

# Data Protection & Privacy

*Contributing editor*  
**Wim Nauwelaerts**



**2017**

GETTING THE  
DEAL THROUGH

GETTING THE  
DEAL THROUGH 

# Data Protection & Privacy 2017

*Contributing editor*  
**Wim Nauwelaerts**  
**Hunton & Williams**

Publisher  
Gideon Robertson  
gideon.roberton@lbresearch.com

Subscriptions  
Sophie Pallier  
subscriptions@gettingthedealthrough.com

Senior business development managers  
Alan Lee  
alan.lee@gettingthedealthrough.com

Adam Sargent  
adam.sargent@gettingthedealthrough.com

Dan White  
dan.white@gettingthedealthrough.com



Published by  
Law Business Research Ltd  
87 Lancaster Road  
London, W11 1QQ, UK  
Tel: +44 20 3708 4199  
Fax: +44 20 7229 6910

© Law Business Research Ltd 2016  
No photocopying without a CLA licence.  
First published 2012  
Fifth edition  
ISSN 2051-1280

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 July and August 2016. Be advised that this is a developing area.

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



## CONTENTS

<b>Introduction</b>	<b>5</b>	<b>Malta</b>	<b>82</b>
Wim Nauwelaerts Hunton & Williams		Olga Finkel, Robert Zammit and Rachel Vella-Baldacchino WH Partners	
<b>EU overview</b>	<b>8</b>	<b>Mexico</b>	<b>88</b>
Wim Nauwelaerts and Anna Pateraki Hunton & Williams		Gustavo A Alcocer and Abraham Díaz Arceo Olivares	
<b>Safe Harbor and the Privacy Shield</b>	<b>10</b>	<b>Poland</b>	<b>94</b>
Aaron P Simpson Hunton & Williams		Arwid Mednis and Gerard Karp Wierzbowski Eversheds	
<b>Australia</b>	<b>12</b>	<b>Russia</b>	<b>101</b>
Alex Hutchens, Jeremy Perier and Eliza Humble McCullough Robertson		Ksenia Andreeva, Anastasia Dergacheva, Vasilisa Strizh and Brian Zimpler Morgan, Lewis & Bockius LLP	
<b>Austria</b>	<b>18</b>	<b>Serbia</b>	<b>108</b>
Rainer Knyrim Preslmayr Rechtsanwälte OG		Bogdan Ivanišević and Milica Basta BDK Advokati	
<b>Belgium</b>	<b>25</b>	<b>Singapore</b>	<b>113</b>
Wim Nauwelaerts and David Dumont Hunton & Williams		Lim Chong Kin and Charmian Aw Drew & Napier LLC	
<b>Brazil</b>	<b>33</b>	<b>Slovakia</b>	<b>126</b>
Ricardo Barretto Ferreira and Paulo Brancher Azevedo Sette Advogados		Radoslava Rybanová and Jana Bezeková Černežová & Hrbek, sro	
<b>Chile</b>	<b>38</b>	<b>South Africa</b>	<b>132</b>
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya García Magliona & Cía Abogados		Danie Strachan and André Visser Adams & Adams	
<b>Denmark</b>	<b>43</b>	<b>Sweden</b>	<b>141</b>
Michael Gorm Madsen Lundgrens Law Firm P/S		Henrik Nilsson Wesslau Söderqvist Advokatbyrå	
<b>Germany</b>	<b>49</b>	<b>Switzerland</b>	<b>148</b>
Peter Huppertz Hoffmann Liebs Fritsch & Partner		Lukas Morscher and Kaj Seidl-Nussbaumer Lenz & Staehelin	
<b>India</b>	<b>55</b>	<b>Taiwan</b>	<b>155</b>
Stephen Mathias and Naqeeb Ahmed Kazia Kochhar & Co		Ken-Ying Tseng and Rebecca Hsiao Lee and Li, Attorneys-at-Law	
<b>Ireland</b>	<b>61</b>	<b>Turkey</b>	<b>161</b>
Anne-Marie Bohan Matheson		Ozan Karaduman and Bentley James Yaffe Gün + Partners	
<b>Japan</b>	<b>70</b>	<b>United Kingdom</b>	<b>167</b>
Akemi Suzuki Nagashima Ohno & Tsunematsu		Bridget Treacy Hunton & Williams	
<b>Luxembourg</b>	<b>76</b>	<b>United States</b>	<b>173</b>
Marielle Stevenot, Rima Guillen and Charles-Henri Laevens MNKS		Lisa J Sotto and Aaron P Simpson Hunton & Williams	

