# THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

**Editor**
Alan Charles Raul

THE LAWREVIEWS

# THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

**Editor**
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.TheLawReviews.co.uk



ISBN 978-1-80449-116-4

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

# ACKNOWLEDGEMENTS

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

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

# CONTENTS

Chapter 1 GLOBAL OVERVIEW ..... 1
*Alan Charles Raul*

Chapter 2 EU OVERVIEW ..... 5
*William R M Long, Francesca Blythe, João D Quartilho and Alan Charles Raul*

Chapter 3 CBPR AND APEC OVERVIEW ..... 46
*Alan Charles Raul and Sheri Porath Rockwell*

Chapter 4 METAVERSE AND THE LAW ..... 63
*Dominique Lecocq and Logaina M Omer*

Chapter 5 CHALLENGES FACED DURING CYBER INCIDENT INVESTIGATIONS ..... 77
*Paul Pu, Dakai Liu and Mohit Kumar*

Chapter 6 ARGENTINA ..... 85
*Adrián Furman, Francisco Zappa and Rocío Barrera*

Chapter 7 AUSTRALIA ..... 97
*Sven Burchartz, Karla Brown and Brighid Virtue*

Chapter 8 BELGIUM ..... 113
*Steven De Schrijver and Olivier Van Fraeyenhoven*

Chapter 9 BRAZIL ..... 129
*Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Isabella da Penha Lopes Santana, Carolina Simioni Perdomo and Bruna Evellyn Pereira Bigas*

Chapter 10 CHINA ..... 147
*Samuel Yang*

Chapter 11 DENMARK ..... 177
*Tommy Angermair, Camilla Sand Fink and Amanda Langeland Knudsen*

Chapter 12 EGYPT ..... 195
*Mohamed Khodeir, Hanan El Dib, Nour Samy, Lina El Sawy, Aly Talaat and Mohamed Nour El Din*

Chapter 13 GERMANY ..... 204
*Olga Stepanova and Patricia Jechel*

Chapter 14 HONG KONG ..... 213
*Yuet Ming Tham, Linh Lieu and Lester Fung*

Chapter 15 HUNGARY ..... 232
*Tamás Gödölle and Márk Pécsvárady*

Chapter 16 INDIA ..... 245
*Aditi Subramaniam and Sanuj Das*

Chapter 17 INDONESIA ..... 257
*Danny Kobrata and Ghifari Baskoro*

Chapter 18 JAPAN ..... 270
*Tomoki Ishiara*

Chapter 19 MALAYSIA ..... 293
*Deepak Pillai and Yong Shih Han*

Chapter 20 MEXICO ..... 317
*Paola Morales and Marcela Flores González*

Chapter 21 NETHERLANDS ..... 334
*Herald Jongen and Emre Yildirim*

Chapter 22 NEW ZEALAND ..... 349
*Derek Roth-Biester, Megan Pearce and Emily Peart*

Chapter 23 PORTUGAL ..... 365
*Jacinto Moniz de Bettencourt, Joana Diniz de Figueiredo and Mafalda Romão Mateus*

Chapter 24 SINGAPORE ..... 378
*Margaret Hope Allen, Yuet Ming Tham and Faraaz Amzar*

Chapter 25 SPAIN ..... 397
*Leticia López-Lapuente*

Chapter 26 SWITZERLAND ..... 413
*Jürg Schneider, Monique Sturny and Hugh Reeves*

Chapter 27 TAIWAN ..... 437
*Jaclyn Tsai, Elizabeth Pai and Jaime Cheng*

Chapter 28 UNITED KINGDOM ..... 450
*William R M Long, Francesca Blythe and Eleanor Dodding*

Chapter 29 UNITED STATES ..... 484
*Alan Charles Raul and Sheri Porath Rockwell*

Appendix 1 ABOUT THE AUTHORS ..... 517
Appendix 2 CONTRIBUTORS' CONTACT DETAILS ..... 539

**Chapter 18**

# JAPAN

*Tomoki Ishiara*[1]

## I OVERVIEW

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

---

1 Tomoki Ishiara is a partner at Sidley Austin Foreign Law Joint Enterprise.

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

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

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

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

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

7 The General Guidelines regarding the Act on the Protection of Personal Information (last updated 8 September 2022, available at https://www.ppc.go.jp/files/pdf/230401_guidelines01.pdf).

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

Pursuant to the supplemental provisions of the amendment to the APPI, the APPI is to be reviewed for any necessary update triennially.[9] In 2020, as a result of the triennial review by the PPC, the further amendment to the APPI was enacted on 12 June 2020 and the amendment in 2020 has been in effect on 1 April 2022.

Further, in 2021, under the Act on the Arrangement of Related laws for the Formation of a Digital Society,[10] the three laws of the APPI, the Act on the Protection of Personal Information Held by Administrative Organs, and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. was integrated into the APPI and accordingly, the article number of provisions of the APPI was revised. These revisions have been in effect step-by-step on 1 September 2021, 1 April 2022 and 1 April 2023.

