of the Institutional Revision for Use of Personal Data (the Policy Outline), and the amendment to the APPI

On 24 June 2014, the government[9] published the Policy Outline,[10] showing the government's direction on the measures to be taken to amend the APPI and the other personal information protection-related laws. The revision bill of the APPI passed the Diet on 3 September 2015 and the amended APPI has been in full force since 30 May 2017. The main changes introduced by the amendment to the APPI are set out below.

Development of a third-party authority system[11]

The government has established an independent agency to serve as a data protection authority to operate ordinances and self-regulation in the private sector to promote the use of personal data. The primary amendments to the previous legal framework are as follows:

a the government has established the structure of the third-party authority ensuring international consistency, so that legal requirements and self-regulation in the private sector are effectively enforced;

b the government has restructured the Specific Personal Information Protection Commission prescribed in the Number Use Act[12] to set up the PPC, the new authority mentioned at (a), for the purpose of promoting a balance between the protection of personal data and effective use of personal data; and

c the third-party authority has the following functions and powers:

- formulation and promotion of basic policy for personal information protection;
- supervision;
- mediation of complaints;
- assessment of specific personal information protection;
- public relations and promotion;
- accreditation of private organisations that process complaints about business operators handling personal information and provide necessary information to such business operators, based on the amended Act on the Protection of Personal Information;
- survey and research the operations stated above at (c); and
- cooperation with data protection authorities in foreign states.[13]

9 Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society.

10 http://japan.kantei.go.jp/policy/it/20140715_2.pdf.

11 The European Commission pointed out the lack of a data protection authority in the Japanese system in its report: Korfe, Brown, et al., 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments' (20 January 2010).

12 Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013). See Section II.ii.

13 Article 61 APPI.

Actions for globalisation

If businesses handling personal data are planning to provide personal data (including personal data provided by overseas businesses and others) to overseas businesses, they have to obtain consent to the transfer from the principal[14] except where:

a no consent is necessary in accordance with the following exceptions to Article 23(1):
- cases based on laws and regulations;
- cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
- cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent; and
- cases in which there is a need to cooperate with a central government organisation or a local government, or a person entrusted by them acting in matters prescribed by laws and regulations,[15] and when there is a possibility that obtaining a principal's consent would interfere with the execution of these duties;

b the overseas businesses establish a system conforming to operating standards prescribed by the PPC rules for overseas businesses to deal with personal information in a manner equivalent to that of a business operator handling personal data pursuant to the provisions of the APPI; and

c the foreign countries in which the overseas businesses are conducted are prescribed by the PPC rules as having established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual's rights and interests.

Framework for promoting the use of personal data (big data issues)

The use of personal data is expected to create innovation with the multidisciplinary utilisation of diverse and vast amounts of data, thereby creating new businesses. However, the system under the previous APPI required consent from principals to use their personal data for purposes other than those specified. Accordingly, providing personal data to third parties was cumbersome for businesses, and created a barrier to the use of personal data, especially launching new business using big data. Under the amended APPI, a business operator handling personal information may produce anonymously processed information (limited to information constituting anonymously processed information databases, etc.) and process personal information in accordance with standards prescribed by the PPC rules such that it is impossible to identify a specific individual from, or de-anonymise, the personal information used for the production.[16] This amendment allows various businesses to share with other businesses the personal data maintained by them, and so develop or foster new business or innovation.