# Japan

Akemi Suzuki

Nagashima Ohno & Tsunematsu

---

## Law and the regulatory authority

### 1 Legislative framework

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

The Act on the Protection of Personal Information of 2003 (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-ever 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.

A limited portion of the Amendment came into effect on 1 January 2016 while the remainder, which would have a major impact on private businesses, remains unenforced. The date of full enforcement has not been published, but it will be no later than 9 September 2017.

At the time of writing, the APPI is implemented by a number of industry- or sector-specific administrative guidelines compiled by governmental ministries. As of November 2015, as many as 38 administrative guidelines covering 27 sectors exist. Numerous self-regulatory organisations and industry associations have also adopted their own policies or guidelines for the protection of PII.

### 2 Data protection authority

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

The Personal Information Protection Committee (the Committee) was established on 1 January 2016 as a cross-sectoral, independent governmental body to oversee the APPI. Until the full implementation of the Amendment, different governmental ministries enforce the APPI in the respective sectors and industries that they supervise. Governmental ministries have the following powers under the APPI:

- to require reports from PII data users (as defined in question 9) for their businesses over which the respective ministries have jurisdiction;
- to give advice necessary for the handling of PII to PII data users;
- upon violation of certain obligations of any PII data 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 governmental ministry deems imminent danger to the affected individual's material rights, to 'order' such measures.

Following the full introduction of the Amendment, the Committee will generally take over the foregoing powers and additionally will be given the power to conduct an on-site inspection of the offices or other premises of PII data users.

### 3 Breaches of data protection

**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 person:

- fails to comply with any order issued by the competent governmental ministry, or the Committee following the full implementation of the Amendment (subject to penal servitude of six months or less or criminal fine of ¥300,000 or less); or
- fails to submit reports, or submits untrue reports, as required by the competent governmental ministry, or the Committee following the full implementation of the Amendment (subject to criminal fine of ¥300,000 or less).

The Amendment will also introduce additional criminal penalties under the following circumstances:

- a person refuses or interrupts an on-site inspection of the offices or other premises by the Committee (subject to a criminal fine of ¥300,000 or less); 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 one year or less or a criminal fine of ¥500,000 or less).

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

---

## Scope

### 4 Exempt sectors and institutions

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

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.
- Private businesses that have owned PII of less than 5,000 individuals in their electronic or manual database at any time in the past six

months are also exempt (small business exception). This exception, however, will be abolished under the Amendment.

- Use of PII for personal purposes is outside the scope of the APPI. Use of PII by not-for-profit organisations or sole proprietorships is within the scope of the APPI.

## 5 Communications, marketing and surveillance laws

**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.

## 6 Other laws

**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.

## 7 PII formats

**What forms of PII are covered by the law?**

In terms of forms of PII, the use of 'database, etc' of PII (PII database) is covered by the APPI. PII database includes not only electronic databases but also 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 comprising a PII database is called PII data.

The Amendment will broaden the definition of PII by expressly including 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.

In addition, the Amendment will introduce 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 will not be considered PII.

## 8 Extraterritoriality

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

Currently, it is widely considered that the APPI does not have extraterritorial application. 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.

However, following the full implementation of the Amendment, the APPI will apply when PII owners use or process, outside of Japan, such PII of individuals residing in Japan as was obtained in connection with the provision of goods or services by the PII owners.

