

Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto



Publisher

Tom Barnes
tom.barnes@lbresearch.com

Subscriptions

Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager

Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by

Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between May and August 2020. Be advised that this is a developing area.

© Law Business Research Ltd 2020
No photocopying without a CLA licence.
First published 2012
Ninth edition
ISBN 978-1-83862-322-7

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



Data Protection & Privacy

2021

Contributing editors**Aaron P Simpson and Lisa J Sotto****Hunton Andrews Kurth LLP**

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.



London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction	5	Germany	95
Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP		Peter Huppertz Hoffmann Liebs Fritsch & Partner	
EU overview	9	Greece	102
Aaron P Simpson, Claire François and James Henderson Hunton Andrews Kurth LLP		Vasiliki Christou Vasiliki Christou, Attorney at Law	
The Privacy Shield	12	Hong Kong	109
Aaron P Simpson and Maeve Olney Hunton Andrews Kurth LLP		Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown	
Australia	17	Hungary	118
Alex Hutchens, Jeremy Perier and Meena Muthuraman McCullough Robertson		Endre Várady and Eszter Kata Tamás VJT & Partners Law Firm	
Austria	25	India	126
Rainer Knyrim Knyrim Trieb Rechtsanwälte		Stephen Mathias and Naqeeb Ahmed Kazia Kochhar & Co	
Belgium	33	Indonesia	133
David Dumont and Laura Léonard Hunton Andrews Kurth LLP		Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Noor Prayoga Mokoginta AKSET Law	
Brazil	45	Italy	142
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados		Paolo Balboni, Luca Bolognini, Antonio Landi and Davide Baldini ICT Legal Consulting	
Canada	53	Japan	150
Doug Tait and Catherine Hamilton Thompson Dorfman Sweatman LLP		Akemi Suzuki and Tomohiro Sekiguchi Nagashima Ohno & Tsunematsu	
Chile	60	Malaysia	159
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya Magliona Abogados		Jillian Chia Yan Ping and Natalie Lim SKRINE	
China	67	Malta	166
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown		Terence Cassar, Ian Gauci and Bernice Saliba GTG Advocates	
Colombia	76	Mexico	174
María Claudia Martínez and Daniela Huertas Vergara DLA Piper		Abraham Diaz and Gustavo A Alcocer OLIVARES	
France	83	Netherlands	182
Benjamin May and Farah Benchelha Aramis Law Firm		Inge de Laat and Margie Breugem Rutgers Posch Visée Endedijk NV	

New Zealand	190	Sweden	253
Derek Roth-Biester and Megan Pearce Anderson Lloyd Lawyers		Henrik Nilsson Wesslau Söderqvist Advokatbyrå	
Portugal	197	Switzerland	261
Helena Tapp Barroso and Tiago Félix da Costa Morais Leitão, Galvão Teles, Soares da Silva & Associados		Lukas Morscher and Leo Rusterholz Lenz & Staehelin	
Romania	206	Taiwan	271
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Laura Dinu MPR Partners Maravela, Popescu & Asociații		Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang Formosa Transnational Attorneys at Law	
Russia	214	Turkey	278
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian L Zimble Morgan Lewis		Esin Çamlıbel, Beste Yıldızili Ergül and Naz Esen Turunç	
Serbia	222	United Kingdom	286
Bogdan Ivanišević and Milica Basta BDK Advokati		Aaron P Simpson, James Henderson and Jonathan Wright Hunton Andrews Kurth LLP	
Singapore	229	United States	296
Lim Chong Kin and Charis Seow Drew & Napier LLC		Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP	
South Korea	243		
Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim LAB Partners			

Japan

Akemi Suzuki and Tomohiro Sekiguchi

Nagashima Ohno & Tsunematsu

LAW AND THE REGULATORY AUTHORITY

Legislative framework

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

The Act on the Protection of Personal Information of 2003, as amended (the APPI), sits at the centre of Japan's regime for the protection of PII. Serving as a comprehensive, cross-sectoral framework, the APPI regulates private businesses using databases of PII and is generally considered to embody the eight basic principles under the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Use of PII by the public sector is regulated by separate statutes or local ordinances providing for rules for protection of PII held by governmental authorities.