Accordingly, the revisions in 2021 are non-substantial and mainly relevant to revisions of the article number of the provisions under the APPI as a result of the integration of the three laws above. In accordance with the revisions in 2021, the reference to article numbers in this chapter have also been revised.

## II THE YEAR IN REVIEW

### i Drastic change of the legal framework under the APPI in 2017

The amendment to the APPI has been in full force since 30 May 2017. The main changes introduced by the amendment are set out below.

***Development of a third-party authority system***[11]

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

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

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

*c* the third-party authority has the following functions and powers:
- formulation and promotion of basic policy for personal information protection;
- supervision;
- mediation of complaints;
- assessment of specific personal information protection;
- public relations and promotion;

9 Article 12 of the supplemental provisions of the Act on the Protection of Personal Information.

10 https://www.japaneselawtranslation.go.jp/outline/36/211105155408_905R305.pdf.

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

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

- accreditation of private organisations that process complaints about business operators handling personal information and provide necessary information to such business operators, based on the APPI;
- survey and research the operations stated above at (c); and
- cooperation with data protection authorities in foreign states.[13]

***Actions for globalisation***

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

*a* no consent is necessary in accordance with the following exceptions to Article 27 (amended in 2021 and effective on 1 April 2022):
- cases based on laws and regulations;
- cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
- cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent; and
- cases in which there is a need to cooperate with a central government organisation or a local government, or a person entrusted by them acting in matters prescribed by laws and regulations,[15] and when there is a possibility that obtaining a principal's consent would interfere with the execution of these duties;

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

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

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

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

13 Article 129 APPI (amended in 2021 and in effective on 4 April 2022).

14 Article 28 APPI (amended in 2021 and in effective on 4 April 2022).

15 Article 27 APPI (amended in 2021 and in effective on 4 April 2022).

information used for the production.[16] This amendment allows various businesses to share with other businesses the personal data maintained by them, and so develop or foster new business or innovation.

***Sensitive personal information***

Initially, the APPI had not defined 'sensitive personal information'; however, the amendment to the APPI defined information regarding an individual's race, creed, social status, criminal record and past record as 'special-care-required personal information' (sensitive personal information), along with any other information that may be the focus of social discrimination.[17] Also, while there was no provision that specifically addressed consent requirements for sensitive personal information in the APPI, the amendment to the APPI explicitly requires that a business operator handling personal information obtain prior consent to acquire sensitive personal information, with certain exceptions.[18]

In addition, the opt-out exception provided under Article 27 (amended in 2021 and effective on 1 April 2022) does not apply to sensitive personal information and consent to provide such information to third parties is required.[19]

***Enhancement of the protection of personal information: traceability of obtained personal information***

The amendment to the APPI:

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

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

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

**ii Reciprocal adequacy decision**

On 17 July 2018, Japan released a press release announcing Japan and the European Union have agreed on reciprocal adequacy of their respective data protection systems. Finally, 23 January 2019, the PPC designated the EU member countries as the ones that qualify for the exemption to the consent requirement for international transfer.[23] Japan and the EU long discussed and agreed on reciprocal adequacy on the condition that Japan would implement guidelines (without revising the APPI) to supplement insufficient protections from the EU perspective as follows:

16 Article 43(1) APPI (amended in 2021 and in effective on 4 April 2022).

17 Article 2(3) APPI.

18 Article 20(2) APPI (amended in 2021 and in effective on 1 April 2022).

19 Article 27(2) APPI (amended in 2021 and in effective on 1 April 2022).

20 Article 29 APPI (amended in 2021 and in effective on 1 April 2022).

21 Article 30 APPI (amended in 2021 and in effective on 1 April 2022).

22 Article 174 APPI (amended in 2021 and in effective on 1 April 2022).

23 The UK has been eligible to the same exemption since 1 February 2020 after Brexit.

*a* information on trade union membership or an individual's sexual orientation[24] shall be regarded as sensitive information in Japan as well as in the EU;

*b* personal data that will be deleted within six months[25] shall be protected as personal data;

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

*d* Japan shall ensure the same level of protection in non-EU countries as the one provided in Japan under the APPI if personal information coming from the EU is transferred from Japan to non-EU countries; and

*e* for the anonymisation of personal information coming from the EU, the complete deletion of a method of reidentification would be required.[26]

### iii Amendment to the APPI in 2020

Article 12 of the supplemental provisions of the APPI provides that the APPI is to be reviewed triennially to ensure that the APPI could meet with any practical need and technical development. The PPC was engaged in monitoring personal data practice and considered any need to update the APPI, finally issuing a report on the recommendation on the updates of the APPI as a result of its review in 2019. Then, the further amendment to the APPI was enacted on 12 June 2020, reflecting a result of the PPC's review and subsequent public consultation. The amendment will become effective on 1 April 2022 with the exception of the amendment to the opt-out requirement (1 October 2021) and penalty (12 December 2020).