Sensitive personal information

The previous APPI did not define 'sensitive personal information'; however, the amended APPI has defined information regarding an individual's race, creed, social status, criminal record and

14 Article 24 APPI.

15 Article 23 APPI.

16 Article 36(1) APPI.

past record as 'special-care-required personal information' (sensitive personal information), along with any other information that may be the focus of social discrimination.[17] Also, there was no provision that specifically addressed consent requirements for sensitive personal information in the previous APPI; instead these were regulated by a number of guidelines issued by government ministries. The amended APPI, however, explicitly requires that a business operator handling personal information obtain prior consent to acquire sensitive personal information, with certain exceptions.[18]

In addition, the opt-out exception provided under Article 23 does not apply to sensitive personal information and consent to provide such information to third parties is required.[19] The Policy Outline also mentions that in view of the actual use of personal information, including sensitive information, and the purpose of the current law, the government will lay down regulations regarding the handling of personal information, such as providing exceptions where required by laws and ordinances and for the protection of human life, health or assets, as well as enabling personal information to be obtained and handled with the consent of the persons concerned.

Enhancement of the protection of personal information: tractability of obtained personal information

The amended revised APPI:

a imposes obligations on business operators handling personal information to make and keep accurate records for a certain period when they provide third parties with personal information;[20]

b imposes obligations on business operators handling personal information to verify third parties' names and how they obtained personal information upon receipt of personal information from those third parties;[21] and

c establishes criminal liability for providing or stealing personal information with a view to making illegal profits.[22]

ii Social security numbers

The bill on the use of numbers to identify specific individuals in administrative procedures (the Number Use Act, also called the Social Security and Tax Number Act) was enacted on 13 May 2013,[23] and provides for the implementation of a national numbering system for social security and taxation purposes. The government will adopt the social security and tax number system to enhance social security for people who truly need it; to achieve the fair distribution of burdens such as income tax payments; and to develop efficient administration. The former independent supervisory authority called the Specific Personal Information Protection Commission was transformed into the PPC, which was established on 1 January 2016 to handle matters with respect to both the Number Use Act and the

17 Article 1(3) APPI.

18 Article 17(2) APPI.

19 Article 23(2) APPI.

20 Article 25 APPI.

21 Article 26 APPI.

22 Article 83 APPI.

23 The revision bill of the Number Use Act was passed on 3 September 2015. The purpose of this revision was to provide further uses for the numbering system (e.g., management of personal medical history).

amended APPI. This authority consists of one chair and eight commission members.[24] The chair and commissioners were appointed by Japan's prime minister and confirmed by the National Diet. The numbering system fully came into effect on 1 January 2016. Unlike other national ID numbering systems, Japan has not set up a centralised database for the numbers because of concerns about data breaches and privacy.

iii Online direct marketing

Under the Act on Regulation of Transmission of Specified Electronic Mail[25] and the Act on Specified Commercial Transactions,[26] businesses are generally required to provide recipients with an opt-in mechanism, namely to obtain prior consent from each recipient for any marketing messages sent by electronic means. A violation of the opt-in obligation may result in imprisonment, a fine, or both.

iv Reciprocal adequacy decision

On 17 July 2018, Japan released a press release announcing Japan and the European Union (EU) have agreed on reciprocal adequacy of their respective data protection systems. Japan and the EU have long discussed and agreed on reciprocal adequacy on the condition that Japan would implement guidelines (without revising the APPI) to supplement insufficient protections from the EU perspective as follows.

a Information on trade union membership or an individual's sexual orientation[27] shall be regarded as sensitive information in Japan as well as in the EU.

b Personal data that will be deleted within six months[28] shall be protected as personal data.

c The purpose of use of personal information provided by a third party is limited to that originally set by the third party.

d Japan shall ensure the same level of protection as in Japan if personal information coming from the EU is transferred from Japan to non-EU countries.

e For the anonymisation of personal information coming from the EU, the complete deletion of a method of re-identification would be required.[29]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Definitions

Personal information

The amended APPI clarifies the scope of 'personal information' as follows:

24 www.ppc.go.jp/en/aboutus/commission/.

25 Act No. 26 of 17 April 2002.

26 Act No. 57 of 4 June 1976.

27 Under the APPI, by definition, this information is not defined as sensitive information.

28 Article 2(7) APPI does not grant the right to correct, add and delete etc. to personal information that would be deleted within six months.