In September 2015, the first significant amendment to the APPI (the Amendment) since its introduction was promulgated. The Amendment aims to eliminate the ambiguity of the current regulatory framework and facilitate the proper use of personal data by businesses while strengthening the protection of privacy. It also aims to address global data transfers and harmonise Japan's data protection regime with that of other major jurisdictions. The Amendment was fully implemented on 30 May 2017.

The APPI, as amended by the Amendment, is implemented by cross-sectoral administrative guidelines prepared by the Personal Information Protection Commission (the Commission). With respect to certain sectors, such as medical, financial and telecommunications, the Commission and the relevant governmental ministries have published sector-specific guidance providing for additional requirements given the highly sensitive nature of personal information handled by private business operators in those sectors. Numerous self-regulatory organisations and industry associations have also adopted their own policies or guidelines for the protection of PII.

Data protection authority

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

The Personal Information Protection Commission (the Commission) was established on 1 January 2016 as a cross-sectoral, independent governmental body to oversee the APPI. The Commission has the following powers under the APPI:

- to require reports concerning the handling of PII or anonymised information from private business operators using 'databases, etc' of PII (PII databases) or private business operators using PII

databases, of anonymised information (for the purposes of this chapter, anonymised information users);

- to conduct an on-site inspection of offices or other premises of PII data users and anonymised information users in order to raise questions and inspect records with respect to their handling of PII or anonymised information;
- to give 'guidance' or 'advice' necessary for the handling of PII or anonymised information to PII data users and anonymised information users;
- upon violation of certain obligations of any PII data users or anonymised information users and to the extent deemed necessary to protect the rights of an affected individual, to 'recommend' cessation or other measures necessary to rectify the violation; and
- if recommended measures are not implemented and the Commission deems imminent danger to the affected individual's material rights, to order such measures.

The Commission may delegate the power to require reports or conduct an on-site inspection as mentioned above to certain governmental ministries in cases where the Commission deems it necessary to be able to give 'guidance' or 'advice' to PII data users or anonymised information users effectively.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Under the APPI, in cases where governmental ministries deem it necessary to ensure the proper handling of personal information, such governmental ministries may request the Commission to take appropriate measures in accordance with the provisions of the APPI.

In addition, under the APPI, the Commission may provide foreign authorities enforcing foreign laws and regulations equivalent to the APPI with information that the Commission deems beneficial to the duties of such foreign authorities that are equivalent to the Commission's duties set forth in the APPI. Upon request from the foreign authorities, the Commission may consent that the information provided by the Commission be used for an investigation of a foreign criminal case, subject to certain exceptions.

Breaches of data protection

- 4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under the APPI, criminal penalties may be imposed if:

- a PII data user or an anonymised information user fails to comply with any order issued by the Commission (subject to penal servitude of up to six months or a criminal fine of up to ¥300,000);
- a PII data user or an anonymised information user fails to submit reports, or submits untrue reports, as required by the Commission (subject to a criminal fine of up to ¥300,000);
- a PII data user or an anonymised information user refuses or interrupts an on-site inspection of the offices or other premises by the Commission (subject to a criminal fine of up to ¥300,000); or
- any current or former officer, employee or representative of a PII data user provides to a third party or steals information from a PII database he or she handled in connection with the business of the PII data user with a view to providing unlawful benefits to himself or herself or third parties (subject to penal servitude of up to one year or a criminal fine of up to ¥500,000).

If the foregoing offences are committed by an officer or employee of a PII data user or an anonymised information user that is a judicial entity, then the entity itself may also be held liable for a criminal fine.

SCOPE

Exempt sectors and institutions

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

The Act on the Protection of Personal Information of 2003, as amended (the APPI) contains notable exemptions, as follows:

- In respect of fundamental constitutional rights, media outlets and journalists, universities and other academic institutions, religious groups and political parties are exempt from the APPI to the extent of the processing of personal data for purposes of journalism, academic research, and religious and political activities, respectively.
- The use of personally identifiable information (PII) for personal purposes is outside the scope of the APPI. The use of PII by not-for-profit organisations or sole proprietorships is within the scope of the APPI.

Communications, marketing and surveillance laws

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

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

Other laws

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

Use of personal information by governmental sectors is regulated by the Act on the Protection of Personal Information Held by Administrative Organs of 2003, the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies of 2003 and various local ordinances providing rules for the protection of PII held by local governments. In addition, the Act on Utilisation of Numbers to Identify Specific Individuals in Administrative Process provides rules concerning the use of personal information acquired through the use of the individual social security and tax numbering system called My Number.

