Lex Mundi
World Ready

Lex Mundi Data Privacy Guide: Focus on the Asia/Pacific Region

Prepared by Lex Mundi member firms
in the Asia/Pacific Region

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series at: www.lexmundi.com/GlobalPracticeGuides.

Lex Mundi is the world's leading network of independent law firms with in-depth experience in 100+ countries. Through close collaboration, our member firms are able to offer their clients preferred access to more than 21,000 lawyers worldwide – a global resource of unmatched breadth and depth.

Lex Mundi – the law firms that know your markets.

About this Guide

The Lex Mundi Data Privacy Guide draws on the expertise of our member firms and is a simple but concise tool for our clients doing business across the Asia/Pacific region. This guide focuses on key data protection concepts and issues across various jurisdictions in the Asia/Pacific region. Each jurisdiction includes a key legislation overview, along with key data protection provisions.

Table of Contents

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Australia

Prepared by Clayton Utz, Lex Mundi member firm for Australia

Key Legislation Overview

What is the Key Legislation?	**The Privacy Act 1988 (Cth) regulates the handling of personal information.** The *Privacy Act 1988* (Cth) (**Privacy Act**) regulates the handling of personal information, largely through the thirteen Australian Privacy Principles (**APPs**). The APPs regulate the handling of personal information, including the collection, use, storage, disclosure and destruction of personal information, as well as rights to access or seek correction of personal information. The Commissioner, as defined under the *Australian Information Commissioner Act 2010* (Cth) has the authority under the Privacy Act to develop or request the development of an APP code, which is a written code of practice about information privacy and when registered is a legislative instrument. The current APP codes in force in Australia are: • *Privacy (Market and Social Research) Code 2014; and* • *Privacy (Credit Reporting) Code 2014.* This Privacy Act does not affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction or disclosure of personal information (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with the Privacy Act.

Key Data Protection Provisions	
What data is protected?	**The Privacy Act protects 'personal information', which is information or an opinion about an identified individual, or an individual who is reasonably identifiable.** The Privacy Act protects 'personal information' which is 'information or an opinion about an identified individual, or an individual who is reasonable identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not.' Examples of personal information includes an individual's name, signature, address, date of birth, medical records and employment details. 'Sensitive information' is defined under the Privacy Act to include information or an opinion about an individual's racial or ethnic origin, political opinions, sexual orientation or criminal record.
Who is subject to privacy obligations?	**The Privacy Act applies to organisations and agencies including both Commonwealth and private sector entities** Under the Privacy Act, an 'APP entity' must not do an act, or engage in a practice that breaches an APP, where an 'APP entity' is defined as an agency or organisation. For the purpose of the Privacy Act an organisation includes an individual, body corporate, partnership, trust or other unincorporated association that is not a small business operator, registered political party, agency or State or Territory authority. An agency includes various government entities, for example, a Minister, Department or body established by a Commonwealth enactment. The key exemptions from the operation of the Privacy Act to the private sector are, first, small businesses (defined in general terms as a business with an annual turnover that is less than $3 million AU), although this exemption does not apply to for profit information businesses or health service

	businesses. The second key exemption is that employee records are not covered by the Privacy Act. Subject to limited exceptions, the Privacy Act does not apply to state or territory government agencies, including state and territory public hospitals and health care facilities which are covered under state and territory legislation.
How is the collection of personal data regulated?	**Subject to a number of exceptions, personal information must not be solicited by an APP entity unless the information is reasonably necessary for the entity's functions or activities. Unsolicited personal information received by an APP entity must be retained in accordance with the regulations or destroyed. APP entities must generally give a collection statement to the data subject at the time of, or as soon as practicable after, collection of personal information.** An APP entity must not collect solicited personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities. Where an APP entity is an agency, it is also sufficient that the information be 'directly related to' those functions or activities. An APP entity must not collect sensitive information unless they have the consent of the individual and the information is reasonably necessary for one or more of the entity's functions or activities. Where an APP entity is an agency, it is sufficient that they have the consent of the individual and the information is 'directly related to' the agencies functions or activities. An entity may collect sensitive information where: • the collection is required/authorised under Australian law; • a permitted general situation exists under the legislation;

	• the entity is an organisation and a permitted health situation exists (for example, the information is necessary for the provision of health services); • the entity is the Immigration Department and reasonably believes the information is reasonably necessary enforcement related activities; • the entity is an enforcement body and reasonably believes the information is reasonably necessary for one or more of the its functions or activities; • the entity is a non-profit and the information relates to the activities of the organisation and solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities. An APP entity must only collect personal information by lawful and fair means. They must only collect that information from the individual unless: • The information is being collected by an agency and the individual consents; • The information is being collected by an agency who is required/authorised to do so under Australian law; or • it is reasonable impracticable to do so. When an APP entity receives personal information that they have not solicited, it must determine within a reasonable period of time whether they could have collected the information if it had been solicited in line with the rules above. If the entity determines they could not have and the information is not contained in a Commonwealth record, the information must be destroyed. When an APP entity has collected personal information, they must take reasonable steps at or before collection or, if that is not practicable, as soon as practicable after collection, to ensure that the individual is notified of such of the following matters as are reasonable in the circumstances:

