The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

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 978-1-910813-32-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

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 applies 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]

Approximately 40 guidelines regarding personal information protection have been 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] These guidelines prescribe in detail the interpretations and practices of the APPI in relevant industries.

---

1 Tomoki Ishiara is an associate at Sidley Austin Nishikawa Foreign Law Joint Enterprise. The author would like to thank Mr Takahiro Nonaka, former Sidley counsel, for his great contribution to the previous year's version of this chapter.

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/280222_amendedlaw.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). Under the revised APPI, this minimum requirement is deleted.

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 Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information (Announcement No. 2 of 9 October 2009 by the

II THE YEAR IN REVIEW

i Policy Outline of the Institutional Revision for Use of Personal Data (Policy Outline), and the revision of the APPI

On 24 June 2014, the government[7] published the Policy Outline.[8] The Policy Outline shows the government's direction on which measures are 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. The main changes proposed in the Policy Outline, which underlies the revision of the APPI, are set out below. A brief summary of the revision is given in Section X, *infra*.

Development of a third-party authority system[9]

The government will develop an independent government body 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 system are as follows:

a the government will develop 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 will restructure the Specific Personal Information Protection Commission prescribed in the Number Use Act[10] to set up a commission 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 shall have the functions and powers of on-site inspection, in addition to the functions and powers that the competent ministers currently have over businesses handling personal information, and shall certify non-governmental self-regulation and certify or supervise non-governmental organisations that conduct conformity assessment in accordance with the privacy protection standards adopted by the country concerned regarding international transfer of personal data.

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 take action, such as concluding a contract, so that overseas businesses to which personal

---

Ministry of Health, Labour and Welfare and the Ministry of Economy, Trade and Industry) (Economic and Industrial Guidelines): www.meti.go.jp/policy/it_policy/privacy/0708english.pdf.

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

8 japan.kantei.go.jp/policy/it/20140715_2.pdf.

9 The European Commission pointed out the lack of a data protection authority in the Japanese system in its 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, B-5: Japan', Graham Greenleaf, 20 January 2010.

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

data will be provided take the necessary and appropriate actions that are compatible with technological development for the safe management of personal data. In addition, the government will consider the details of actions based on the types of data transfer and a framework for ensuring their effectiveness. The government will also establish a framework for non-governmental organisations that are certified by the third-party authority to certify businesses that are planning to distribute data across borders, examining their compliance with the privacy protection standards acknowledged by the countries concerned.

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. The current system of the APPI requires consent from persons to use their personal data for purposes other than those specified. Providing personal data to third parties is cumbersome for businesses, and creates a barrier to the use of personal data. Because the consent of the person is required to prevent a violation of personal rights and interests, the government will in the future implement a new framework to enable personal data to be provided to third parties without the individuals' consent to promote the use of personal data but prohibiting the identification of specific individuals.

Sensitive personal information

The APPI does not currently define 'sensitive personal information'; however, according to the Policy Outline, the amendments to the APPI will define information regarding an individual's race, creed, social status, criminal record and past record as sensitive personal information, along with any other information that may cause social discrimination.

The government will consider measures on the handling of sensitive information, such as prohibiting such data from being handled if they are included in personal information.

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 according to 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.

In this regard, there is currently no provision that specifically addresses consent requirements for sensitive personal information in the APPI; instead these are regulated by a number of guidelines issued by government ministries (see, e.g., Section III.i.(e), *infra*).

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,[11] and provides for the implementation of a national numbering system of 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; achieve the fair

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

distribution of burdens such as income tax payments; and develop efficient administration. An independent supervisory authority called the Specific Personal Information Protection Commission (PPC) was established on 1 January 2016. This authority consists of one chair and eight commission members. 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[12] and the Act on Specified Commercial Transactions,[13] 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.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Definitions

a Personal information:[14] information about a living person that can identify him or her by name, date of birth or other description contained in such information (including information that will allow easy reference to other information that will enable the identification of the specific individual).

b Personal information database:[15] an assembly of information including:
- information systematically arranged in such a way that specific personal information can be retrieved by a computer; or
- 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.

c A business operator handling personal information:[16] a business operator using a personal information database, etc., for its business.[17] However, the following entities shall be excluded:
- state organs;
- local governments;
- incorporated administrative agencies, etc.;[18]

12 Act No. 26 of 17 April 2002.

13 Act No. 57 of 4 June 1976.

14 Article 2(1) APPI.

15 Article 2(2) APPI.

16 Article 2(3) APPI.

17 The APPI applies to business operators that use any personal information database containing details of more than 5,000 persons on any day in the past six months. See footnote 3.