With respect to employee monitoring, while there is no statute regulating employee monitoring in Japan, the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines) provide for the best practice in cases of carrying out employee monitoring.

PII formats

- 8 | What forms of PII are covered by the law?

In terms of forms of PII, the use of 'databases, etc' of PII (PII databases) is covered by the APPI. 'PII databases' includes electronic databases and manual filing systems that are structured by reference to certain classification criteria so that information on specific individuals is easily searchable.

For purposes of the APPI, 'PII' is defined as information related to a living individual that can identify the specific individual by name, date of birth or other description contained in such information. Information that, by itself, is not personally identifiable but may be easily linked to other information and thereby can be used to identify a specific individual is also regarded as PII. PII also includes signs, code or data that identify physical features of specific individuals, such as fingerprint or face recognition data, or that are assigned to each individual by government or providers of goods or services, such as a driving licence number or passport number. PII comprising a PII database is called PII data.

In addition, the amendment to the APPI (the Amendment) introduced the concept of 'anonymised information'; that is, personal information of a particular individual that has been irreversibly processed in such a manner that the individual is no longer identifiable. Anonymised information that complies with the requirements of the techniques and processes for anonymisation under the Amendment is not considered PII. Anonymised information may be disclosed to third parties without the consent of the relevant individual, provided that the business operator who processes and discloses anonymised information to third parties comply with certain disclosure requirements.

Extraterritoriality

- 9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The APPI has limited extraterritorial application. Specifically, the APPI is applicable to foreign PII data users or anonymised information users when they use or process, outside of Japan:

- PII of individuals residing in Japan as was obtained in connection with the provision of goods or services by the PII data users to Japanese resident individuals; or
- anonymised information produced by the PII data users based on such PII.

Separately, PII of individuals residing outside of Japan is considered to be protected under the APPI as long as such PII is held by private business operators established or operating in Japan.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The APPI distinguishes between:

- 1 obligations imposed on PII data users; and
- 2 obligations imposed only on those PII data users who control the relevant PII data (for the purposes of this chapter, PII data owners).

Generally, service providers are subject to the obligations of PII data users but not subject to the obligations of PII data owners.

The obligations of all PII data users mentioned in (1) include:

- to specify the purposes for which the PII is used as explicitly as possible;
- to process the PII only to the extent necessary for achieving such specified purposes unless the relevant individual's prior consent is obtained, subject to limited exceptions;
- to notify the relevant individual of, or publicise, the purposes of use prior to or at the time of collecting PII unless such purposes were publicised prior to the collection of the PII;
- not to use deceptive or wrongful means in collecting PII;
- to obtain the consent of the individual prior to collecting sensitive personal information, which includes race, beliefs, social status, medical history, criminal records and the fact of having been a victim of a crime and disabilities (subject to certain exceptions);
- to endeavour to keep its PII data accurate and up to date to the extent necessary for the purposes of use, and erase, without delay, its PII data that is no longer needed to be used;
- to undertake necessary and appropriate measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the PII data it holds;
- to conduct necessary and appropriate supervision over its employees and its service providers who process its PII data;
- not to disclose the PII data to any third party without the consent of the individual (subject to certain exemptions);
- to prepare and keep records of third-party transfers of personal data (subject to certain exceptions);
- when acquiring personal data from a third party other than data subjects (subject to certain exceptions), to verify the name of the third party and how the third party acquired such personal data; and
- not to conduct cross-border transfers of personal data without the consent of the individual (subject to certain exceptions).

The PII data owners mentioned in (2) have additional and more stringent obligations, which are imposed only in respect to PII data for which a PII data owner has the right to provide a copy of, modify (ie, correct, add or delete), discontinue using, erase and discontinue disclosing to third parties (retained PII data):

- to make accessible to the relevant individual certain information regarding the retained PII data, including:
 - the name of the PII data owner;
 - all purposes for which retained PII data held by the PII data owner is generally used; and
 - procedures for submitting a request or filing complaints to the PII data owner;
- to provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (subject to certain exceptions);

- to correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon the request of the relevant individual (subject to certain exceptions);
- to discontinue the use of or erase such retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI (subject to certain exceptions); and
- to discontinue disclosure of retained PII data to third parties upon the request of the relevant individual if such disclosure is or was made in violation of the APPI (subject to certain exceptions).