	• the identity and contact details of the APP entity; • where it is not clear to the individual, the fact that the entity has collected information and the circumstances in which it was collected; • where the collection was required under Australian Law, the details of this requirement; • the purpose for collection; • consequences for the individual; • any other bodies, persons or entities to which the APP entity is likely to disclose the information; • the entity's APP privacy policy containing how the individual may access or correct the personal information; • the entity's APP privacy policy containing how the individual may complain about a breach of the APPs and how that breach will be dealt with; and • if the APP entity is likely to disclose the personal information to overseas recipients, the countries in which they are likely to be located.
How are the use and disclosure of personal data regulated?	**Subject to a number of exceptions, an APP entity must only use or disclose personal information for the primary purpose for which it was collected.** An APP entity must not use or disclose personal information held for a primary purpose for any other secondary purpose, unless: • the individual has consented to the use or disclosure; • the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose which is: o for sensitive information—directly related to the primary purpose; or o for all other personal information —related to the primary purpose;

	• the use or disclosure is required/authorised by Australian law; • a permitted general situation exists; • the APP entity is an organisation and a permitted health situation exists; • the APP entity reasonably believes that the use or disclosure is reasonably necessary for enforcement related activities; or • the information is relevant to public health or public safety and the entity has taken reasonable steps to ensure the information has been de-identified before its use or disclosure. For the purposes of direct marketing, an organisation must not use or disclose personal information (other than sensitive information) unless: • information is collected from an individual; • the individual reasonably expects it would be used for that purpose; • the organisation has provided an easily available means of the individual requesting not to receive the marketing; and • the individual has not made such a request. Personal information may also be used for direct marketing where information was obtained from the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose but the individual has either given their consent, or obtaining consent was impracticable. This is permitted under the APPs so long as the organisation provides a simple means by which the individual may easily request not to receive the direct marketing and in each communication to the individual the organisation makes clear how such a request can be made. A request by the individual to stop direct marketing must be given effect to within a reasonable period of time.

	Sensitive information may be disclosed and used for the purposes of direct marketing only with the consent of the individual. Where the organisation is a contract service provider, they may disclose personal information for the purpose of direct marketing if they are required to do so to meet their obligations under the contract.
How are storage, security and retention of personal data regulated?	**Where an APP entity holds personal information, they must take reasonable steps to ensure it is protected. Where it is no longer required, it must be destroyed.** Where an APP entity holds personal information, it must take reasonable steps to ensure it is protected. This includes protection from misuse, interference, loss, unauthorised access or disclosure. If the information is no longer required by the entity and is not contained in a Commonwealth record and the entity is not required to retain it under Australian law, the entity must take reasonable steps to destroy the information or to make sure it is de-identified
Are there rights of access to and correction of personal data?	**Subject to a number of exceptions, an APP entity must give an individual access to their personal information held by the APP entity, if they request it. They must also allow an individual to correct incorrect personal information.** **Rights of access** Where an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. There are a number of exceptions to this rule.

	The rule will not apply to an agency where that agency is able to refuse such a request or limit the information given following a request under the *Freedom of Information Act 1982* (Cth) or another Australian Law. An organisation may also refuse a request to the extent that giving access would: • pose a serious threat to the life, health or safety of any individual or the public; • have an unreasonable impact on the privacy of other individuals; • reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; • be unlawful; • be likely to prejudice enforcement related activities; or • reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process. Access may also be refused to the extent that: • the request is frivolous or vexatious; • the information relates to existing or anticipated legal proceedings and would not be accessible by the process of discovery in those proceedings; • denying access is required/authorised under Australian law; or • there is a reasonable suspicion of unlawful activities or misconduct relating to the entity's functions or activities and access would likely prejudice the taking of appropriate action in relation to the matter. When dealing with requests for access, an APP entity must respond within a reasonable period of time and give access where it is reasonable and practicable to do so. Charges may apply where the APP entity is an organisation, but they must not be excessive and must not apply to the making of the request.

	Where access has been refused based on one of the exceptions, or the APP entity has refused to give information in the manner requested, the entity must give the individual notice setting out the reasons for the refusal and avenues of complaint. **Rights of correction** An APP entity must take reasonable steps to correct information where it is satisfied that it is incorrect, inadequate, out-of-date, irrelevant or misleading or an individual requests the correction of their information. Where a correction is made to information previously disclosed to another APP entity and the individual requests that the other APP entity be notified of the correction, steps must be taken to make the notification. Where an individual requests a correction be made, the APP entity must respond within 30 days if it is an agency, or within a reasonable period of time if it is an organisation and the entity must not charge for these acts. Refusal to meet a request for the correction of information requires written notice to be provided to the individual, stating the reasons for the refusal and avenues for complaint.
Are there restrictions on cross border data transfers?	**Subject to a number of exceptions, an APP entity must not disclose personal information about an individual to an overseas recipient unless they have taken reasonable steps to ensure that the overseas recipient will not breach the APPs.** Prior to disclosing personal information about an individual to an overseas recipient, an APP entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This rule does not apply:

	• If the APP entity reasonably believes that the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a similar way to the APPs and there are ways an individual can enforce that protection; • If the individual consents after having been expressly informed by the APP entity that by so consenting, they will lose the relevant protections under the Privacy Act; • if the disclosure is required by Australian law; • if there is a permitted general situation; • if the disclosure is required under an international agreement which Australia has signed; • if the entity is an agency and they reasonably believe that the disclosure is necessary for enforcement related activities and the overseas recipient is an enforcement body.
Are there any notification requirements for data breaches?	**There are no current provisions relating to notification requirements for data breaches. However, the OAIC has issued a voluntary data breach reporting guide and mandatory data breach legislation is expected to be passed shortly.** The Privacy Act does not contain any notification requirements for data breaches. However, the Office of the Australian Information Commissioner released the *Data breach notification guide: a guide to handling personal information security breaches* (August 2014). The guide is not legally enforceable and offers recommendations in relation to the notification of individuals affected by a data breach. The guide suggests there are four key steps an organisation should undertake when responding to a breach or suspected breach, one of which (Step 3) is to notify the affected individuals of the breach. The steps are: • Step 1: contain the breach and do a preliminary assessment;

	• Step 2: evaluate the risk associated with the breach; • Step 3: notification; and • Step 4: prevent further breaches In December 2015, the Commonwealth Government released an exposure draft to the mandatory data breach notification bill, *Privacy Amendment (Notification of Serious Data Breaches)* Bill 2015 and undertook consultation regarding the proposed changes to the legislation. The bill is still in draft form with submissions having closed on 4 March 2016. It is anticipated that this legislation will be passed in the near future.
Who is the privacy regulator?	**The Commissioner, as defined under the *Australian Information Commissioner Act 2010* (Cth) has the authority to act in relation to the privacy functions as set out in the Privacy Act.** The Commissioner has a number of functions under the Privacy Act. Under Part IV of the Privacy Act, the Commissioner has the power to do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions. These include guidance, monitoring and advice related functions. The Commissioner may conduct an assessment in relation to the personal information held by an APP entity, in order to determine if that information is being maintained and handled in accordance with the regulations. The Commissioner may also investigate complaints made about practices that may be interfering with the privacy of an individual. The Commissioner has the power to make guidelines and legislative instruments under the Privacy Act under certain conditions, for example in relation to an APP entity's acts and practices. They also have various other powers related for

	privacy under separate acts, for example, the Telecommunications Act.
What are the consequences of a privacy breach?	**The maximum pecuniary penalty for a serious interference with privacy is AUD 1.8 million. There is also a very wide power for the Commissioner and "any person" to seek an injunction to restrain conduct that would constitute a breach of the Act. The Commissioner also has powers to investigate complaints, require rectification and order compensation to be paid to complainants.** A breach of an APP will occur when an act or practice is contrary to or inconsistent with that principle. Where a breach of an APP or an APP code occurs, it is considered 'interference with the privacy of an individual' and the Commissioner has power to act on the breach. Following the investigation of a complaint, the Commissioner has a range of actions available to them. The Commissioner may make: • a determination dismissing the complaint; • a declaration that the respondent in the complaint has engaged in conduct constituting interference with the privacy of an individual which must not be repeated or continued; • a declaration that the respondent must take specified steps within a specified period of time to ensure the conduct is not repeated or continued; • a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant; • a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or

- a declaration that it would be inappropriate for any further action to be taken in the matter.

The Commissioner may also take these actions following an investigation in to the practice of an entity where a complaint has not occurred.

Where required, the Commissioner or a complainant may commence proceedings in the Federal Court or the Federal Circuit Court in order to enforce a determination made by the Commissioner. If satisfied that the entity was responsible for the interference with the privacy of an individual, the Court may make orders as it sees fit in relation to the declaration.

Where a determination is made that applies to an agency, there are additional requirements for the principal executive of the agency to ensure that all members, officers and employees of the agency are aware of the determination. In this situation, a complainant will also be entitled to compensation. Where an agency fails to comply, proceedings may be brought in the Federal Court or the Federal Circuit Court by the Complainant or the Commissioner.

Where an entity contravenes a civil penalty provision under the Privacy Act, the Commissioner may apply for a court order that pecuniary penalties be payable by the entity to the Commonwealth. If an entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual or repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals, it may be liable for a penalty of up to A$1.8 million.

There is also a very wide power for the Commissioner and "any person" to seek an injunction to restrain conduct that would constitute a breach of the Act.