18 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,

- local incorporated administrative institutions;[19] and
- entities specified by a Cabinet order as having little likelihood of harming the rights and interests of individuals considering the volume and the manner of use of personal information they handle.[20]

d Personal data:[21] 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).

e Sensitive personal information: the APPI itself does not have a definition of sensitive personal information (see Section II.i, *supra*). However, for example, the Japan Financial Services Agency's Guidelines for Personal Information Protection in the Financial Field (JFSA Guidelines)[22] define 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.[23] The JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[24] although some exceptions exist.

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.*

To this end, the Economic and Industrial Guidelines specifically prescribe the recommended items that should be included in privacy policies or privacy statements.

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

---

etc. (Act No. 59 of 2003).

19 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).

20 Under the revised APPI, this exception is deleted. See footnote 3.

21 Article 2(4) APPI.

22 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).

23 Article 6(1) of the JFSA Guidelines.

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

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.

A business operator handling personal information also must not change the use of personal information beyond a reasonable extent. The purpose of use after the change must therefore be duly related to that before the change.[25]

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.[26]

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.[27]

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.[28]

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.[29]

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.[30]

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 security control of the entrusted personal data.[31]

---

25 Article 15(2) APPI.

26 Article 16(1) APPI.

27 Article 17 APPI.

28 Article 18(1) APPI.

29 Article 19 APPI.

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

31 Article 22 APPI. The Economic and Industrial Guidelines say: 'The necessary and appropriate supervision includes that an entrustment contract contains the measures which are mutually agreed upon by both parties of entruster and trustee as necessary and appropriate measures regarding the handling of personal data, and that it is confirmed periodically in the predetermined time interval whether such measures are properly executed.' The Economic and Industrial Guidelines also mention the matters that are preferable to be contained in a contract when the handling of personal data is entrusted, such as clarification

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.[32]

The principal exceptions to this restriction are as follows:

a where the provision of personal data is required by laws and regulations;[33]

b where a business operator handling personal information agrees to discontinue, at the request of the subject, providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the person of the following or makes such information readily available to the person:[34]

- 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; and
- 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;

c where 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;[35]

d where personal information is provided as a result of the takeover of business in a merger or other similar transaction;[36] and

e where 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.[37]

---

of the responsibilities of entruster and trustee, reporting in writing to an entruster when re-entrusting, and content and frequency of reporting regarding the status of handling personal data to an entruster, etc. (p. 49).

32 Article 23(1) APPI.

33 Article 23(1)(i) APPI. The Economic and Industrial Guidelines mention the following cases:

a submission of a payment record to the Director of the Taxation Office in accordance with Paragraph 1 of Article 225 of the Income Tax Law, etc.;

b response to the investigation of a subsidiary company by the auditors of a parent company in accordance with Paragraph 3 of Article 381 of the Company Law; and

c response to an audit of financial statements pursuant to the provisions of Article 396 of the Company Law and Sub-article 2 of Article 193 of the Securities and Exchange Law.

34 Article 23(2) APPI.

35 Article 23(4)(i) APPI.

36 Article 23(4)(ii) APPI.

37 Article 23(4)(iii) APPI.

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 (such a condition of accessibility includes cases in which a response is made without delay upon the request of the person).[38]

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.[39]

IV INTERNATIONAL DATA TRANSFER

There is no specific provision regarding international data transfers in the APPI. However, 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 would be applicable to the entity handling personal information in Japan. With some exceptions prescribed in the APPI (see Section III.ii, 'Restrictions on provision to a third party', *supra*), prior consent is required for the transfer of personal information to a third party.[40] The Economic and Industrial Guidelines provide examples of providing data to a third party pursuant to Article 23(1) APPI. Among these are the transfer of personal data between companies within the same group, including the exchange of personal data between a parent company and a subsidiary company, among fellow subsidiary companies and among group companies.