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

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

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

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

The Act on the Protection of Personal Information of 2003, as amended (the APPI) does not contain specific criteria for legitimate data collection or processing. The APPI does, however, prohibit the collection of personally identifiable information (PII) by deceptive or wrongful means, and requires that the purposes of use must be identified as specifically as possible, and must generally be notified or made available to the relevant individual in advance. Processing of PII beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

The APPI imposes stringent rules for sensitive personal information, including race, beliefs, social status, medical history, disabilities, criminal records and the fact of having been a victim of a crime. Collection or disclosure under the 'opt-out' mechanism of sensitive personal information without the consent of the relevant individual is generally prohibited.

In addition, the administrative guidelines for the financial sector provide for a similar category of sensitive information. Such information is considered to include trade union membership, domicile of birth and sexual orientation, in addition to sensitive personal information. The collection, processing or transfer of such sensitive information by financial institutions is prohibited, even with the consent of the relevant individual, except under limited circumstances permitted under such administrative guidelines.

Further, in January 2019, upon the decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the European Union's General Data Protection Regulation (GDPR), the administrative guidelines regarding

the handling of PII data transferred from the European Economic Area (EEA) based on an adequacy decision by the European Commission (EEA Data Guidelines) have taken effect. The EEA Data Guidelines imposes stringent rules for the PII data transferred from the EEA based on an adequacy decision by the European Commission (EEA data). The guidelines can be summarised as follows:

- 1 In cases where EEA data includes data concerning sex life, sexual orientation or trade union membership it is categorised as a special category of PII data under the GDPR, such EEA data is treated as 'sensitive personal information' under the APPI.
- 2 EEA data is treated as retained PII data under the APPI, regardless of whether or not such EEA data is erased within six months.
- 3 When a PII data user receives EEA data from the EEA, the PII data user is required to confirm and record the purposes of use of such EEA data specified at the time of acquisition from the relevant data subject (original purposes of use).
- 4 When a PII data user receives EEA data from another PII data user who received such EEA data from EEA, the PII data user is also required to confirm and record the original purposes of use of such EEA data.
- 5 In each case of (3) and (4), the PII data user must specify the purposes of use of EEA data within the scope of the original purposes of use of such EEA data, and use such EEA data in accordance with such specified purposes of use.
- 6 When a PII data user processes EEA data to create anonymised information under the APPI, the PII data user is required to delete any information that could be used to re-identify the relevant individuals, including any information concerning method of process for anonymisation.
- 7 In cases where a PII data user proposes to transfer EEA data it received from the EEA on to a third party transferee located outside of Japan (ie, onward transfer), the PII data user must:
 - provide the data subjects of such EEA data with information concerning the transferee, and obtain prior consent to the proposed cross-border transfer from data subject; or
 - transfer relying on applicable exemptions of such cross-border transfer.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

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

There are several notification requirements under the Act on the Protection of Personal Information of 2003, as amended (the APPI).

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

Second, when a PII data user is to disclose PII data to third parties without the individual's consent under the 'opt-out' mechanism, one of the requirements that the PII data user must satisfy is that certain information regarding the third-party disclosure is notified, or made easily accessible, to the individual prior to such disclosure. Such information includes types of information being disclosed and the manner of disclosure.

Third, when a PII data user is to disclose PII data to third parties without the individual's consent under the 'joint-use' arrangement, the PII data user must notify or make easily accessible, certain information

regarding the third-party disclosure prior to such disclosure. Such information includes items of PII data to be jointly used, the scope of third parties who would jointly use the PII data, the purpose of use by such third parties, and the name of a party responsible for the control of the PII data in question.

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

Exemption from notification

14 | When is notice not required?

There is an exception to the notice requirement imposed on a PII data user when collecting PII where, among other circumstances:

- such notice would harm the interest of the individual or a third party;
- such notice would harm the legitimate interest of the PII data user; and
- the purposes of use are evident from the context of the collection of the relevant PII data.