How is electronic marketing regulated?	***The Spam Act 2003* (Cth) prohibits the sending of unsolicited commercial electronic messages which have an Australian link.** The *Spam Act 2003* (Cth) (**Spam Act**) prohibits the sending of unsolicited commercial electronic messages (**CEM**) that have an Australian link. A CEM is defined as an electronic message that is sent for the purpose of offering, or advertising goods, services, land, business opportunities or investment opportunities. An electronic message will also be a CEM if its purpose is to assist or enable a person to dishonestly obtain a financial advantage, property or gain from another person by deception. An unsolicited CEM is a CEM which the recipient has not consented to receiving. Consent under the Spam Act can be either express or reasonably inferred from the conduct of the individual concerned. A CEM will have an Australian link if: • the message originated in Australia; • the individual or organisation who sent or authorized the message was: o physically present in Australia when the message is sent; or o an organisation whose central management and control is in Australia when the message is sent; • the computer, server or device that is used to access the message is located in Australia; • the relevant electronic account holder is: o an individual who is physically present in Australia when the message is accessed; or

	○ an organisation that carries on business or activities in Australia when the message is accessed; or • if the message cannot be delivered because the relevant electronic address does not exist—assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server or device located in Australia.
Are there any recent developments or expected reforms?	**The Government has invited public comment on a serious data breach notification bill before legislation prior to the legislation being introduced in Parliament in 2016.** The *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* came out of the Australian Law Reform Commission (ALRC) Report in 2008 titled *For Your Information: Australian Privacy Law and Practice.* The Bill is still in draft form with consultation having closed on 4 March 2016. The Bill proposes to amend the Privacy Act and to define when a 'serious data breach' would occur and set out requirements for dealing with such a breach. notifications that would be required where a serious breach had occurred.

Contact Information

Steven Klimt sklimt@claytonutz.com	**Clayton Utz** Level 15,Sydney New South Wales Australia 2000 Tel 61.2.9353.4000

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

China

Prepared by JunHe LLP, Lex Mundi member firm for China

Key Legislation Overview	
What is the Key Legislation?	**China has not enacted a single piece of comprehensive personal data law or regulation. Provisions relating to the protection of personal information and privacy are scattered in major civil and criminal laws and administrative regulations.** The Decision on Strengthening the Network Information Protection ("**NPC Decision**") issued by the Standing Committee of the National People's Congress in December 2012, addressing to the protection of personal electronic information. The Regulation on the Protection of Personal Information of Telecommunication and Internet Users ("**MIIT Regulation**"), issued by the Ministry of Industry and Information Technology ("**MIIT**") in June 2013, addressing to the collection and use of users' personal information in the course of telecom and Internet information services. The Tort Law (2009) protects the right to privacy. The Consumer Rights and Interests Protection Law (2013 Revision) ("**CPL**") includes provisions on the protection of consumers' personal information. The Criminal Law (1997) criminalizes illegal sale and provision of personal information and illegal acquisition of personal information. In addition, there are several laws and regulations addressing to protection of personal information in certain industries or sectors (e.g. telecom and financial banking), or personal

	information of a specific nature (e.g. personal credit information).
Key Data Protection Provisions	
What data is protected?	**In general, these laws and regulations protects personal information, which refers to information that can be used to identify an individual, either independently or in combination with other information.** As stated above, China has not enacted an omnibus personal information protection law. As a result, the personal information falls into the scope of these sectoral laws and regulations are explicitly protected. For example, electronic personal information is protected by the NPC Decision, and consumer personal information is protected by the CPL. For other personal information in arenas other than those covered by sectoral laws and regulations, e.g. employee personal information, it may be protected by the Tort Law as privacy. However, since the law does not clearly define the scope of privacy, the protection to such information is less certain under current legal regime.
Who is subject to privacy obligations?	**In general, such entity and individual that collects and uses personal information is subject to obligation of personal information protection.** The NPC Decision applies to network service providers and other enterprises and entities. The MIIT Regulation applies to telecom and Internet service providers. The CPL applies to business operators. Certain institutions, such as banking financial institutions, medical institutions, credit report agencies undertake personal information protection obligation under the relevant sectoral regulations.

How is the collection of personal data regulated?	**According to the aforesaid laws and regulations, telecom and Internet service providers and other business operators shall collect and use personal information in accordance with the principle of lawfulness, appropriateness and necessity, inform the concerned individuals the purpose, method and scope of collection and use of personal information, and obtain their consent.** According to the NPC Decision, MIIT Regulation and CPL, telecom and Internet service providers and other business operators shall collect and use personal information in accordance with the principle of lawfulness, appropriateness and necessity, inform the concerned individuals the purpose, method and scope of collection and use of personal information, and obtain their consent. Unlike the personal information protection law in some other jurisdictions, existing PRC laws and regulations do not explicitly provide any exception to the “inform and consent” requirement, such as performance of contract or public interest.
How are the use and disclosure of personal data regulated?	**According to the aforesaid laws and regulations, telecom and Internet service providers and other business operators shall collect and use personal information in accordance with the principle of lawfulness, appropriateness and necessity, inform the concerned individuals the purpose, method and scope of collection and use of personal information, and obtain their consent.** **Disclosure and transfer of personal data is deemed as a form of use of personal data under existing PRC laws.** According to the NPC Decision, MIIT Regulation and CPL, telecom and Internet service providers and other business operators shall collect and use personal information in