#### *Enhancement of a data subject's right*

The amendment to the APPI in 2020:

*a* entitles a data subject to ask a business operator to stop using personal data when a business operator handling personal information does not need to use personal data any more, the personal data is leaked or the data subject's right or interest may be undermined;[27]

*b* entitles a data subject to ask a business operator handling personal information to disclose a record of the provision of its personal data to any third party;[28]

*c* entitles a data subject to designate a method by which personal data retained by a business operator should be disclosed to the data subject;[29]

*d* entitles a data subject to request for disclosure of any record showing that its personal data is provided to any third party;[30]

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

25 Article 2(7) APPI did not grant the right to correct, add and delete etc. to personal information that would be deleted within six months but the amendment to the APPI in 2020 has granted such rights without a short-term restriction.

26 Article 43(2) (amended in 2021 and in effective on 1 April 2022) APPI does not require a personal information handling business operator to delete the information on a method of anonymisation but take actions for security control such information.

27 Article 35(5), (6) APPI (amended in 2021 and in effective on 1 April 2022).

28 Article 33(5) APPI (amended in 2021 and in effective on 1 April 2022).

29 Article 33(1), (2) APPI (amended in 2021 and in effective on 1 April 2022).

30 Article 33(5) APPI (amended in 2021 and in effective on 1 April 2022)..

*e* clarifies that the opt-out exception provided under Article 27 does not apply where personal data provided to any third party is the data obtained in an improper manner or where personal data provided by relying on an opt-out exception is further provided to any third party;[31] and

*f* grants the right to correct, add and delete, etc. to personal information even if such information is scheduled to be deleted within six months.[32]

***New obligation imposed on a business operator handling personal information***

The amendment to the APPI in 2020:

*a* imposes an obligation to report[33] any personal data leak incident that falls under certain categories to be specified by the PPC;[34] and

*b* prohibits a business operator handling personal information from handling personal data in an inappropriate way that may facilitate illegal or improper action.[35]

***Facilitating reasonable use of data while protecting interests of a data subject***

The amendment to the APPI in 2020 (in effect as of 12 December 2020):

*a* creates a notion of 'pseudonymously processed data'[36] and excludes it from a data subject's right to ask a business operator handling personal information to disclose such data to the data subject or stop using personal data for the business operator to ensure that analysis or use of personal data will be more convenient for a business operator;[37]

*b* clarifies that pseudonymously processed data is still protected as personal data (unlike anonymously processed data) and sets out obligations of a business operator handling pseudonymously processed data[38] (e.g., the business operator is required to modify personal data in compliance with rules to be set by the PPC); and

*c* requires a third-party receiver of any data that does not constitute personal data on its provider side to obtain consent from the data subject if the third party could identify the data subject based upon the provided data.

***Strengthening penalties against a violation of an order to be issue by the PPC, etc.***

The amendment to the PPI in 2020:

*a* increases criminal punishment (e.g., one year's imprisonment or ¥1 million for violation of the PPC's order);[39] and

*b* increases the amount of the fine against a corporation compared to the one against an individual (i.e., the upper limit of the fine against a corporation is ¥100 million for the

31 Article 27(2) APPI (amended in 2021 and in effective on 1 April 2022). This amendment came into effect as of 1 October 2021.

32 Article 2 (7) APPI. Prior to the amendment in 2020, the personal data that is to be deleted within six months was not recognised as personal data retained by a business operator handling personal information.

33 Article 26 APPI (amended in 2021 and in effective on 1 April 2022).

34 Prior to the amendment in 2020, such report was not mandatory and just recommended by the PPC to file in accordance with a guidance set by the PPC.

35 Article 19 APPI (amended in 2021 and in effective on 1 April 2022).

36 Article 2(5) APPI.

37 Article 41 APPI (amended in 2021 and in effective on 1 April 2022).

38 Article 41 APPI.

39 Article 173 APPI (amended in 2021 and in effective on 1 April 2022).

violation of the PPC's order or for an illegal provision or theft of personal information database and the upper limits of the fine against an individual for the same violations are ¥0.5 and ¥1 million).[40]

***Expansion of extraterritorial application of the PPC's order and imposition of the new obligation on international transfer***

The amendment to the PPI in 2020:

*a* entitles the PPC to oblige overseas business operator handing personal information[41] in connection with any product or service provided to individuals in Japan to report on something designated by the PPC and to issue an order for improvement, a violation of which may lead to the public announcement by the PPC of such violation and may further subject to the fine sanction; and

*b* requires a business operator handling personal information to provide a data subject with any information on how a foreign receiver of his or her personal data handles it in the case where the consent to the personal data's international transfer is obtained.[42]

**iv Establishment of supplemental rules for the 2020 amendment in 2021**

***Reporting obligation of a business operator handling personal information***[43]

As mentioned above, the amendment in 2020 set forth an obligation to report data leak incident. The PPC has specifically required businesses operator handling personal information to report to the PPC or relevant governmental agencies on data leak with 30 days (60 days in the case of unlawful computer access) after a prompt notice in the following cases where:

*a* sensitive information is leaked;

*b* financial damage may be caused;

*c* unlawful computer access is found; or

*d* more than 1,000 pieces of personal information are leaked.