Control of use

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

A PII data owner must:

- 1 disclose, without delay, retained PII data in written form to the relevant individual upon his or her request;
- 2 correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon request from the relevant individual;
- 3 discontinue the use of or erase the retained PII data upon the request of the relevant individual if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI; and
- 4 discontinue disclosure to third parties of retained PII data upon the request of the relevant individual if such disclosure is or was made in violation of the APPI.

Exemptions from obligations (3) and (4) is available where the discontinuance or erasure costs significantly or otherwise impose hardships on the PII data owner and one or more alternative measures to protect the individual's interests are taken.

Data accuracy

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

The APPI requires all PII data users to endeavour to:

- keep the PII data they hold accurate and up to date to the extent necessary for the purposes for which the PII data is to be used; and
- erase, without delay, such PII data that is no longer needed.

Amount and duration of data holding

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

No. PII data may be held as long as is necessary for the purposes for which it is used. Under the APPI, PII data users must endeavour to erase, without delay, such PII data that is no longer needed to be used.

Finality principle

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

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

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

Use for new purposes

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

Under the APPI, the purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be related to the previous purposes.

PII may be used for such amended purposes, provided that the amended purposes be notified or made available to the affected individuals.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The Act on the Protection of Personal Information of 2003, as amended (the APPI) provides that all personally identifiable information (PII) data users must have in place 'necessary and appropriate' measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the PII data they hold or process; and conduct necessary and appropriate supervision over their employees and service providers who process such PII data. What constitutes 'necessary and appropriate' security measures is elaborated on in the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines). The Commission Guidelines set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical – as well as the requirement to adopt internal security rules or policies.

Some of the sector-specific guidelines, such as the administrative guidelines for the financial sector, provide for more stringent requirements on security measures.

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The APPI does not include obligations to notify the regulators or affected individuals of any breaches of security. However, upon the occurrence of any such breach, notification to the Commission, governmental ministries delegated by the Commission or an accredited personal information protection organisation, if applicable, is generally required or recommended under the Commission Guidelines. Such reporting is not required if the compromised personal data is considered not to have leaked; for instance, if the relevant personal data is securely encrypted, was recovered before a third party had access to it or was destroyed and no third party is reasonably expected to view the relevant personal data. Regulatory reporting is also not required if the relevant data breach is minor; for instance, erroneous transmission of emails or facsimiles or wrong delivery of packages where the compromised personal data is limited to the names of the sender and recipient.

In addition, under the Commission Guidelines, notification of data breaches to data subjects may be necessary depending on the subject and manner of such breaches. If a particular data breach is not expected to result in damage to the relevant data subjects, such as where the breached personal data was securely encrypted, notification to data subjects will not be necessary.

Some of the sector-specific administrative guidelines provide for more stringent requirements on notification of data breaches. For instance, under the administrative guidelines for the financial sector, upon the occurrence of any data breach, notifications to both the relevant government ministries and the data subject are required for PII data users in the financial sector without any exceptions.

INTERNAL CONTROLS

Data protection officer

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

There is no statutory requirement to appoint a data protection officer. However, the appointment of a 'chief privacy officer' is generally recommended under the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines). The Commission Guidelines do not provide for the qualifications, roles or responsibilities of a chief privacy officer.

Record keeping

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

Personally identifiable information (PII) data users are generally required under the Commission Guidelines to establish internal processes to safeguard PII data.

Under the APPI, PII data users that have disclosed PII data to third parties must generally keep records of such disclosure. In addition, PII data users receiving PII data from third parties rather than the relevant individuals must generally verify how the PII data was acquired by such third parties and keep records of such verification.

The foregoing obligation is not applicable to disclosure of PII data to outsourced processing service providers, as part of mergers and acquisitions transactions or for joint use, as long as the disclosure is not subject to the cross-border transfer restrictions.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

No. However, the Commission Guidelines generally require that, when implementing security measures to safeguard the PII data it holds or processes, each PII data user should consider the degree of the impact of any unauthorised disclosure or other incident on the right or interest of one or more data subjects affected by such an incident.

REGISTRATION AND NOTIFICATION

Registration

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

Under Act on the Protection of Personal Information of 2003, as amended (the APPI), personally identifiable information (PII) data users who disclose PII data (other than sensitive personal information) under the 'opt-out' mechanism are required to submit a notification to the Personal Information Protection Commission prior to such disclosure. According to the Commission, the primary target of this requirement is mailing list brokers.