	accordance with the principle of lawfulness, appropriateness and necessity, inform the concerned individuals the purpose, method and scope of collection and use of personal information, and obtain their consent. Telecom and Internet service providers and other business operators shall not use the personal information for purpose other than the one agreed by the relevant individual.
How are storage, security and retention of personal data regulated?	**The NPC Decision, MIIT regulation and CPL all provide that business operator shall take technical measures and other necessary measures to ensure information security and prevent electronic personal information of citizens gathered in their business activities from being divulged, damaged or lost.** **There is no clear data retention requirement under existing PRC laws except for certain special types of data.** To be more specific, the MIIT Regulation requires telecom and Internet service provider to take the following measures to prevent the divulgence, destruction, alteration or loss of users' personal information: (1) Determining the security management responsibilities among various departments, posts and branches for users' personal information; (B) Establishing the workflows and security management systems for collection and use of users' personal information and other relevant activities; (3) Administering the authorities of staff members and agents, examining the channelling, reproduction and destruction of information, and taking anti-phishing measures; (4) Properly keeping the paper, optic, electromagnetic and other media that record users' personal information, and taking corresponding security storage measures; (5) Reviewing the access to the information systems which store users' personal information, and taking anti-invasion, anti-virus and other measures; (6) Recording the personnel operating users' personal information, and the time, places, matters and other information thereof;

	(7) Conducting the communication network security protection work in accordance with the provisions of telecommunications administrative organs; and (8) Other necessary measures as specified by telecommunications administrative organs.
Are there rights of access to and correction of personal data?	**To certain extent.** Right to access and correction of personal data is not included in PRC law as a specific type of right for data subject, but some regulations, for example, the MIIT Regulation, requires that telecom and Internet service providers shall provide users with the channels for inquiry and correction of information.
Are there restrictions on cross border data transfers?	**Yes, there are restrictions for certain types of data or in certain industries.** At present, certain types of personal information, such as personal credit information, personal financial information and population health information, and information that falls into the scope of state secret, are restricted to be transferred abroad.
Are there any notification requirements for data breaches?	**Yes, there are some notification requirements under the current law.** According to the MIIT Regulation, in case users' personal information under the custody of telecom and Internet service providers is or may be divulged, destructed or lost, remedial measures shall be taken immediately. Where serious consequences are or may be caused, they shall immediately report to the telecommunications administrative organs which issued their licensing or approved their registration, and cooperate with the relevant departments in investigation and handling.

Who is the privacy regulator?	**There is no single privacy regulator. Some industrial regulators are responsible for the protection of personal information in the correspondent industrial sectors.** Examples are: the collection and use of personal information by telecom and Internet service providers is regulated by MIIT. The collection and use of consumers' personal information is generally regulated by State Administration for Industry and Commerce. There are also other regulators in charge of specific types of personal information.
What are the consequences of a privacy breach?	**The breaching party may be subject to administrative punishment or face tort infringement lawsuit, or criminal liability.** According to the MIIT Regulation, telecom and Internet service provider violating the regulation may be ordered to make rectification and imposed administrative fine for up to RMB 30,000. According to the CPL, business operators infringing the consumer's right to personal information shall be ordered by SAIC and its local counterparts to make correction. Their illegal income may be confiscated and they may be imposed a fine of not less than the illegal income but not more than ten times the illegal income or, if there is no illegal income, a fine of not more than RMB 500,000; and if the circumstances are serious, they may be ordered to suspend business operation and their business license may be revoked. The infringing party may also face privacy lawsuit filed against by the injuring party. Criminal liability may also be applicable for illegal sale or acquisition of personal information that falls under the scope of criminal law.

How is electronic marketing regulated?	**In general, no one may send commercial electronic information to individuals without the consent of or the request from the recipients.** The Law on Advertising (2015 Revision) provides that no organization or individual may deliver advertisements (including electronic advertisement) to any persons without their consent or their request. When an advertisement is sent through electronic message, the true identity and contact information of the sender shall be clearly indicated and those to whom the advertisement is sent shall be provided with the methods for refusing to continue to receive the advertisements. Further, sending advertisement via internet shall not interrupt the normal use of internet by the users and if the advertisement is sent via pop-up, the pop-up shall have an obvious button for turning off to ensure that the users can turn off the pop-up with one click. There are also specific rules for sending advertisement by email or text message.
Are there any recent developments or expected reforms?	**In general, the state is considering more comprehensive protection of personal information and stricter localization requirements for personal information in certain key industries in draft laws.** The first draft the Cyber Security Law released by National People's Congress Standing Committee ("**NPCSC**") in July 2015 provides that personal information held by key information infrastructure shall be stored within China. The draft is still under deliberation by the NPCSC now and has not been finally adopted.

