The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 12

JAPAN

Takahiro Nonaka[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 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 Takahiro Nonaka is an associate at Sidley Austin Nishikawa Foreign Law Joint Enterprise.

2 Act No. 57 of 30 May 2003, Enacted on 30 May 2003 except for Chapter 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. www.caa.go.jp/planning/kojin/foreign/act_1.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 Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information (Announcement No. 2 of 9 October 2009 by the Ministry of Health, Labour and Welfare and the Ministry of Economy, Trade and Industry)

II THE YEAR IN REVIEW

i Policy Outline of the Institutional Revision for Use of Personal Data

On 24 June 2014, the Japanese government[7] published the Policy Outline of the Institutional Revision for Use of Personal Data.[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 is planned to be submitted to the Diet in or after January 2015. The main changes proposed in the Policy Outline are set out below.

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-regulations 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-regulations 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-regulations and certify or supervise the non-governmental organisation 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

(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 http://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 (the EC Comparative Study).

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

have to take action, such as concluding a contract, so that overseas businesses to which personal 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. Also, the government will 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 the person 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 their 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 it is 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 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, for example, 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 and provides for the implementation of a national numbering system of social security and taxation purposes. The Japanese government will adopt the social security and tax number system to: (1) enhance the social security for people who

truly need it; (2) achieve the fair distribution of burdens such as income tax payments; and (3) develop efficient administration. An independent supervisory authority called the Specific Personal Information Protection Commission will be established. This authority will consist of one chairman and six commission members. The chairman and commissioners will be appointed by Japan's Prime Minister, and confirmed by the National Diet. The numbering system will be in effect from January 2016. Unlike other national ID numbering systems, Japan has not set up a centralised database for the numbers due to concerns about data breach and privacy.

iii Online direct marketing

Under the Act on Regulation of Transmission of Specified Electronic Mail[11] and the Act on Specified Commercial Transactions,[12] 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:[13] 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:[14] 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:[15] a business operator using a personal information database, etc., for its business.[16] However, the following entities shall be excluded:
- state organs;
- local governments;

11 Act No. 26 of 17 April 2002.

12 Act No. 57 of 4 June 1976.

13 Article 2(1) APPI.

14 Article 2(2) APPI.

15 Article 2(3) APPI.

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

- incorporated administrative agencies, etc.;[17]
- local incorporated administrative institutions;[18] and
- entities specified by a Cabinet Order as having little likelihood to harm the rights and interests of individuals considering the volume and the manner of use of personal information they handle.

d Personal data:[19] personal information constituting a personal information database, etc. (when personal information such as name 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)[20] defines information related to political opinion, religious belief (religion, pilosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information.[21] The JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[22] although some exceptions exist.

ii General obligations for data handlers

Purpose of use

Pursuant to Article 15(1) of the 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 (the 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.*

17 Which means 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).

18 Which means local incorporated administrative agencies as provided in paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003).

19 Article 2(4) APPI.

20 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).

21 Article 6(1) of the JFSA Guidelines.

22 Article 6(1)1 to 8 of the JFSA Guidelines.

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 has formulated the Basic Policy, based on Article 7, Paragraph 1 of 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 measure to be taken by the state. This Basic Policy of the government requires a wide range of government and private entities to take specific measures for the protection of personal information.

Also, a business operator handling personal information 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.[23]

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.[24]

Proper acquisition of personal information and notification of purpose

A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.[25]

Also, having acquired personal information, a business operator handling personal information must 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.[26]

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.[27]

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.[28]

Also, 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

23 Article 15(2) APPI.

24 Article 16(1) APPI.

25 Article 17 APPI.

26 Article 18(1) APPI.

27 Article 19 APPI.

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

shall exercise necessary and appropriate supervision over the outsourcing contractor to ensure the security control of the entrusted personal data.[29]

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.[30]

The principal exceptions to this restriction are as follows:

a where the provision of personal data is required by laws and regulations;[31]

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:[32]

- 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;

29 Article 22 APPI. The Economic and Industrial Guidelines says '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 mentions the matters which are preferable to be contained in a contract when the handling of personal data is trusted, such as clarification of the responsibilities of entruster and trustee, report in writing to an entruster when reentrusting and content and frequency of report regarding the status of handling personal data to an entruster etc. (p.49).

30 Article 23(1) APPI.

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

(1) 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.;

(2) 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

(3) 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.

32 Article 23(2) APPI.

c where a business operator handling personal information outsources the handling of personal data (for example, to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;[33]

d where personal information is provided as a result of the takeover of business in a merger or other similar transaction;[34] and

e where personal data is used jointly between specific individuals or entities and where: (1) the facts, (2) the items of the personal data used jointly, (3) the scope of the joint users, (4) the purpose for which the personal data is used by them, and (5) the name of the individual or entity responsible for the management of the personal data concerned, are notified in advance to the person or put in a readily accessible condition for the person.[35]

Public announcement of matters concerning retained personal data

Pursuant to Article 24(1) of the 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 condition includes cases in which a response is made without delay at the request of the person).[36]

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 is 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.[37]

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

33 Article 23(4)(i) APPI.

34 Article 23(4)(ii) APPI.

35 Article 23(4)(iii) APPI

36 The Economic and Industrial Guidelines provides some examples corresponding to the accessible condition for the person, such as creating an enquiry counter and to establish a system so that a response to an enquiry is made verbally or in writing, having the placement of brochures in store sales, and clearly describing the e-mail address for inquiries in online electronic commerce.