Formalities

26 | What are the formalities for registration?

PII data users who disclose PII data under the 'opt-out' mechanism are required to notify the Commission, in a prescribed format, of the categories of personal data to be disclosed, the method of disclosure, the manner in which the relevant individual may request to cancel such 'opt-out' disclosure to the PII data users and other designated matters. Upon receipt of such notification, the Commission will publicise certain information included in the notification.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

No penalties are statutorily provided for the failure to submit a notification of the 'opt-out' disclosure.

Refusal of registration

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

Not applicable.

Public access

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

Notifications of the 'opt-out' disclosure mentioned are partially made public on the Commission's website.

Effect of registration

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

A notification of the 'opt-out' disclosure is a requirement to lawfully disclose PII data (other than sensitive personal information) to third parties without the relevant individual's consent under the 'opt-out' mechanism.

Other transparency duties

31 | Are there any other public transparency duties?

Apart from the matters required under the APPI to notify individuals as separately mentioned in this chapter, the Commission Guidelines recommend that PII data users make public an outline of the processing of PII data such as whether PII data users outsource the processing of PII data and the contents of the processing to be outsourced.

In addition, the administrative guidelines for the financial sector recommend that PII data users make public:

- the purpose of use of personal information specified in accordance with types of customers;
- whether PII data users outsource the processing of PII data;
- the contents of the processing to be outsourced;
- the types of personal information;
- the methods of obtaining personal information; and
- a statement to the effect that upon request from individuals, the use of retained PII data will be discontinued.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

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

The Act on the Protection of Personal Information of 2003, as amended (the APPI) generally prohibits disclosure of personally identifiable information (PII) data to third parties without the relevant individual's consent. As an exception to such prohibition, the transfer of all or part of PII data to persons that provide outsourced processing services is permitted to the extent such services are necessary for achieving the permitted purposes of use. PII data users are required to engage in 'necessary and appropriate' supervision over such service providers in order to safeguard the transferred PII data. Necessary and appropriate supervision by PII data users is generally considered to include proper selection of service providers; entering into a written contract setting forth necessary and appropriate security measures; and collecting necessary reports and information from the service providers.

Restrictions on disclosure

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

In principle, the APPI prohibits disclosure of PII to a third party without the individual's consent. Important exceptions to the general prohibition include the following, in addition to disclosure for outsourced processing services:

Disclosure under the 'opt-out' mechanism

A PII data user may disclose PII data to third parties without the individual's consent, provided that it is prepared to cease such disclosure upon request from the individual; certain information regarding such disclosure is notified, or made easily accessible, to the individual prior to such disclosure; and such information is notified to the Commission in advance.

Transfer in mergers and acquisitions transactions

PII data may be transferred without the consent of the individual in connection with the transfer of business as a result of a merger or other transactions.

Disclosure for joint use

A PII data user may disclose PII data it holds to a third party for joint use, provided that certain information regarding such joint use is notified, or

made easily accessible, to the individual prior to such disclosure. Such disclosure is most typically made when sharing customer information among group companies to provide seamless services within the permitted purposes of use. Information required to be notified or made available includes items of PII data to be jointly used, the scope of third parties who would jointly use the PII data, the purpose of use by such third parties, and the name of a party responsible for the control of the PII data in question.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

Under the APPI, the transfer of PII data to a third party located outside Japan is generally subject to prior consent of the relevant individual, subject to the important exceptions mentioned below.

First, no prior consent of the relevant individual is required if the third party is located in a foreign country that the Commission considers has the same level of protection of personal information as Japan. On 23 January 2019, countries in the European Economic Area were designated as such by the Personal Information Protection Commission in exchange for the parallel decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the General Data Protection Regulation.

The second exception is applicable where the relevant third-party transferee has established a system to continuously ensure its undertaking of the same level of protective measures as PII data users would be required under the APPI. According to the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines), for this exception to apply, the PII data user and the foreign third party may ensure in a contract that the third party undertakes such protective measures; and if the third party is an intra-group affiliate, the data user and the foreign third party may rely on a privacy statement or internal policies applicable to the group that are appropriately drafted and enforced.