Business operators handling personal information are required to give a notice of data leak to the data subject whose information may be leaked, to the extent necessary.

***Requirements in connection with how to create pseudonymously processed data***[44]

In creating pseudonymously processed data, a business operator handling personal information is required to comply with the following points:

*a* delete or replace any description included in personal information that makes someone identifiable;

*b* delete or replace any code included in personal information that makes someone identifiable;

*c* delete or replace any description in personal information, inappropriate use of which may cause any financial damage.

40 Article 173, 174, 179(1)(i) APPI (amended in 2021 and effective on 1 April 2022).

41 Article 166 APPI.

42 Article 28(2) APPI.

43 Article 26(1) APPI.

44 Article 43(1) APPI.

When a business operator handling personal information creates or receives pseudonymously processed data, it is required to take following security measures:

*a* clarifying authority and responsibility of persons who are in charge of handling the deleted or replaced information;

*b* setting out rules on handling the deleted or replaced information, monitoring the compliance of the rules and improving the management of the deleted or replaced information; and

*c* taking necessary and appropriate measures to avoid unauthorised handling of the deleted or replaced information.

***Data providers' new obligations***

The data provider has an obligation to confirm the consent from the data subject that provided non-personal information for this to become personal information on the receiver side.

Where non-personal information may constitute personal information on a receiver's side, a data provision is required to:

*a* obtain a statement from the data receiver that the consent from data subject has been obtained; and

*b* keep the information on the date of data provision, the name of data receiver, etc., for three years.

***New requirement for international transfer of personal information***[45]

Where a business operator handling personal information obtains consent to transfer personal information to foreign countries, it is required to provide the data subject with the following information:

*a* the name of country to which personal information is transferred;

*b* that country's legal system in connection with data protection, to a reasonable extent; and

*c* any measure to be taken by a receiver of personal information.

Where a business operator handling personal information transfers personal information without consent because a foreign data receiver has established a system conforming to the standards set by the PPC rules, it is required to:

*a* monitor how personal information has been managed and any development or revision of personal protection law of the country in which the data receiver is located;[46]

*b* take proper actions when any problem if found in connection with the management of the personal information; and

*c* provide the data subject with specific actions taken above and relevant information if requested.[47]

45 Article 28 (2), (3) APPI.

46 The PPC has provided the information on foreign countries' data protection law for reference purposes: https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf, https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R4_03.pdf.

47 Article 18 Rules of APPI.

### v Consolidation of the existing data protection related laws into the APPI

Since its enactment, the APPI has been applied only to a business operator handling personal information and data subject. The personal information controlled by the governmental sectors has been governed by the Law for the Protection of Personal Data Held by Administrative Organs. Further, the personal information controlled by a local government has been governed by its local ordinance. To take more consistent approach to the handling of personal information, the APPI was revised on 19 May 2021 to replace those laws, and the PPC will in charge of protection of personal information held by governmental agencies as well. The revision will be in effect by 19 May 2023.

## III REGULATORY FRAMEWORK

### i Privacy and data protection legislation and standards

#### *Definitions*

*Personal information*

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

*a* information about a living person that can identify him or her by name, date of birth or other description contained in the information (including information that will allow easy reference to other information that will enable the identification of the specific individual);[48] or

*b* information about a living person that contains an individual identification code, which means any character, letter, number, symbol or other codes designated by Cabinet Order,[49] falling under any of the following items:

- those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily or partial feature of the specific individual has been converted to be provided for use by computers; and
- those characters, letters, numbers, symbols or other codes assigned in relation to the use of services provided to an individual, or to the purchase of goods sold to an individual, or that are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or stated or recoded for the said user or purchaser, or recipient of issuance.[50]

*Personal information database*

A 'personal information database'[51] is an assembly of information including:

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

48 Article 2(1)(i) APPI.

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

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

51 Article 16(1) APPI (amended in 2021 and effective on 1 April 2022).

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

*Business operator handling personal information*

A 'business operator handling personal information'[52] is a business operator using a personal information database, etc. for its business.[53] However, the following entities shall be excluded:

*a* state organs;
*b* local governments;
*c* incorporated administrative agencies, etc.;[54] and
*d* local incorporated administrative institutions.[55]

*Personal data*

'Personal data' comprises personal information constituting a personal information database, etc. (when personal information such as names and addresses is compiled as a database, it is personal data in terms of the APPI).[56]

*Anonymously processed information*

The amendment to the APPI in 2017 creates the notion of 'anonymously processed information' to promote the effective use of personal information. 'Anonymously processed information' means processed personal information from which it is not possible to identify a specific individual by deleting the information or the code identifying a specific individual.[57]

*Pseudonymously processed information*

The amendment to the APPI in 2020 creates the notion of 'pseudonymously processed information' to promote the effective internal use (e.g., analysis) of personal information inside a corporation. 'Pseudonymously processed information' means information relating to an individual that can be produced from processing personal information by deleting the information or identification code identifying a specific person so as not to identify a specific individual unless it is to be considered together with other information.[58]

52 Article 16(2) APPI (amended in 2021 and effective on 1 April 2022).

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

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

55 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).