29 Article 36(2) APPI does not require a personal information handling business operator to delete the information on a method of anonymisation but take actions for security control such information.

a information about a living person that can identify him or her by name, date of birth or other description contained in the information (including information that will allow easy reference to other information that will enable the identification of the specific individual);[30] or

b information about a living person that contains an individual identification code, which means any character, letter, number, symbol or other codes designated by Cabinet Order,[31] falling under any of the following items:

- those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily or partial feature of the specific individual has been converted to be provided for use by computers; and
- those characters, letters, numbers, symbols or other codes assigned in relation to the use of services provided to an individual, or to the purchase of goods sold to an individual, or that are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or stated or recoded for the said user or purchaser, or recipient of issuance.[32]

Personal information database

A 'personal information database'[33] is an assembly of information including:

a information systematically arranged in such a way that specific personal information can be retrieved by a computer; or

b in addition, an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved.

Business operator handling personal information

A 'business operator handling personal information'[34] is a business operator using a personal information database, etc. for its business.[35] However, the following entities shall be excluded:

a state organs;

b local governments;

c incorporated administrative agencies, etc.;[36] and

d local incorporated administrative institutions.[37]

30 Article 2(1)(i) APPI.

31 Article 2(1)(ii), Article 2(2) APPI.

32 For example, according to the Cabinet Order, the information on sequences of bases of DNA, fingerprints, facial recognition (Article 2(2)(i)) and the information on driver licence, passport and insurance policy number (Article 2(2)(ii)) are regarded as an individual identification code.

33 Article 2(4) APPI.

34 Article 2(5) APPI.

35 As mentioned in Section I, the amended APPI applies to business operators that use any personal information database, regardless of the number of principals of personal information. Prior to the amendment, the APPI was applied solely to any personal information database containing details of more than 5,000 persons on any day in the past six months. See footnote 3.

36 Meaning independent administrative agencies as provided in Paragraph (1) of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003).

37 Meaning local incorporated administrative agencies as provided in Paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003).

Personal data[38]

'Personal data' comprises personal information constituting a personal information database, etc. (when personal information such as names and addresses is compiled as a database, it is personal data in terms of the APPI).

Sensitive personal information

The previous APPI did not have a definition of 'sensitive personal information'. However, for example, the Japan Financial Services Agency's Guidelines for Personal Information Protection in the Financial Field (the JFSA Guidelines)[39] have defined information related to political opinion, religious belief (religion, philosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information.[40] Furthermore, the JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[41] although some exceptions exist. Following these practices, the amended APPI has explicitly provided a definition of 'sensitive personal information' and its special treatment (see Section II.i).

ii General obligations for data handlers

Purpose of use

Pursuant to Article 15(1) APPI, a business operator handling personal information must as far as possible specify the purpose of that use. In this regard, the Basic Policy on the Protection of Personal Information (Basic Policy) (Cabinet Decision of 2 April 2004) prescribes as follows:

> *To maintain society's trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so-called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy-to-understand manner, their procedures relating to the handling of personal information, such as notification and announcement of the purpose of use and disclosure, etc., as well as comply with the relevant laws and ordinances.*

The government formulated the Basic Policy based on Article 7, Paragraph 1 APPI. To provide for the complete protection of personal information, the Basic Policy shows the orientation of measures to be taken by local public bodies and other organisations, such as businesses that handle personal information, as well as the basic direction concerning the promotion of measures for the protection of personal information and the establishment of measures to be taken by the state. The Basic Policy requires a wide range of government and private entities to take specific measures for the protection of personal information.

In this respect, under the previous APPI, a business operator handling personal information could not change the use of personal information 'beyond a reasonable extent'. The purpose of use after the change therefore had to be duly related to that before the change.

38 Article 2(6) APPI.

39 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).