In addition, this exception is generally applicable if the foreign third party has certification from an internationally recognised framework of protection of personal data; specifically, certification under the Asia-Pacific Economic Cooperation's Cross Border Privacy Rules system.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

No, cross-border transfer of personally identifiable information (PII) does not trigger a requirement to notify or obtain authorisation from a supervisory authority.

Further transfer

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

The restrictions on the cross-border transfers of PII under the APPI are equally applicable to transfers to service providers. They may also be applicable to onward transfers in the sense that the initial PII data users must ensure that not only the transferors of such onward transfers but also their transferees adhere to the cross-border restrictions of the APPI.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

The Act on the Protection of Personal Information of 2003, as amended (the APPI) imposes on personally identifiable information (PII) data owners, obligations to respond to individuals' requests for access to their PII data. Specifically, upon request from individuals, PII data owners are obligated to disclose, without delay, retained PII data of the requesting individuals (the obligation of disclosure). Such disclosure, however, is exempted as a whole or in part if such disclosure would:

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

The Amendment clarifies that individuals have the right to require disclosure of their PII held by PII data owners.

Other rights

38 | Do individuals have other substantive rights?

Under the APPI, upon request from individuals, PII data owners are obligated to:

- correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use – the obligations of correction etc;
- discontinue the use of or erase the retained PII data if such use is or was made, or the retained PII data in question was obtained, in violation of the APPI (subject to certain exceptions) – the obligation of cessation of use, etc); and
- discontinue disclosure to third parties of retained PII data if such disclosure is or was made in violation of the APPI (subject to certain exceptions) – the obligation of cessation of third-party disclosure.

Under the Amendment, individuals have the right to require PII data owners to correct, add or delete inaccurate retained PII regarding the individuals, to discontinue the use of or erase the retained PII data that is used or was collected in violation of the APPI, or discontinue unlawful disclosure to third parties of retained PII data.

In addition to the obligations to respond to the individuals' requests (ie, obligations of disclosure, correction, etc, cessation of use, etc, and cessation of third-party disclosure), PII data owners are subject to an obligation to cease disclosure of PII data to third parties if the relevant individual 'opts out' of the third-party disclosure.

Compensation

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

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

Enforcement

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

Individuals' right to monetary compensation is enforced through the judicial system. With regard to violations by PII data owners of the obligations to respond to individuals' requests as separately mentioned in this chapter (ie, obligations of disclosure, correction, etc, cessation of use, etc, and cessation of third-party disclosure), individuals may exercise their rights to require PII data owners to respond to such requests through the judicial system, provided that they first request the relevant PII data users to comply with such obligations and two weeks have passed after such request was made. Separately, the Personal Information Protection Commission may recommend PII data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for the protection of individuals' rights.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

Not applicable.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Administrative law in Japan usually provides for an appeal of a governmental ministry's decision to a court with proper jurisdiction. Therefore, if the Personal Information Protection Commission or the relevant governmental ministry to which powers of the Commission are duly delegated by the Commission takes administrative actions against a personally identifiable information (PII) data user, the PII data user will generally be able to challenge the actions judicially.

SPECIFIC DATA PROCESSING

Internet use

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

There are no binding rules applicable to the use of 'cookies' or equivalent technology. Any data collected through the use of cookies is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and thereby can identify a specific individual, then the data will constitute personal data subject to the Act on the Protection of Personal Information of 2003, as amended.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Unsolicited marketing by email is regulated principally by the Act on Regulation of Transmission of Specified Electronic Mail. Pursuant to the Act, marketing emails can be sent only to a recipient who:

- has 'opted in' to receive them;
- has provided the sender with his or her email address in writing (for instance, by providing a business card);

NAGASHIMA OHNO & TSUNEMATSU

Akemi Suzuki

akemi_suzuki@noandt.com

Tomohiro Sekiguchi

tomohiro_sekiguchi@noandt.com

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan
Tel +81 3 6889 7000
www.noandt.com

- has a business relationship with the sender; or
- makes his or her email address available on the internet for business purposes.

In addition, the Act requires the senders to allow the recipients to 'opt out'. Marketing emails sent from overseas will be subject to this Act as long as they are received in Japan.