	There also has been discussion about a unified personal information protection law but there is no official agenda of whether and when the law will be promulgated.

Contact Information

Marissa Dong dongx@junhe.com	**JunHe LLP** China Resources Building, 26th Floor Beijing China 100005 Tel 86.10.8519.1300

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Hong Kong

Prepared by Deacons, Lex Mundi member firm for Hong Kong

Key Legislation Overview	
What is the Key Legislation?	**The Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong)**. The key legislation governing privacy in Hong Kong is the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) ("**PDPO**"). The PDPO sets out, among other things, six Data Protection Principles ("**DPPs**") that govern the: (i) purpose and manner of collection of personal data; (ii) accuracy and duration of retention of personal data; (iii) use of personal data; (iv) security of personal; (v) information to be generally available; and (vi) access to personal data and disclosure of personal information. Under Section 4 of the PDPO, a data uder shall not do any act, or engage in a practice, that contravenes a DPP unless the act or practice, as the case may be, is required or permitted under the PDPO. The PDPO allows the Privacy Commissioner to issue guidance on how the Privacy Commissioner intends to interpret the provisions of the PDPO. These are generally known as "**Guidance Notes**". However, these Guidance Notes are not legally binding. Currently, the following Guidance Notes have been issued by the Privacy Commissioner in Hong Kong: • Collection and Use of Biometric Data • CCTV Surveillance and Use of Drones • Data Breach Handling and the Giving of Breach Notifications • Data Users on the Collection and Use of Personal Data

	• Data Users on the Collection and Use of Personal Data through the Internet • Direct Marketing • Electioneering Activities • Mobile Service Operators • Personal Data Erasure and Anonymisation • Personal Data Protection in Cross-border Data Transfer • Preparing Personal Information Collection Statement and Privacy Policy Statement • Proper Handling of Customers' Personal Data for the Banking Industry • Proper Handling of Customers' Personal Data for the Insurance Industry • Proper Handling of Data Correction Request by Data Users • Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users • Property Management Practices • Use of Personal Data Obtained from the Public Domain • Use of Portable Storage Devices
Key Data Protection Provisions	
What data is protected?	**The PDPO protects personal data being data about an identifiable individual.** The PDPO protects "**personal data**", which is defined in the PDPO as "any data: (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable".

Who is subject to privacy obligations?	**The PDPO applies to any data user (including the government)** The PDPO applies to any "**data user**" (including the government), which is defined in the PDPO as "in relation to personal data, a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data". The PDPO sets out certain exemptions including (without limitation): • performance of judicial functions; • security in respect of Hong Kong; • crime; • health; • news; • statistics and research; • emergency situations. Such exemptions do not necessarily give blanket exemptions to the whole of the PDPO, but instead may provide exemptions for only parts of the PDPO.
How is the collection of personal data regulated?	**Generally, personal data collected from a data subject must be for a lawful purpose connected with a function or activity of the data user, necessary for that purposes, and adequate but not excessive, and the data user must take all practicable steps to make the data subject aware of certain matters before collection.** DPP 1 of the PDPO sets out certain requirements in relation to the purpose and manner of collection of personal data. Generally, personal data should not be collected unless: • the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

	• the collection of the data is necessary for or directly related to that purpose; • the data is adequate but not excessive in relation to that purpose. If personal data is to be collected directly from a data subject, all practicable steps should be taken to ensure: • he is explicitly or implicitly informed on or before collection whether it is obligatory or voluntary for personal data to be collected and, if obligatory, the consequences of not providing such personal data; • he is explicitly informed on or before collecting the data of: (i) the purposes (in general or specific terms) for which such personal data are to be used; and (ii) the classes of persons to whom such personal data might be transferred; and • he is explicitly informed on or before first use of the data for the purpose for which it was collected of: (i) his right of access to, and to request the correction of such personal data; and (ii) the name or job title and address of the individual who is to handle any such request.
How are the use and disclosure of personal data regulated?	**Generally, subject to a data subject's prescribed consent, a data user may use or disclose personal data only for the purpose for which it was collected or a purpose directly related to such purpose.** Under DPP 3, a data user must not, without the "**prescribed consent**" (express consent of the person given voluntarily and not withdrawn) of the data subject, use (which includes disclose or transfer) any personal data collected in accordance with DPP 1 for any purpose other than the purpose for which the personal data was to be used at the time of the collection of the personal data (or a purpose directly related to such purpose).