40 Article 6(1) of the JFSA Guidelines.

41 Article 6(1)1–8 of the JFSA Guidelines.

The amended APPI has slightly expanded the scope of altering the purpose of use to enable flexible operations by prohibiting alteration of the utilisation purpose 'beyond the scope recognised reasonably relevant to the pre-altered utilisation purpose'.[42]

In addition, a business operator handling personal information must not handle personal information about a person beyond the scope necessary for the achievement of the purpose of use, without obtaining the prior consent of the person.[43]

Proper acquisition of personal information and notification of purpose

A business operator handling personal information shall not acquire personal information by deception or other wrongful means.[44]

Having acquired personal information, a business operator handling personal information must also promptly notify the data subject of the purpose of use of that information or publicly announce the purpose of use, except in cases in which the purpose of use has already been publicly announced.[45]

Maintenance of the accuracy of data and supervision of employees or outsourcing contractors

A business operator handling personal information must endeavour to keep any personal data it holds accurate and up to date within the scope necessary for the achievement of the purpose of use. Under the amended APPI,[46] a business operator handling personal information also must endeavour to delete personal data without delay when it becomes unnecessary.

In addition, when a business operator handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee to ensure the secure control of the personal data.[47]

When a business operator handling personal information entrusts another individual or business operator with the handling of personal data in whole or in part, it shall also exercise necessary and appropriate supervision over the outsourcing contractor to ensure the secure control of the entrusted personal data.[48]

Restrictions on provision to a third party

In general, a business operator handling personal information must not provide personal data to a third party without obtaining the prior consent of the data subject.[49]

42 Article 15(2) APPI.

43 Article 16(1) APPI.

44 Article 17 APPI.

45 Article 18(1) APPI.

46 Article 19 APPI.

47 Article 21 APPI. For example, during training sessions and monitoring, whether employees comply with internal rules regarding personal information protection.

48 Article 22 APPI. The APPI Guidelines point out: (1) a business operator handling personal information has to prepare rules on the specific handling of personal data to avoid unlawful disclosure and maintain the security of personal data; and (2) a business operator handling personal information has to take systemic security measures (e.g., coordinate an organisation's operations with regard to the rules on the handling of personal data, implement measures to confirm the treatment status of personal data, arrange a system responding to unlawful disclosure of personal data and review the implementation or improvement of security measures).

49 Article 23(1) APPI.

The principal exceptions to this restriction are where:

a the provision of personal data is required by laws and regulations;[50]

b a business operator handling personal information agrees, at the request of the subject, to discontinue providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the PPC and the person of the following or makes this information readily available to the person in accordance with the rules set by the PPC:[51]

- the fact that the provision to a third party is the purpose of use;
- which items of personal data will be provided to a third party;
- the method of provision to a third party;
- the fact that the provision of such personal data as might lead to the identification of the person to a third party will be discontinued at the request of the person; and
- the method of receiving the request of the person.

c a business operator handling personal information outsources the handling of personal data (e.g., to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;[52]

d personal information is provided as a result of the takeover of business in a merger or other similar transaction;[53] and

e personal data is used jointly between specific individuals or entities and where the following are notified in advance to the person or put in a readily accessible condition for the person:

- the facts;
- the items of the personal data used jointly;
- the scope of the joint users;
- the purpose for which the personal data is used by them; and
- the name of the individual or entity responsible for the management of the personal data concerned.[54]

Public announcement of matters concerning retained personal data

Pursuant to Article 24(1) APPI, a business operator handling personal information must put the name of the business operator handling personal information and the purpose of use of all retained personal data in an accessible condition for the person concerned (this condition

50 Article 23(1)(i) APPI. The APPI Guidelines mention the following cases:
a response to a criminal investigation in accordance with Article 197(2) of the Criminal Procedure Law;
b response to an investigation based upon a warrant issued by the court in accordance with Article 218 of the Criminal Procedure Law; and
c response to an inspection conducted by the tax authority.