56 Article 16(3) APPI (amended in 2021 and effective on 1 April 2022).

57 Article 16(6).

58 Article 16(5).

*Sensitive personal information*

The APPI originally did not have a definition of 'sensitive personal information'. However, for example, the Japan Financial Services Agency's Guidelines for Personal Information Protection in the Financial Field (the JFSA Guidelines)[59] had defined information related to political opinion, religious belief (religion, philosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information.[60] Furthermore, the JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[61] although some exceptions exist. Following these practices, the amendment to the APPI in 2017 explicitly provided a definition of 'sensitive personal information' and its special treatment (see Section II.i).

### ii General obligations for data handlers

***Purpose of use***

Pursuant to Article 17(1) APPI, a business operator handling personal information must as far as possible specify the purpose of that use. In this regard, the Basic Policy on the Protection of Personal Information (Basic Policy) (Cabinet Decision of 2 April 2004) prescribes as follows.

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

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

In this respect, under the previous APPI, a business operator handling personal information could not change the use of personal information 'beyond a reasonable extent'. The purpose of use after the change therefore had to be duly related to that before the change. The amendment to the APPI in 2017 has slightly expanded the scope of altering the purpose of use to enable flexible operations by prohibiting alteration of the utilisation purpose 'beyond the scope recognised reasonably relevant to the pre-altered utilisation purpose'.[62]

59 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).

60 Article 5(1) of the JFSA Guidelines (latest update April 2022, available at https://www.fsa.go.jp/common/law/kj-hogo-2/01-2.pdf).

61 Article 5(1)1–8 of the JFSA Guidelines.

62 Article 17(2) APPI (amended in 2021 and effective on 1 April 2022).

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.[63]

*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.[64]

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.[65]

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

A business operator handling personal information must endeavour to keep any personal data it holds accurate and up to date within the scope necessary for the achievement of the purpose of use. Under the APPI,[66] a business operator handling personal information also must endeavour to delete personal data without delay when it becomes unnecessary.

In addition, when a business operator handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee to ensure the secure control of the personal data.[67]

When a business operator handling personal information entrusts another individual or business operator with the handling of personal data in whole or in part, it shall also exercise necessary and appropriate supervision over the outsourcing contractor to ensure the secure control of the entrusted personal data.[68]

***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.[69]

The principal exceptions to this restriction are where:

*a* the provision of personal data is required by laws and regulations;[70]

63 Article 18(1) APPI.

64 Article 20 APPI.

65 Article 21(1) APPI.

66 Article 22 APPI.

67 Article 24 APPI. For example, providing training sessions and monitoring whether employees comply with internal rules regarding personal information protection.

68 Article 25 APPI. The APPI Guidelines point out: (1) a business operator handling personal information has to prepare rules on the specific handling of personal data to avoid unlawful disclosure and maintain the security of personal data; and (2) a business operator handling personal information has to take systemic security measures (e.g., coordinate an organisation's operations with regard to the rules on the handling of personal data, implement measures to confirm the treatment status of personal data, arrange a system responding to unlawful disclosure of personal data and review the implementation or improvement of security measures).

69 Article 27(1) APPI.

70 Article 27(1)(i) APPI. The APPI Guidelines mention the following cases: (1) response to a criminal investigation in accordance with Article 197(2) of the Criminal Procedure Law; (2) response to an

*b* a business operator handling personal information agrees, at the request of the subject, to discontinue providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the PPC and the person of the following or makes this information readily available to the person in accordance with the rules set by the PPC:[71]
- the fact that the provision to a third party is the purpose of use;
- which items of personal data will be provided to a third party;
- the method of provision to a third party;
- the fact that the provision of such personal data as might lead to the identification of the person to a third party will be discontinued at the request of the person; and
- the method of receiving the request of the person.

*c* a business operator handling personal information outsources the handling of personal data (e.g., to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;[72]

*d* personal information is provided as a result of the takeover of business in a merger or other similar transaction;[73] and

*e* personal data is used jointly between specific individuals or entities and where the following are notified in advance to the person or put in a readily accessible condition for the person:
- the facts;
- the items of the personal data used jointly;
- the scope of the joint users;
- the purpose for which the personal data is used by them; and
- the name of the individual or entity responsible for the management of the personal data concerned.[74]

***Public announcement of matters concerning retained personal data***

Pursuant to Article 32(1) APPI (amended in 2021 and effective on 1 April 2022), a business operator handling personal information must put the name of the business operator handling personal information and the purpose of use of all retained personal data in an accessible condition for the person concerned (this condition of accessibility includes cases in which a response is made without delay upon the request of the person), the procedures for responding to a request for disclosure, correction and cessation of the retention of the personal data.[75]

investigation based upon a warrant issued by the court in accordance with Article 218 of the Criminal Procedure Law; and (3) response to an inspection conducted by the tax authority.