37 Article 26(1) APPI.

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.[38] The Economic and Industrial Guidelines provide examples of providing data to a third party pursuant to Article 23(1) of the 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.[39] Control measures may be systemic, human, physical or technical. Examples of these are listed below.

Systemic security control measures[40]

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;[41]

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[42]

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.

38 Article 23(1) APPI.

39 Article 20 of APPI.

40 2-2-3-2 [Security Control Measures (an issue related to Article 20 of APPI)] (p.32) of the Economic and Industrial Guidelines.

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

42 2-2-3-2 (p.44) of the Economic and Industrial Guidelines.

Physical security control measures[43]

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[44]

a Identification and authentication for access to personal data;
b control of access to personal data;
c management of 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 system 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 US. Electronic data that includes 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.[45] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed:[46]

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.

---

43 2-2-3-2 (p.45) of the Economic and Industrial Guidelines.

44 2-2-3-2 (p.46) of the Economic and Industrial Guidelines.

45 The method specified by a Cabinet Order under Paragraph 1 of Article 25 of 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 employes.

46 Article 25(1) APPI.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement and sanctions:

Enforcement agencies

The enforcement agencies in data protection matters are the Consumer Affairs Agency;[47] and ministries and agencies concerned with jurisdiction over the business of the covered entities.[48]

Main penalties[49]

A business operator who violates orders issued under Paragraph 2 or 3 of Article 34 (recommendations and orders by the competent minister in the event of 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.[50]

A business operator who does not make a report[51] as required by Article 32 or 46 or who has made a false report shall be sentenced to a fine of not more than ¥300,000 yen.[52]

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 their security control measures, supervision of outsourcing contractors and training for outsourcing

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

48 Covered entities means an entity (Entity Handling Personal Information) that has used a personal information database concerning over 5,000 individuals on any day in the last 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).

49 The Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (Unfair Competition), including (1) an act to acquire trade secret from the holder by theft, fraud or other wrongful methods; and (2) 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 damage 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).

50 Article 56 of APPI.

51 The competent minister may have a business operator handling personal information make a report on the handle of personal information to the extent necessary for fulfilling duties of a business operator. (Article 32 and 46 of APPI).

52 Article 57 of APPI.

contractors and employees (violation of the duty regarding supervision of an outsourcing contractor under Article 22[53] of the APPI).[54]

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 (violation of the duty regarding security control measures under Article 20[55] of the APPI).[56]

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 (violation of the duty regarding security control measures under Article 20 of the APPI and Article 11 of the MIC Guideline on Protection of Personal Information in Telecommunications.[57] There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 22 of the APPI and Article 12 of the above-mentioned MIC Guideline).[58]

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 (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.[59]

---

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

54 www.meti.go.jp/english/press/2011/0527_04.html.

55 See Section V.i, 'Security control measures'.

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

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

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

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

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.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code,[60] 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, now, a person who not only actively creates, provides or distributes a computer virus, but who acquires or stores a computer virus for the purpose of providing or distributing it to the computers of others without justification may be held criminally liable under the amendments.

Following the 2011 amendments, three primary types of behaviours are considered as cybercrimes: (1) the creation or provision of a computer virus; (2) the release of a computer virus; and (3) the acquisition or storage of a computer virus. Also, the Act on the Prohibition of Unauthorised Computer Access[61] (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[62] 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.[63]

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.

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

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

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

63 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.

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 or governmental authorities promptly upon the occurrence of a data security breach.[64] In addition, the competent ministries have the authority to collect reports from, advise, instruct, or give orders to the data controllers.[65]

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

As stated in Section II, *supra*, on 24 June 2014, the Japanese government published the Policy Outline of the Institutional Revision for Use of Personal Data, and the revision bill of the APPI is planned to be submitted to the Diet during or after January 2015.

64 The Economic and Industrial Guidelines says it is preferable to apologise to the person for the accident or violation and to contact the person as much as possible in order to prevent a secondary damage except in certain instances, including where the personal data that was lost was immediately recovered without being seen by a third party, since it is conceivable that a contact to the person can be omitted when the rights and interests of the person are not 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 mentions the obligations in case of data security breach.

65 Articles 32–34 APPI.

Appendix 1

ABOUT THE AUTHORS

TAKAHIRO NONAKA

Sidley Austin Nishikawa Foreign Law Joint Enterprise

Takahiro Nonaka assists foreign companies with compliance matters, including with research, negotiating with government officials, conducting internal investigations and drafting internal codes, related to such areas of Japanese law as data privacy, pharmaceutical, corporate and labour. In high-profile crisis cases, he works with all of the associated investigative agencies and mass media.

Before joining Sidley, he served for nearly 10 years as a judge of the District Court in Tokyo, Nagoya and Kochi. He presided over cases relating to privacy, disclosure, defamation, labour, corporate law, intellectual property and medicine.

He was seconded to the Embassy of Japan in Washington, DC from 2006 to 2008, and as a diplomat, he handled FCPA and antitrust issues, export controls and legal actions against Japanese companies. He currently handles US antitrust law and FCPA issues, cross-border litigations and international arbitration with the lawyers of Sidley Austin LLP.

Mr Nonaka was also seconded to the human resources department of a leading global Japanese automotive company. He provides clients with strategic services on wide range of labour issues, including collective bargaining and regulatory correspondence.

He is a member of the privacy, data security and information law and the FCPA and anti-corruption practice teams within Sidley Austin LLP.

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
tnonaka@sidley.com

www.sidley.com