51 Article 23(2) APPI.

52 Article 23(5)(i) APPI.

53 Article 23(5)(ii) APPI.

54 Article 23(5)(iii) APPI.

of accessibility includes cases in which a response is made without delay upon the request of the person), the procedures for responding to a request for disclosure, correction and cessation of the retention of the personal data.[55]

Correction

When a business operator handling personal information is requested by a person to correct, add or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data are incorrect, the business operator must make an investigation without delay within the scope necessary for the achievement of the purpose of use and, on the basis of the results, correct, add or delete the retained personal data, except in cases where special procedures are prescribed by any other laws and regulations for such correction, addition or deletion.[56]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

i Extraterritorial application of the APPI

It was generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity handling personal information in Japan. In accordance with this accepted understanding, the amended APPI explicitly provides that the APPI applies to a business operator located outside Japan under certain circumstances.

The provisions of Article 15, Article 16, Article 18 (excluding Paragraph (2)), Articles 19 to 25, Articles 27 to 36, Article 41, Article 42 Paragraph (1), Article 43 and Article 76 apply in those cases where, in relation to provision of a good or service to a person in Japan, a business operator handling personal information has acquired personal information relating to that person and handles the personal information or anonymously processed information produced using the said personal information in a foreign country.[57]

ii International data transfers

With some exceptions prescribed in the APPI (see Section III.ii, 'Restrictions on provision to a third party'), prior consent is required for the transfer of personal information to a third party.[58] However, there was no specific provision regarding international data transfers in the previous APPI. To deal with the globalisation of data transfers, the amended APPI requires the consent of the principal to international transfers of personal data except in the following cases:[59]

a international personal data transfer to a third party (in a foreign country) that has established a system conforming to the standards set by the PPC rules[60] (i.e., proper

55 The APPI Guidelines provide examples of what corresponds to such an accessible condition for the person, such as posting on the website, distributing brochures, replying without delay to a request by the person and providing the email address for enquiries in online electronic commerce.

56 Article 29(1) APPI.

57 Article 75 APPI.

58 Article 23(1) APPI.

59 Article 24 APPI.

60 Article 11 Rules of the PPC.

and reasonable measures taken in accordance with the provisions of the APPI or accreditation as a receiver of personal data according to international standards on the protection of personal information, such as being certified under the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules) for operating in a manner equivalent to that of a business operator handling personal data; and

b international personal data transfer to a third party in a foreign country that is considered, according to the rules of the PPC, to have established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual's rights and interests.[61]

V COMPANY POLICIES AND PRACTICES

i Security control measures

A business operator handling personal information must take necessary and proper measures for the prevention of leakage, loss or damage of the personal data.[62] Control measures may be systemic, human, physical or technical. Examples of these are listed below.

Systemic security control measures[63]

a Preparing the organisation's structure to take security control measures for personal data;

b preparing the regulations and procedure manuals that provide security control measures for personal data, and operating in accordance with the regulations and procedure manuals;

c preparing the means by which the status of handling personal data can be looked through;

d assessing, reviewing and improving the security control measures for personal data; and

e responding to data security incidents or violations.

Human security control measures[64]

a Concluding a non-disclosure agreement with workers when signing the employment contract and concluding a non-disclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of a temporary labourer); and

b familiarising workers with internal regulations and procedures through education and training.

61 At the time of writing, the PPC has not yet designated any country as having standards equivalent to those in Japan regarding the protection of personal information but the PPC has announced that it will designate member countries of the EU as qualified ones. See Section II.iv.

62 Article 20 APPI.

63 8-3 (Systemic Security Control Measures) of the APPI Guidelines, p. 88.

64 8-4 (Human Security Control Measures) and 3-3-3 (Supervision of Employees) of the APPI Guidelines, pp. 92, 41.

Physical security control measures[65]

a Implementing controls on entering and leaving a building or room where appropriate;
b preventing theft, etc.; and
c physically protecting equipment and devices.