71 Article 27(2) APPI.

72 Article 27(5)(i) APPI.

73 Article 27(5)(ii) APPI.

74 Article 27(5)(iii) APPI.

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

***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.[76]

### iii 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,[77] and provides for the implementation of a national numbering system for social security and taxation purposes. The government will adopt the social security and tax number system to enhance social security for people who truly need it, to achieve the fair distribution of burdens such as income tax payments and to develop efficient administration. The former independent supervisory authority called the Specific Personal Information Protection Commission was transformed into the PPC, which was established on 1 January 2016 to handle matters with respect to both the Number Use Act and the amendment to the APPI in 2017. This authority consists of one chair and eight commission members.[78] 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.

### iv Online direct marketing

Under the Act on Regulation of Transmission of Specified Electronic Mail[79] and the Act on Specified Commercial Transactions,[80] businesses are generally required to provide recipients with an opt-in mechanism, namely to obtain prior consent from each recipient for any marketing messages sent by electronic means. A violation of the opt-in obligation may result in imprisonment, a fine or both.

## IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

### i Extraterritorial application of the APPI

It was generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity

76 Article 34(1) APPI.

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

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

79 Act No. 26 of 17 April 2002.

80 Act No. 57 of 4 June 1976.

handling personal information in Japan. In accordance with this accepted understanding, the APPI explicitly provides that the APPI applies to a business operator located outside Japan under certain circumstances.

The provisions of the APPI apply in those cases where, in relation to provision of a good or service to a person in Japan, a business operator handling personal information has acquired personal information relating to that person and handles the personal information or anonymously processed information produced using the said personal information in a foreign country.[81]

### ii International data transfers

With some exceptions prescribed in the APPI (see Section III.ii, 'Restrictions on provision to a third party'), prior consent is required for the transfer of personal information to a third party.[82] However, there was no specific provision regarding international data transfers in the previous APPI. To deal with the globalisation of data transfers, the APPI requires the consent of the principal to international transfers of personal data[83] except in the following cases:

*a* international personal data transfer to a third party (in a foreign country) that has established a system conforming to the standards set by the PPC rules[84] (i.e., proper and reasonable measures taken in accordance with the provisions of the APPI or accreditation as a receiver of personal data according to international standards on the protection of personal information, such as being certified under the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules) for operating in a manner equivalent to that of a business operator handling personal data; and

*b* international personal data transfer to a third party in a foreign country that is considered, according to the rules of the PPC, to have established a personal information protection system with standards equivalent to those in Japan regarding the protection of an individual's rights and interests. Since 23 January 2019, the EU has been considered a jurisdiction that provides the same level of protection of personal data in Japan. The PPC will review this designation within two years and then continues to review every four years or at any time when the PPC considers it to be necessary.[85]

## V COMPANY POLICIES AND PRACTICES

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

81 Article 171 APPI.

82 Article 27(1) APPI.

83 Article 28 APPI.

84 Article 16 Rules of the PPC.

85 The PPC Announcement No. 1 (23 January 2019), https://www.ppc.go.jp/files/pdf/210101_h31iinkaikokuji01.pdf, the designated countries include Iceland, Ireland, Italy, the United Kingdom, Estonia, Austria, the Netherlands, Cyprus, Greek, Croatia, Sweden, Spain, Slovakia, Slovenia, Czech Republic, Denmark, Germany, Norway, Hungary, Finland, France, Bulgaria, Belgium, Poland, Portugal, Malta, Latvia, Lithuania, Liechtenstein, Romania and Luxembourg.

86 Article 23 APPI.

*Systemic security control measures*

Systemic security control measures are required for:

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

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

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

*d* assessing, reviewing and improving the security control measures for personal data; and responding to data security incidents or violations.[87]

*Human security control measures*

Human security control measures are required for:

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

*b* familiarising workers with internal regulations and procedures through education and training.[88]

*Physical security control measures*

Physical security control measures are required for:

*a* implementing controls on entering and leaving a building or room where appropriate; preventing theft, etc.; and

*b* physically protecting equipment and devices.[89]

*Technical security control measures*

Technical security control measures are required for:

*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.[90]

87 10-3 (Systemic Security Control Measures) of the APPI Guidelines, p. 88.

88 10-4 (Human Security Control Measures) and 3-4-3 (Supervision of Employees) of the APPI Guidelines, pp. 92, 41.

89 10-5 (Physical Security Control Measures) of the APPI Guidelines, p. 93.

90 10-6 (Technical Security Control Measures) of the APPI Guidelines, p. 96.

## 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.[91] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed where disclosure:

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

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

*c* violates other laws and regulations.[92]

## VII PUBLIC AND PRIVATE ENFORCEMENT

### i Enforcement and sanctions

***Enforcement agencies***

Prior to the amendment, the enforcement agencies in data protection matters were the Consumer Affairs Agency, and ministries and agencies concerned with jurisdiction over the business of the relevant entities. Under the APPI, the PPC is the sole enforcement authority and it may transfer its authorities to request for report and to inspect to ministries and agencies if necessary for effective recommendations and orders under Article 147.[93]

91 The method specified by a Cabinet Order under Article 33(2) APPI shall be the provision of documents (or 'the method agreed upon by the person requesting disclosure, if any'). Alternatively, according to the APPI Guidelines, if the person who made a request for disclosure did not specify a method or make any specific objections, then they may be deemed to have agreed to whatever method the disclosing entity employs.