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.[41] Control measures may be systemic, human, physical or technical. Examples of these are listed below.

38 The Economic and Industrial Guidelines provide examples of what corresponds to such an accessible condition for the person, such as creating an enquiry counter and establishing a system so that a response to an enquiry is made verbally or in writing; ensuring placement of brochures in sales stores; and clearly describing the e-mail address for enquiries in online electronic commerce.

39 Article 26(1) APPI.

40 Article 23(1) APPI.

41 Article 20 APPI.

Systemic security control measures[42]

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;[43]

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[44]

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).

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

Physical security control measures[45]

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[46]

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.

---

42 2-2-3-2 [Security Control Measures (an issue related to Article 20 APPI)] (p. 32) of the Economic and Industrial Guidelines.

43 The Economic and Industrial Guidelines provide in detail the preferable means of preparing regulations and procedure manuals (p. 31).

44 2-2-3-2 (p. 44) of the Economic and Industrial Guidelines.

45 2-2-3-2 (p. 45) of the Economic and Industrial Guidelines.

46 2-2-3-2 (p. 46) of the Economic and Industrial Guidelines.

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.[47] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed:[48]

a where disclosure is likely to harm the life, person, property, or other rights or interests of the person or a third party;

b where disclosure is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or

c where disclosure violates other laws and regulations.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement and sanctions:

Enforcement agencies

The enforcement agencies in data protection matters are the Consumer Affairs Agency,[49] and ministries and agencies concerned with jurisdiction over the business of the relevant entities.[50]

47 The method specified by a Cabinet order under Paragraph 1 of Article 25 APPI shall be the provision of documents (or 'the method agreed upon by the person requesting disclosure, if any'). Alternatively, according to the Economic and Industrial 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.

48 Article 25(1) APPI.

49 In Japan, there is no single central data protection authority. The Consumer Affairs Agency is the central authority in respect of the APPI in general.

50 The relevant entities are those entities (entities handling personal information) that have used a personal information database with details of over 5,000 individuals on any day in the past six months. (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).

Main penalties[51]

A business operator that violates orders issued under Paragraphs 2 or 3 of Article 34 (recommendations and orders by the competent minister 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.[52]

A business operator that does not make a report[53] as required by Articles 32 or 46 or that has made a false report shall be sentenced to a fine of not more than ¥300,000.[54]

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[55] APPI).

Information breach at a mobile phone company

The e-mail addresses of a mobile phone company were reset and e-mail 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 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[56] APPI).[57]

---

51 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 five years or a fine in an amount not exceeding ¥5 million. In the case of a juridical person, a fine not exceeding ¥300 million (in certain cases the fine is not to exceed ¥100 million) may be imposed (Articles 21 and 22)).

52 Article 56 APPI.

53 The competent minister 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 32 and 46 APPI).

54 Article 57 APPI.

55 See Section III.ii, 'Maintenance of the accuracy of data and supervision of employees or outsourcing contractors', *supra*.

56 See Section V.i, 'Security control measures', *supra*.

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

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.[58] 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).[59]

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.[60]

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).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As stated in Section IV, *supra*, 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 would be applicable to the entity handling personal information in Japan.

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

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

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

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code,[61] 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[62] (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,[63] 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.[64]

A bill on the Basic Law of Cybersecurity, which obliges all government ministries and agencies to report cyberattacks and aims to strengthen the authority of the National Information Security Centre, is being discussed in the Diet.