## 9 Covered uses of PII

**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?**

The APPI distinguishes between: (i) obligations imposed on all private business operators using PII database (for the purposes of this chapter, called PII data users); and (ii) obligations imposed only on those PII data users who control the relevant PII data (for the purposes of this chapter, called 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 (i) include:

- to specify the purposes for which the PII is used and to process the PII only to the extent necessary for achieving such specified purposes (see question 10);
- to notify the relevant individual of, or publicise, the purposes of use prior to or at the time of collecting PII (see question 12);
- to not use deceptive or wrongful means in collecting PII (see question 10);
- to endeavour to keep its PII data accurate and up to date to the extent necessary for the purposes of use (see question 15);
- to undertake necessary and appropriate measures to safeguard the PII data it holds (see question 19);
- to conduct necessary and appropriate supervision over its employees and its service providers who process its PII data (see question 19); and
- not disclosing the PII data to any third party without the consent of the individual (subject to certain exemptions) (see question 29).

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

- to make accessible to the relevant individual certain information regarding the retained PII data (see question 12);
- to provide, without delay, a copy of retained PII data to the relevant individual upon his or her request (see question 34);
- 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 (see question 14);
- 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 (see question 14); 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 (see question 14).

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

### 10 Legitimate processing – grounds

**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 APPI does not contain specific criteria for legitimate data collection or processing. The APPI does, however, prohibit the collection of 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.

**11 Legitimate processing – types of PII****Does the law impose more stringent rules for specific types of PII?**

Presently, the APPI does not have special rules for specific types of personal data. Some of the administrative guidelines for the APPI adopted by governmental ministries, however, impose stringent restrictions on the collection, use and disclosure to third parties of certain sensitive data.

The Amendment will introduce the concept of ‘sensitive personal information,’ which includes race, beliefs, social status, health and criminal records. Collection or disclosure under the ‘opt-out’ mechanism of sensitive personal information without the consent of the relevant individual will be generally prohibited.

**Data handling responsibilities of owners of PII****12 Notification****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 APPI.

First, the APPI requires all PII data users to notify individuals of, or make available to individuals, the purpose for which their PII data is used, promptly after the collection of the PII, unless such 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 (see question 30). Such information includes types of information being disclosed and manner of disclosure.

Third, the APPI requires each PII data owner to keep certain information accessible to those individuals whose retained PII data is held. Such information includes: name of the PII data owner; all purposes for which retained PII data held by the PII data owner is used generally; 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.

**13 Exemption from notification****When is notice not required?**

There is an exception to the first notice requirement mentioned in question 12 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 acquisition of the relevant PII data.

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

Upon request from an individual, a PII data owner must:

- disclose, without delay, retained PII data in written form to the relevant individual upon his or her request (see question 34);
- correct, add or delete the retained PII data to the extent necessary for achieving the purposes of use upon request from the relevant individual;
- 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
- 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.

An exemption from the third and fourth obligations mentioned above 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.

**15 Data accuracy****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. In addition, the Amendment requires that all PII data users endeavour to erase, without delay, such PII data that is no longer needed to be used.

**16 Amount and duration of data holding****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 Amendment, PII data users must endeavour to erase, without delay, such PII data that is no longer needed to be used.

**17 Finality principle****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 in a manner mentioned in question 12. 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 an individual and it is difficult to obtain consent of the affected individual.

**18 Use for new purposes****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?**

Purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be reasonably related to the previous purposes. PII may be used for such amended purposes, provided that the amended purposes are notified or made available to the affected individuals.

Under the Amendment, purpose for use may be amended to the extent reasonably deemed to be related (as opposed to ‘reasonably’ related) to the previous purposes. The implications of this change are unclear at this point.

**Security****19 Security obligations****What security obligations are imposed on PII owners and service providers that process PII on their behalf?**

The APPI provides that all 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 in many of the administrative guidelines for the APPI. For instance, the administrative guidelines prepared by the Ministry of Economy, Trade and Industry (METI Guidelines) set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical measures.

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

The APPI, either before or after the Amendment, 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 regulator or an accredited personal information protection organisation, if applicable, is generally required or recommended under most administrative guidelines for the APPI. In addition, such guidelines generally recommend or require notification to the affected individuals or public announcement in case of serious security breach incidents.