92 Article 33(2) APPI.

93 Article 147 APPI.

***Main penalties***[94]

A business operator that violates orders issued under Paragraphs 2 or 3 of Article 145 (recommendations and orders by the PPC in the event of a data security breach) shall be sentenced to imprisonment with forced labour of not more than one year or to a fine of not more than ¥1 million where a business operator is a corporation; the upper limit of the fine shall be ¥100 million.[95]

A business operator that does not make a report[96] as required by Articles 143 or 150 or that has made a false report shall be sentenced to a fine of not more than ¥500,000.[97]

**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 25 APPI).[98]

***Information breach at a mobile phone company***

The email addresses of a mobile phone company were reset and email addresses of the customers and the mail texts were disclosed to third parties. In January 2012, the Ministry of Internal Affairs and Communications (MIC) promulgated an administrative guidance requesting 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 23[99] APPI).[100]

***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

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

95 Article 173 APPI.

96 The PPC may have a business operator handling personal information make a report on the handling of personal information to the extent necessary for fulfilling the duties of a business operator (Articles 143 and 150 APPI).

97 Article 177 APPI.

98 3-4-4 of the APPI Guidelines.

99 3-4-2 of the APPI Guidelines.

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

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 23 APPI and Article 12 of the MIC Guideline on Protection of Personal Information in Telecommunications.[101] There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 25 APPI and Article 13 of the above-mentioned MIC Guideline).[102]

***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.[103]

***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 23 APPI. There was also found to be a violation of the duty regarding the supervision of an outsourcing contractor under Article 25 APPI). Benesse Corporation actually distributed a premium ticket (with a value of ¥500) to its customers to compensate for the damage incurred by the customers. Currently, however, a lawsuit is pending before the Supreme Court brought by a customer requesting damages of ¥100,000 (Osaka High Court dismissed the customer's claim). On 29 October 2017, the Supreme Court sent the case back to Osaka High Court for further examination, holding that Osaka High Court erred in stating that any concern over the leak of personal information without any monetary damage is insufficient to establish any damage against the appellant (customer) under Article 709 of the Civil Code. At the time of writing, it is anticipated that Osaka High Court will hand down a new decision clarifying the liability of businesses handling personal information for the leaking of customer's personal information and a method of calculating the amount of damages arising from the information leak.

Further, in a case where a different plaintiff filed a lawsuit against Benesse Corporation, on 20 June 2018, the Tokyo District Court denied measurable damages caused by Benesse Corporation's negligence as in the Osaka High Court decision above. The plaintiff appealed and on 27 June 2019, the Tokyo High Court overturned the District Court's decision, holding that the appellant (plaintiff) was mentally injured by any possibility of the use of his

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

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

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

personal information without his consent (e.g., unknown persons could contact him directly by using his leaked private address) and the compensation for such mental damage amounts to ¥2,000 per data subject.

***Unlawful provision of personal data to third parties***

In 2018, an employment recruiting service provider (Recruit Careers) collected personal information on university and college students who were job hunting (name, address, school name and other details such as job preference, interest in companies) through its website, which was popular among student looking for jobs. Using artificial intelligence technology, Recruit Careers calculated and provided companies with students' expected rates of declination of job offers. However, Recruit Careers did not obtain consent to provide such personal data to third-party companies, which violated Article 27 of the APPI. The PPC issued recommendations for improvement to Recruit Careers on 26 August 2019. Further to this, on 4 December 2019, the PPC issued recommendations for improvement to some client companies because they had not disclosed expected rates of declination service as the purpose of use when providing applicants' personal information to Recruit Careers, and because they did so without obtaining the applicants' consent.[104]

***Insufficient management of the access to personal information by a third party vendor***

A social network company, LINE corporation has provided free communication tool called 'LINE' in Japan. On 17 March 2021, it was revealed by a news reporting that LINE users' personal information obtained through LINE services has been transferred to China and could be accessed by Chinese maintenance service companies. As many users had not expected this data transfer to China, the company was criticised fiercely about its data management. On 23 April 2021, the PPC issued an instruction suggesting that LINE Corporation improve the management of third party vendors that may have access to users' personal information and take necessary measures to protect more strongly users' personal information (e.g., by recording access logs and monitoring the handling of personal information by its third party vendors).[105]

***Illegal provision of personal information to the public by a business operator***

A business operator has created and maintained on the website a database of personal information on bankrupt persons based upon an official gazette publicly announcing the commencement of bankruptcy procedures without consent from the bankrupt persons. The database was accessible from and searchable by anyone, and it may have caused discrimination against such bankrupt persons. On 18 February 2022, the PPC issued an instruction urging the business operator to stop making the database workable until getting consent to the provision of such data to third parties from the bankrupt persons and taking necessary protective measures. The business operator did not, however, follow the PPC's instruction and accordingly, on 23 March 2022, the PPC issued an order to take the actions above, the failure of which may be subject to criminal penalty.[106]

104 https://www.ppc.go.jp/files/pdf/191204_houdou.pdf (available only in Japanese).