Technical security control measures[66]

a Identification and authentication for access to personal data;
b control of access to personal data;
c management of the authority to access personal data;
d recording access to personal data;
e countermeasures preventing unauthorised software on an information system handling personal data;
f measures when transferring and transmitting personal data;
g measures when confirming the operation of information systems handling personal data; and
h monitoring information systems that handle personal data.

VI DISCOVERY AND DISCLOSURE

i E-discovery

Japan does not have an e-discovery system equivalent to that in the United States. Electronic data that include personal information can be subjected to a judicial order of disclosure by a Japanese court during litigation.

ii Disclosure

When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person, the business operator must disclose the retained personal data without delay by a method prescribed by a Cabinet Order.[67] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed where disclosure:

a is likely to harm the life, person, property, or other rights or interests of the person or a third party;
b is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or
c violates other laws and regulations.[68]

65 8-5 (Physical Security Control Measures) of the APPI Guidelines, p. 93.
66 8-6 (Technical Security Control Measures) of the APPI Guidelines, p. 96.
67 The method specified by a Cabinet Order under Article 28(2) APPI shall be the provision of documents (or 'the method agreed upon by the person requesting disclosure, if any'). Alternatively, according to the APPI Guidelines, if the person who made a request for disclosure did not specify a method or make any specific objections, then they may be deemed to have agreed to whatever method the disclosing entity employs.
68 Article 28(2) APPI.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement and sanctions

Enforcement agencies

Prior to the amendment, the enforcement agencies in data protection matters were the Consumer Affairs Agency, and ministries and agencies concerned with jurisdiction over the business of the relevant entities. Under the amended APPI, the PPC is the sole enforcement authority and it may transfer its authorities to request for report and to inspect to ministries and agencies if necessary for effective recommendations and orders under Article 42.[69]

Main penalties[70]

A business operator that violates orders issued under Paragraphs 2 or 3 of Article 42 (recommendations and orders by the PPC in the event of a data security breach) shall be sentenced to imprisonment with forced labour of not more than six months or to a fine of not more than ¥300,000.[71]

A business operator that does not make a report[72] as required by Articles 40 or 56 or that has made a false report shall be sentenced to a fine of not more than ¥300,000.[73]

ii Recent enforcement cases

Information breach at a computer company

An outsourcing contractor of a computer company had their customer information acquired by a criminal following an illegal intrusion into the company's network system. In May 2011, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the computer company reform its security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding supervision of an outsourcing contractor under Article 22 APPI).[74]

Information breach at a mobile phone company

The email addresses of a mobile phone company were reset and email addresses of the customers and the mail texts were disclosed to third parties. In January 2012, the Ministry of Internal Affairs and Communications (MIC) promulgated an administrative guidance requesting

69 Article 44 APPI.

70 The Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (unfair competition), including an act to acquire a trade secret from the holder by theft, fraud or other wrongful methods; and an act to use or disclose the trade secret so acquired. For the prevention of unfair competition, the Act provides measures, such as injunctions, claims for damages and penal provisions (imprisonment for a term not exceeding 10 years or a fine in an amount not exceeding ¥20 million. In the case of a juridical person, a fine not exceeding ¥1 billion (in certain cases the fine is not to exceed ¥500 million) may be imposed (Articles 21 and 22)).

71 Article 84 APPI.

72 The PPC may have a business operator handling personal information make a report on the handling of personal information to the extent necessary for fulfilling the duties of a business operator (Articles 40 and 56 APPI).