	The use and disclosure of personal data for direct marketing purposes is strictly regulated in Hong Kong, where "**direct marketing**" is the offering, or advertising of the availability of goods, facilities or services through direct marketing means (i.e. sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or making telephone calls to specific persons): • data users who intend to use a data subject's personal data in direct marketing must, before using personal data in direct marketing: (a) inform the data subject (i) that the data user intends to so use the personal data; and (ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use; (b) provide the data subject with the following information in relation to the intended use (i) the kinds of personal data to be used; and (ii) the classes of marketing subjects in relation to which the data is to be used; and (c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subjects consent to the intended use. • data users must obtain the data subject's "consent" (which, in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision;) to use personal data in direct marketing; • data users must notify the data subject when using personal data in direct marketing for the first time that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires; • data users must cease to use the personal data for direct marketing upon a data subject's request; • data users who intend to provide a data subject's personal data to another party for use by that other

	person in direct marketing must, before providing personal data to the other party: (a) inform the data subject in writing (i) that the data user intends to so provide the personal data; and (ii) that the data user may not so provide the data unless the data user has received the data subject's consent to the intended provision; (b) provide the data subject with the following written information in relation to the intended provision (i) if the personal data is to be provided for gain, that the personal data is to be so provided; (ii) the kinds of personal data to be provided; (iii) the classes of persons to which the personal data is to be provided; and (iv) the classes of marketing subjects in relation to which the personal data is to be used; and (c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subjects consent to the intended provision in writing. • data users must obtain the data subject's consent to provide personal data to another party for use in direct marketing; • data users must cease to provide personal data to another party for use in direct marketing upon a data subject's request.
How are storage, security and retention of personal data regulated?	**Personal information must be protected from unauthorised loss, use, modification or disclosure with reasonable security safeguards. Agencies must not keep personal information for longer than is required.** In terms of the storage and security of personal data, under DPP 4, a data user must take all practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to:

	• the kind of data and the harm that could result if any of those things should occur; • the physical location where the data is stored; • any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; • any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and any measures taken for ensuring the secure transmission of the data. In terms of the retention of personal data, under DPP 2, a data user must take all practicable steps shall be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the personal data is or is to be used.
Are there rights of access to and correction of personal data?	**Generally, a data user must take all practicable steps to ensure that personal data is accurate. Subject to specific grounds for refusing access or correction, a data subject is entitled to have access to any personal data about them held by a data user, and for correction of such personal data.** Under DPP 2, a data user must take all practicable steps to ensure that: • personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used; • where there are reasonable grounds for believing that personal data is inaccurate: (i) the personal data is not used for that purpose unless and until those grounds cease to be applicable to the personal data, whether by the rectification of the data or otherwise; or (ii) the personal data is erased; • where it is practicable in all the circumstances of the case to know that: (i) personal data disclosed on or

	after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and (ii) that personal data was inaccurate at the time of such disclosure, that the third party: (A) is informed that the data is inaccurate; and (B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose. Under DPP 6, a data subject shall be entitled to: • ascertain whether a data user holds personal data of which he is the data subject; • request access to personal data: (i) within a reasonable time; (ii) at a fee, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is intelligible; • be given reasons if a request for access to personal data is refused; • object to a refusal for access to personal data; • request the correction of personal data; • be given reasons if a request for the correction of personal data is refused; and • object to a refusal for the correction of personal data. Under the PDPO, in certain circumstances, a data user must refuse to comply with a personal data access request or a personal data correction request (e.g. if the data user is not supplied with such information as the data user may reasonably require in order to satisfy the data user as to the identity of the requestor), while in other circumstances a data user may refuse the same (e.g. if the data user is not satisfied that the personal data to which the request relates is inaccurate).

Are there restrictions on cross border data transfers?	**Section 33 of the PDPO restricts/controls the transfer of personal data outside of Hong Kong (except in certain circumstances, but it is not yet in force.** Section 33 of the PDPO restricts/controls the transfer of personal data outside of Hong Kong, but it is not yet in force. Section 33 of the PDPO provides that a data user shall not transfer personal data to a place outside of Hong Kong unless at least one of the following conditions are met: • the place has been approved by the Privacy Commissioner in writing; • the data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the PDPO; • the data subject has consented in writing to the transfer; • the data user has reasonable grounds for believing that, in all the circumstances of the case, the transfer is for the avoidance or mitigation of adverse action against the data subject; and it is not practicable to obtain the data subject's consent but, if practicable, such consent would be given; • the data is exempt from Principle 3 under Part VIII of the PDPO (i.e. the personal data is held for certain purposes such as domestic purposes, employment or staff planning, the prevention or detection of crime, the security or defence of Hong Kong, legal professional privilege, news activities etc); The Privacy Commissioner has also issued a Guidance Note on cross border transfer of personal data (Personal Data Protection in Cross-border Data Transfer), which recommends steps a data user should take to comply with Section 33 of the PDPO, notwithstanding that Section 33 of the PDPO is not yet in force.