105 https://www.ppc.go.jp/files/pdf/210423_houdou.pdf (available only in Japanese).

106 https://www.ppc.go.jp/files/pdf/220323_houdou.pdf (available only in Japanese).

## VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

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

Further, the amendment to the APPI in 2020 expands extraterritorial application of the APPI and the PPC may require a foreign organisation to report what it needs and imposes upon a business operator engaging in international data transfer an obligation to provide a data subject with information on how such personal data is protected by foreign data receivers (see Section II.iii).

## IX CYBERSECURITY AND DATA BREACHES

### i Cybersecurity

The amendments to the Criminal Code,[107] 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[108] (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,[109] 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.[110]

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

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

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

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

Finally, the Basic Act on Cybersecurity, which provides the fundamental framework of cybersecurity policy in Japan, was passed in 2014.[111]

### ii Data security breach

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

*a* internal report on the data breach, etc. and measures to prevent expansion of the damage;
*b* investigation into any cause of the data breach, etc.;
*c* confirmation of the scope of those affected by the data breach, etc.;
*d* consideration and implementation of preventive measures;
*e* notifications to any person (to whom the personal information belongs) affected by the data breach etc.;
*f* prompt public announcement of the facts of the data breach, etc. and preventive measures to be taken; and
*g* prompt notifications to the PPC about the facts of the data breach, etc. and preventive measures to be taken except for where the data breach, etc. has caused no actual, or only minor, harm (e.g., wrong transmissions of facsimiles or emails that do not include personal data other than names of senders and receivers).[112]

In addition, the PPC has the authority to collect reports from, or advise, instruct or give orders to, the data controllers.[113]

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

## X OUTLOOK

### i Triennial review to be conducted by the APPI

As stated in Section II, the amendment to the APPI, which entered fully into force in May 2017, drastically changed the legal framework for the protection of personal information in Japan. The PPC has continued to hear from relevant parties for its review of the APPI every three years, and has monitored day-to-day practice in various sectors of Japanese society. Actually, the PPC's review and monitoring led to the amendment of the APPI in 2020. In accordance with Article 12 of the supplemental provisions of the APPI, the PPC is continuing to monitor the handling of personal information and personal data and will consider whether the current law needs to be updated for the next three years. It is generally expected that the PPC may propose some revisions of the APPI in 2023 based upon ongoing review.

111 Act No. 104 of 12 November 2014.
112 PPC Announcement No.1 of 2017.
113 Articles 143–145 APPI.

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

As stated in Section VII, Tokyo High Court expressed its views regarding the damage caused by a data breach case in the *Benesse* case and this case has been appealed to the Supreme Court. In addition, another case (see Section VII.ii) in connection with Benesse's data leakage is still pending before Osaka High Court. The Supreme Court may revisit the *Benesse* data leakage case and clarify the extent and scope of the duty of care of business operators handling personal information and the calculation of damages arising from data breaches caused by a violation of such duty of care.

### iii Guidelines are to be updated by the PPC

In accordance with the amendment to the APPI in 2020 and 2021, the PPC has been engaged with necessary updates of the guidelines (the Guidelines) initially set out in 2017, following the public comments procedure. The updated Guidelines were finally published on 8 September 2022 (effective on 1 April 2023). To comply with the revised APPI, a business operator handling personal information should regularly pay attention to new guidance updated by the PPC. As mentioned in Section II.v, the PPC's role and power have been strengthened and the PPC has been expected to more actively and severely monitor and supervise the management of personal information. For this reason, a business operator should pay more and more attention to the Guidelines and make and follow its own internal rules on the management of personal information in line with the Guidelines.

### iv Monitoring a foreign business operator handling personal information

As stated in Section VIII, as a result of the amendment to the APPI in 2020, the PPC has new power to instruct a foreign business operator handling personal information related to products and services provided to Japan. As the PPC may publicly announce any violation of its order if a foreign business operator does not follow the PPC's instructions, it will undermine its reputation. As of 12 September 2022, no such instruction to a foreign business operator handling personal information exists but it should continue to pay careful attention to its compliance with the requirements under the APPI.

**Appendix 1**

# ABOUT THE AUTHORS


**TOMOKI ISHIARA**

*Sidley Austin Foreign Law Joint Enterprise*


Mr Ishiara's practice areas include corporate law, intellectual property law, antitrust law, data security and privacy law, entertainment law, investigation, litigation and arbitration. Mr Ishiara has extensive experience in the field of corporate law and intellectual property law. In addition, Mr Ishiara regularly advises foreign clients on Japanese regulatory matters on finance, life sciences and anti-bribery matters.


**SIDLEY AUSTIN LLP**

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

ISBN 978-1-80449-116-4