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

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

The Personal Information Protection Commission has published its stance that the use of cloud server services to store PII data does not constitute disclosure to outsourced processing service providers as long as it is ensured by contract or otherwise that the service providers are properly restricted from accessing PII data stored on their servers. If the use of a particular cloud computing service is considered to constitute disclosure to outsourced processing service providers, PII data users are required to engage in 'necessary and appropriate' supervision over the cloud service providers to safeguard the transferred PII data. Additionally, PII data users need to confirm that the service providers, if the servers are located outside of Japan, meet the equivalency test so as not to trigger the requirement to obtain prior consent from the individuals to the cross-border transfer of data.

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Diet has passed a bill to amend Act on the Protection of Personal Information of 2003 (the APPI) on 5 June 2020. The main topics of this amendment include the following.

- to strengthen the individuals' rights to require personally identifiable information (PII) data owners to discontinue the use of or to erase the retained PII data;
- to establish obligations of PII data users to notify the regulators or affected individuals in case of serious leakage of PII;
- to create a new concept of 'pseudonymised information' which is the intermediate concept between PII and anonymised information;
- to create a new concept of 'information related to an individual' and restricting a transfer of such information related to the individual in certain cases where a transferee can identify the relevant individual by linking such information related to an individual with the PII held by the transferee;
- to strengthen the current criminal penalties (eg, non-compliance with any order issued by Commission by a judicial entity will be subject to a criminal fine up to ¥100 million); and
- to strengthen the Commission's powers to supervise foreign PII data users, anonymised information users, and business operators handling 'databases, etc' of pseudonymised information or 'databases, etc' of information related to an individual to which the APPI is applicable.

The portion related to the criminal penalties will take effect within six months from its promulgation while the remainder, which would have a more impact on private businesses will come into effect within two years from its promulgation.

Other titles available in this series

Acquisition Finance	Distribution & Agency	Investment Treaty Arbitration	Public M&A
Advertising & Marketing	Domains & Domain Names	Islamic Finance & Markets	Public Procurement
Agribusiness	Dominance	Joint Ventures	Public-Private Partnerships
Air Transport	Drone Regulation	Labour & Employment	Rail Transport
Anti-Corruption Regulation	e-Commerce	Legal Privilege & Professional Secrecy	Real Estate
Anti-Money Laundering	Electricity Regulation	Licensing	Real Estate M&A
Appeals	Energy Disputes	Life Sciences	Renewable Energy
Arbitration	Enforcement of Foreign Judgments	Litigation Funding	Restructuring & Insolvency
Art Law	Environment & Climate Regulation	Loans & Secured Financing	Right of Publicity
Asset Recovery	Equity Derivatives	Luxury & Fashion	Risk & Compliance Management
Automotive	Executive Compensation & Employee Benefits	M&A Litigation	Securities Finance
Aviation Finance & Leasing	Financial Services Compliance	Mediation	Securities Litigation
Aviation Liability	Financial Services Litigation	Merger Control	Shareholder Activism & Engagement
Banking Regulation	Fintech	Mining	Ship Finance
Business & Human Rights	Foreign Investment Review	Oil Regulation	Shipbuilding
Cartel Regulation	Franchise	Partnerships	Shipping
Class Actions	Fund Management	Patents	Sovereign Immunity
Cloud Computing	Gaming	Pensions & Retirement Plans	Sports Law
Commercial Contracts	Gas Regulation	Pharma & Medical Device Regulation	State Aid
Competition Compliance	Government Investigations	Pharmaceutical Antitrust	Structured Finance & Securitisation
Complex Commercial Litigation	Government Relations	Ports & Terminals	Tax Controversy
Construction	Healthcare Enforcement & Litigation	Private Antitrust Litigation	Tax on Inbound Investment
Copyright	Healthcare M&A	Private Banking & Wealth Management	Technology M&A
Corporate Governance	High-Yield Debt	Private Client	Telecoms & Media
Corporate Immigration	Initial Public Offerings	Private Equity	Trade & Customs
Corporate Reorganisations	Insurance & Reinsurance	Private M&A	Trademarks
Cybersecurity	Insurance Litigation	Product Liability	Transfer Pricing
Data Protection & Privacy	Intellectual Property & Antitrust	Product Recall	Vertical Agreements
Debt Capital Markets		Project Finance	
Defence & Security			
Procurement			
Dispute Resolution			

Also available digitally

[lexology.com/gtdt](https://www.lexology.com/gtdt)