Thresholds for or exceptions to such requirement or recommendation vary depending on individual guidelines – the METI Guidelines, for instance, recommend reporting to the METI, as opposed to an accredited personal information protection organisation, if sensitive information or credit card information was possibly compromised. On the other hand, under the METI Guidelines, neither notification to the affected individuals nor public announcement is necessary if the lost or disclosed data was protected by advanced encryption or other security enhancing measures and the risk of violation of privacy or other rights of the relevant individuals are nil or very low.

---

## Internal controls

### 21 Data protection officer

**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 METI Guidelines and a number of other administrative guidelines on the APPI. The METI Guidelines do not provide for qualifications, roles or responsibilities of a chief privacy officer.

### 22 Record keeping

**Are owners of PII required to maintain any internal records or establish internal processes or documentation?**

PII data users are generally required under applicable administrative guidelines on the APPI to establish internal processes to safeguard the PII data.

Under the Amendment, 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 verify how the PII data was acquired by such third parties and keep records of such verification.

---

## Registration and notification

### 23 Registration

**Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?**

Currently, there is no such registration requirement in Japan. Under the Amendment, PII data users who disclose PII data (other than sensitive personal information) under the 'opt-out' mechanism are required to submit a notification of such disclosure to the Committee.

### 24 Formalities

**What are the formalities for registration?**

Formalities for registration are not applicable. Formalities for a notification of disclosure under the 'opt-out' mechanism mentioned in question 23 are yet to be published by the government. Upon the receipt of such notification, the Committee will publicise certain information included in the notification.

### 25 Penalties

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

Not applicable.

### 26 Refusal of registration

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

Not applicable.

---

### 27 Public access

**Is the register publicly available? How can it be accessed?**

Not applicable.

### 28 Effect of registration

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

Not applicable.

---

## Transfer and disclosure of PII

### 29 Transfer of PII

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

The APPI generally prohibits disclosure of 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.

### 30 Restrictions on disclosure

**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:

- 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; and certain information regarding such disclosure is notified, or made easily accessible, to the individual prior to such disclosure;
- transfer in M&A 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; and
- 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 in order 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.

With respect to disclosure under the opt-out mechanism mentioned above, the Amendment requires that it must also be notified in advance to the Committee.

---

### 31 Cross-border transfer

**Is the transfer of PII outside the jurisdiction restricted?**

At present, there are no general restrictions on the ability of a data owner to transfer PII outside Japan. Under the Amendment, however, transfer of PII data to a third party located outside of Japan will be subject to prior consent of the relevant individual except to the extent that the third party is located in foreign countries that the Committee determines warrant the equivalent level of protection of PII as Japan, or that the relevant third party has established on a continuous basis the equivalent level of protective measures as PII data users are required to establish under the amended APPI. At the time of writing, the Committee has not published its decision on the countries or businesses that meet the respective equivalency test. It is generally anticipated that transfer of PII data to foreign businesses certified under the APEC Cross-Border Privacy Rules will not be subject to the requirement to obtain prior consent of the individuals.

**32 Notification of cross-border transfer**

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

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

**33 Further transfer**

**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 mentioned in question 31 under the Amendment will be applicable to transfers to service providers. They may also be applicable to onward transfers as long as the transferors of such onward transfers are subject to the APPI as amended.

**Rights of individuals****34 Access**

**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.**

Currently, the APPI imposes on 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. 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.

**35 Other rights**

**Do individuals have other substantive rights?**

In addition to the obligations set forth in question 14, 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.

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 erasure of 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.

**36 Compensation**

**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.

**37 Enforcement**

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

Individuals' right to monetary compensation (mentioned in question 36) is enforced through the judicial system. With regard to violations by PII data owners of the obligations described in questions 34 and 35, currently, individuals do not have any statutory right to demand enforcement by the competent governmental ministry. The ministry may, however, recommend PII data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for protection of individuals' rights.

Under the Amendment, individuals may exercise their rights described in questions 34 and 35 through the judicial system, provided that they first request the relevant PII data owners to perform such obligations and two weeks have passed after such request was made.