73 Article 85 APPI.

74 3-3-4 of the APPI Guidelines, p.42.

that the mobile phone company take the necessary measures to prevent a recurrence and to report the result to the Ministry (in respect of violation of the duty regarding security control measures under Article 20[75] APPI).[76]

Information theft from mobile phone companies

The manager and employees of an outsourcing contractor of three mobile phone companies acquired customer information from the mobile phone companies unlawfully through their customer information management system and disclosed the customer information to a third party. In November 2012, the MIC introduced an administrative guidance requesting that the mobile phone companies reform their security control measures, supervision of outsourcing contractors, and training for outsourcing contractors and employees (in respect of violation of the duty regarding security control measures under Article 20 APPI and Article 11 of the MIC Guideline on Protection of Personal Information in Telecommunications.[77] There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 22 APPI and Article 12 of the above-mentioned MIC Guideline).[78]

Information theft from a mobile phone company

In July 2012, a former store manager of an agent company of a mobile phone company was arrested for disclosing customer information of the mobile phone company to a research company (in respect of violation of the Unfair Competition Prevention Act). The Nagoya District Court in November 2012 gave the defendant a sentence of one year and eight months' imprisonment with a four-year stay of execution and a fine of ¥1 million.[79]

Information theft from an educational company

In July 2014, it was revealed that the customer information of an educational company (Benesse Corporation) had been stolen and sold to third parties by employees of an outsourcing contractor of the educational company. In September 2014, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the educational company reform its security control measures and supervision of outsourcing contractors (in respect of violation of the duty regarding security control measures under Article 20 APPI. There was also found to be a violation of the duty regarding the supervision of an outsourcing contractor under Article 22 APPI). Benesse Corporation actually distributed a premium ticket (with a value of ¥500) to its customers to compensate for the damage incurred by the customers. Currently, however, a lawsuit is pending before the Supreme Court brought by a customer requesting damages of ¥100,000 (Osaka High Court dismissed the customer's claim). On 29 October 2017, the Supreme Court sent the case back to Osaka High Court for further examination, holding that Osaka High Court erred in stating that any concern over the leak of personal information without any monetary damage is insufficient to establish any damage against the appellant (customer) under Article 709 of the Civil Code. At the time of writing, it is anticipated that Osaka High Court will hand

75 3-3-2 of the APPI Guidelines, p. 41.

76 www.soumu.go.jp/menu_news/s-news/01kiban05_02000017.html (available only in Japanese).

77 Announcement No. 695 of 31 August 2004 by the MIC.

78 www.soumu.go.jp/menu_news/s-news/01kiban08_02000094.html (available only in Japanese).

79 Nikkei News website article on November 6 of 2012 (available only in Japanese): www.nikkei.com/article/DGXNASFD05015_V01C12A1CN8000.

down a new decision clarifying the liability of businesses handling personal information for the leaking of customer's personal information and a method of calculating the amount of damages arising from the information leak.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As stated in Section IV, it is generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI is applicable to the entity handling personal information in Japan. The amended APPI requires that business operators obtain consent from the principal for international transfers of personal data. However, foreign business operators may circumvent this restriction by implementing proper and reasonable measures to protect personal information in accordance with the standards provided by the APPI.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code,[80] effective since 14 July 2011, were enacted to prevent and prosecute cybercrimes. Since under the previous law it was difficult to prosecute a person who merely stored a computer virus in his or her computer for the purpose of providing or distributing it to the computers of others, a person who not only actively creates, provides or distributes a computer virus, but also who acquires or stores a computer virus for the purpose of providing or distributing it to the computers of others without justification, may not be held criminally liable under the amendments.

Following the 2011 amendments, three primary types of behaviours are considered as cybercrimes: the creation or provision of a computer virus; the release of a computer virus; and the acquisition or storage of a computer virus. The Act on the Prohibition of Unauthorised Computer Access[81] (APUCA) was also amended on 31 March 2012 and took effect in May of that year. The APUCA identified additional criminal activities, such as the unlawful acquisition of a data subject's user ID or password for the purpose of unauthorised computer access, and the provision of a data subject's user ID or password to a third party without justification.