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, there are various guidelines issued by government ministries, some of which stipulate notifying the affected data subjects

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

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

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

64 See 'Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts', NISC: 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.

or governmental authorities promptly upon the occurrence of a data security breach.[65] In addition, the competent ministries have the authority to collect reports from, or advise, instruct or give orders to, the data controllers.[66]

An organisation that is involved in a data breach may, depending on the circumstances, be subject to a 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 revision of the APPI

As stated in Section II, *supra*, on 24 June 2014, the government published the Policy Outline, and the revised APPI legislation passed the Diet on 3 September 2015. The revised APPI will be in full force in 2017, but its effective date has not been set (as at the time of writing). This revision is the first major amendment to the APPI. A brief summary of the revision is given below. Until recently, the government (through the PPC) was in the process of formulating a regulation that sets out the following items:

a the definitions of 'personal identifiable code' and 'sensitive personal information';

b details of the requirements for internal data protection system that a third party receiving personal information outside Japan should maintain;

c details of the records that a business operator handling personal information should keep in providing such information to third parties; and

d standards on methods of creating anonymised personal information and security measures to be taken to protect such information.

The PPC promulgated the regulation on 5 October 2016. The regulation will finally be in full force on the effective date of the revised APPI, which is to be set by government ordinance before 30 May 2017. The PPC has published and requested comments on a draft guideline of the revised APPI.

ii Clarification of the definition of personal information

Under Article 2 APPI, 'personal information' is defined as the information about a living person that can identify him or her by name, date of birth or other description contained in

65 The Economic and Industrial Guidelines say it is preferable to apologise to the person for the accident or violation, and to contact the person as much as possible to prevent secondary damage, except in certain instances, including where the personal data that were lost were immediately recovered without being seen by a third party, since it is conceivable that contacting the person can be omitted when the rights and interests of the person have not been infringed and it seems that there is no or extremely little likelihood of infringement. The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information also mention the obligations that apply in the event of a data security breach.

66 Articles 32–34 APPI.

such information (including information that will allow easy reference to other information that will enable the identification of the specific individual). Under the revised APPI, the following information is clarified as personal information:

a personal identifiable codes, including, but not limited to, any code on physical characteristics of individuals (i.e., fingerprints) and individually allocated numbers (i.e., passport numbers and driver licence numbers); and

b sensitive personal information (i.e., race, creed, social status, medical history, criminal records, damage caused by a crime and the other information that may be designated by the Cabinet Order), the handling of which requires certain special measures.

iii Ensuring effective use of personal information

To ensure effective use of huge amounts of personal data (big data), the revised APPI provides that a business operator handling personal information may anonymise personal information and provide it to third parties without individuals' consent to the extent that such treatment complies with regulations to be promulgated by the data protection authority newly created under the revised APPI.

iv Enhancement of the protection of personal information

The revised APPI:

a imposes obligations on business operators handling personal information to verify third parties' names and how they obtained personal information when they receive personal information from those third parties;

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

c establishes criminal liability for handling personal information with a view to making illegal profits.

v Establishment of the PPC

The revised APPI creates a new independent data protection authority, the PPC, which is authorised to address legal requirements and self-regulation matters.

vi Globalisation of personal information handling

The revised APPI introduces the following provisions on cross-border data transfers:

a personal data may not be transferred overseas without prior consent from the person, except where a transferee foreign country is regarded by the PPC as having data protection standards equivalent to those of Japan; and

b the PPC may, under some circumstances, provide foreign enforcement authorities with useful information to assist their enforcement actions.

vii Other amendments

a The revised APPI requires that provision of personal information to third parties without consent be filed with the PPC.

b The revised APPI will be applied to business operators that have used any personal information database, regardless of the number of individuals whose personal information is involved.[67]

67 See footnote 3.

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, telecommunications, data security and privacy law, entertainment law, compliance/investigation, litigation and arbitration. Mr Ishiara has extensive experience in the field of intellectual property law and antitrust law, including giving advice to clients on patent, utility model, design patent, copyright, trademark matters (including advice on employee invention rules), engaging in licensing negotiations and litigations (including actions to annul trial decisions at the IP High Court and trials for patent invalidation at the Japanese Patent Office), and dealing with rapidly increasing IT-related disputes arising out of system development or maintenance M&A transactions.

SIDLEY AUSTIN LLP

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 5006
Fax: +81 3 3218 5922
tishiara@sidley.com

www.sidley.com