**Exemptions, derogations and restrictions****38 Further exemptions and restrictions**

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

Not applicable.

**Supervision****39 Judicial review**

**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 relevant supervising ministry or the Commission takes administrative actions against a PII data user, the PII data user will generally be able to challenge the actions judicially.

# NAGASHIMA OHNO & TSUNEMATSU

**Akemi Suzuki**

**akemi\_suzuki@noandt.com**

JP Tower  
2-7-2 Marunouchi, Chiyoda-ku  
Tokyo 100-7036  
Japan

Tel: +81 3 6889 7000  
Fax: +81 3 6889 8000  
www.noandt.com



---

**Specific data processing**

---

**40 Internet use**

**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 APPI.

**41 Electronic communications marketing**

**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; who has provided the sender with his or her email address in writing (for instance, by providing a business card); who has a business relationship with the sender; or who 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.

---

**42 Cloud services**

---

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

The precursor of the Committee published regulatory guidance with respect to the use of cloud server services to store personal information obtained through the use of stored individual social security and tax numbers (specified personal information). Based on the guidance, the use of cloud server services to store specified personal information constitutes disclosure to outsourced processing service providers unless it is ensured by contract or otherwise that the service providers are properly restricted from accessing specified personal information stored on their servers. If the Committee is to take the same stance with respect to the storage of PII on third-party cloud servers, PII data users are required to engage in 'necessary and appropriate' supervision over the cloud service providers in order to safeguard the transferred PII data (see question 29). Additionally, under the Amendment PII data users would need to confirm that the service providers offer functions of record-keeping (see question 22) and also 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 (see question 31).

## Getting the Deal Through

Acquisition Finance  
Advertising & Marketing  
Air Transport  
Anti-Corruption Regulation  
Anti-Money Laundering  
Arbitration  
Asset Recovery  
Aviation Finance & Leasing  
Banking Regulation  
Cartel Regulation  
Class Actions  
Construction  
Copyright  
Corporate Governance  
Corporate Immigration  
Cybersecurity  
Data Protection & Privacy  
Debt Capital Markets  
Dispute Resolution  
Distribution & Agency  
Domains & Domain Names  
Dominance  
e-Commerce  
Electricity Regulation  
Energy Disputes  
Enforcement of Foreign Judgments  
Environment & Climate Regulation  
Equity Derivatives  
Executive Compensation & Employee Benefits  
Foreign Investment Review  
Franchise  
Fund Management  
Gas Regulation  
Government Investigations  
Healthcare Enforcement & Litigation  
Initial Public Offerings  
Insurance & Reinsurance  
Insurance Litigation  
Intellectual Property & Antitrust  
Investment Treaty Arbitration  
Islamic Finance & Markets  
Labour & Employment  
Legal Privilege & Professional Secrecy  
Licensing  
Life Sciences  
Loans & Secured Financing  
Mediation  
Merger Control  
Mergers & Acquisitions  
Mining  
Oil Regulation  
Outsourcing  
Patents  
Pensions & Retirement Plans  
Pharmaceutical Antitrust  
Ports & Terminals  
Private Antitrust Litigation  
Private Client  
Private Equity  
Product Liability  
Product Recall  
Project Finance  
Public-Private Partnerships  
Public Procurement  
Real Estate  
Restructuring & Insolvency  
Right of Publicity  
Securities Finance  
Securities Litigation  
Shareholder Activism & Engagement  
Ship Finance  
Shipbuilding  
Shipping  
State Aid  
Structured Finance & Securitisation  
Tax Controversy  
Tax on Inbound Investment  
Telecoms & Media  
Trade & Customs  
Trademarks  
Transfer Pricing  
Vertical Agreements

Also available digitally



# Online

[www.gettingthedealthrough.com](http://www.gettingthedealthrough.com)



Data Protection & Privacy  
ISSN 2051-1280



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
2012



Official Partner of the Latin American  
Corporate Counsel Association



Strategic Research Sponsor of the  
ABA Section of International Law