Following a 2004 review,[82] the government has begun developing essential functions and frameworks aimed at addressing information security issues. For example, the National Information Security Centre was established on 25 April 2005, and the Information Security Policy Council was established under the aegis of an IT Strategic Headquarters (itself part of the Cabinet) on 30 May 2005.[83]

80 Act No. 45 of 1907, Amendment: Act No. 74 of 2011.

81 Act No. 128 of 199, Amendment: Act No. 12 of 2012.

82 Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues (IT Strategic Headquarters, 7 December 2004).

83 See NISC, 'Japanese Government's Efforts to Address Information Security Issues: Focusing on the Cabinet Secretariat's Efforts': www.nisc.go.jp/eng/pdf/overview_eng.pdf; and the government's international cybersecurity strategy: www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

Finally, the Basic Act on Cybersecurity, which provides the fundamental framework of cybersecurity policy in Japan, was passed in 2014.[84]

ii Data security breach

There is no express provision in the APPI creating an obligation to notify data subjects or data authorities in the event of a data security breach. However, the APPI Guidelines stipulate that actions to be taken in response to data breach, etc. should be set out separately from the Guidelines. The PPC has set out desirable actions as follows:[85]

a internal report on the data breach, etc. and measures to prevent expansion of the damage;

b investigation into any cause of the data breach, etc.;

c confirmation of the scope of those affected by the data breach, etc.;

d consideration and implementation of preventive measures;

e notifications to any person (to whom the personal information belongs) affected by the data breach etc.;

f prompt public announcement of the facts of the data breach, etc. and preventive measures to be taken; and

g prompt notifications to the PPC about the facts of the data breach, etc. and preventive measures to be taken except for where the data breach, etc. has caused no actual, or only minor, harm (e.g., wrong transmissions of facsimiles or emails that do not include personal data other than names of senders and receivers).

In addition, the PPC has the authority to collect reports from, or advise, instruct or give orders to, the data controllers.[86]

An organisation that is involved in a data breach may, depending on the circumstances, be subject to the suspension, closure or cancellation of the whole or part of its business operations, an administrative fine, penalty or sanction, civil actions and class actions or a criminal prosecution.

X OUTLOOK

i The future development of the amended APPI

As stated in Section II, the amended APPI, which entered fully into force in May 2017, has drastically changed the legal framework for the protection of personal information in Japan. As of this writing, there have as yet been no leading cases or new matters to which the amended APPI applies and, led by the PPC, new practices based upon the new framework have just started. It is anticipated that the role of the PPC will be central to the new privacy policy in Japan and thus special attention should be paid to its activities for insight into the future development of the amended APPI.

84 Act No. 104 of 12 November 2014.

85 PPC Announcement No.1 of 2017.

86 Articles 40–42 APPI.

ii The judicial reaction to the leaking of personal information in Japan

As stated in Section VII, an important data breach case (Benesse Corporation) is currently pending before Osaka High Court and its decision (and its subsequent Supreme Court decision, if any) may articulate the scope of the obligations of business operators handling personal information and the calculation of damages arising from data breaches in Japan.

Appendix 1

ABOUT THE AUTHORS

TOMOKI ISHIARA

Sidley Austin Nishikawa Foreign Law Joint Enterprise

Mr Ishiara's practice areas include intellectual property law, antitrust law, data security and privacy law, entertainment law, investigation, litigation and arbitration. Mr. Ishiara has extensive experience in the field of intellectual property law, including giving advice to clients on patent, utility model, design patent, copyright, and trademark matters (including advice on employee invention rules), engaging in litigations and arbitrations. Also, Mr. Ishiara regularly advises foreign clients on compliance matters (e.g. data privacy, FCPA) and engages in subsequent investigations on such violations.

SIDLEY AUSTIN NISHIKAWA FOREIGN LAW JOINT ENTERPRISE

Marunouchi Building 23F 4-1
Marunouchi 2-Chome
Chiyoda-ku
Tokyo 100-6323
Japan
Tel: +81 3 3218 5900
Fax: +81 3 3218 5922
tishiara@sidley.com
www.sidley.com

ISBN 978-1-912228-62-1