Are there any notification requirements for data breaches?	**There are no mandatory reporting requirements for breaches of the PDPO.** There are currently no requirements under the PDPO for a data user in breach of the PDPO to notify the Privacy Commissioner or any third parties. However, the Privacy Commissioner has issued a Guidance Note (Guidance Note on Data Breach Handling and the Giving of Breach Notifications) which includes, among other things, a recommendation from the Privacy Commissioner that data users adopt a system of notification in handling a data breach.
Who is the privacy regulator?	**The PDPO establishes the office of the Privacy Commissioner. The functions and powers of the Privacy Commissioner range from monitoring and supervising compliance with the provisions of the PDPO, to investigating complaints of contravention of the PDPO and serving enforcement notices.** The Privacy Commissioner has a range of functions and powers under the PDPO including, but not limited to, in relation to the monitoring and supervising compliance with the provisions of the PDPO; promote awareness and understanding of, and compliance with, the PDPO (including undertaking promotional or educational activities); carrying out inspections of data users' personal data systems; and investigating complaints of contravention of the PDPO and serving enforcement notices. The PDPO also gives the Privacy Commissioner the power to issue guidelines for data users and data subjects on the PDPO indicating the manner in which the Privacy Commissioner proposes to perform the functions, or exercise any of the powers, of the Privacy Commissioner (see above Question 1 for a list of Guidance Notes issued by the Privacy Commissioner). The Privacy Commissioner also has the power to promote and assist bodies representing data users

	to prepare codes of practice. As with the Guidance Notes, these codes of practice are not legally binding. The current codes of practice in effect are: • Code of Practice on Consumer Credit Data (January 2013) • Code of Practice on Human Resource Management (April 2016) • Code of Practice on the Identity Card Number and Other Personal Identifiers (December 1997) • Privacy Guidelines: Monitoring and Personal Data Privacy at Work (April 2016)
What are the consequences of a privacy breach?	**A failure to comply with the PDPO may result in an Enforcement Notice which if not complied with may result in a fine and/or imprisonment. Other breaches of the PDPO may also result in an offence which, on conviction, may result in fines and/or imprisonment, with particularly rigorous fines and imprisonment for breaches of the PDPO in relation to the direct marketing regime.** If a person believes there has been a breach of the PDPO, a complaint may be made to the Privacy Commissioner. The Privacy Commissioner then has the power to investigate the complaint. Investigations may also be initiated on the Privacy Commissioner's own initiative. If the Privacy Commissioner is of the opinion that the relevant data user is contravening or has contravened the PDPO, the Privacy Commissioner may serve on the data user a notice in writing directing the data user to remedy and, if appropriate, prevent any recurrence of the contravention (known as an "Enforcement Notice"). There is a miscellaneous offence where a data user who, without reasonable excuse, contravenes any requirement under the PDPO commits an offence and is liable on conviction to a fine of up to HK$10,000 (though this does not apply to breaches of a DPP or certain specific sections of the

	PDPO). Such specific offences with corresponding fines and/or imprisonment depending on the relevant offence, include (without limitation): • a data user who knowingly or recklessly in a data user return or change notice supplies any information which is false or misleading in a material particular, commits an offence and is liable on conviction to a fine of up to HK$10,000 and to imprisonment for up to 6 months; • a person who, in a data access request, supplies any information which is false or misleading in a material particular for the purposes of having the data user: (a) inform the person whether the data user holds any personal data which is the subject of the request; and (b) if applicable, supply a copy of the data, commits an offence and is liable on conviction to a fine of up to HK$10,000 and to imprisonment for up to 6 months; • a person who, in a data correction request, supplies any information which is false or misleading in a material particular for the purpose of having the personal data corrected as indicated in the request, commits an offence and is liable on conviction to a fine up to HK$10,000 and to imprisonment for up to 6 months; • any data user that contravenes an Enforcement Notice commits an offence and is liable: (a) on a first conviction, to a fine of up to HK$50,000 and to imprisonment for up to 2 years and if the offence continues after the conviction to a daily penalty of up to HK$1000; (b) on a second or subsequent conviction, to a fine of up to HK$100,000 and to imprisonment for up to 2 years, and if the offence continues after the conviction, to a daily penalty of up to HK$2000. • a data user who, having complied with an Enforcement Notice, intentionally does the same act or makes the same omission in contravention of the requirement under the PDPO, as specified in the Enforcement Notice, commits an offence and is liable

	on conviction to a fine of up to HK$50,000 and to imprisonment for up to 2 years, and if the offence continues after the conviction, to a daily penalty of up to HK$1000; • if a person: (a) without lawful excuse, obstructs, hinders or resists the Privacy Commissioner or a prescribed officer in performing the functions or exercising the powers of the Privacy Commissioner or the officer; (b) without lawful excuse, fails to comply with any lawful requirement of the Privacy Commissioner or a prescribed officer; or (c) in the course of the performance or exercise by the Privacy Commissioner or a prescribed officer of functions or powers: (i) makes to the Privacy Commissioner or the officer a statement which the person knows to be false or does not believe to be true; or (ii) otherwise knowingly misleads the Privacy Commissioner or the officer, the person commits an offence and is liable on conviction to a fine up to HK$10,000 and to imprisonment for up to 6 months; • if a person (1) discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent: (a) to obtain gain in money or other property, whether for the benefit of the person or another person; or (b) to cause loss in money or other property to the data subject; or (2) (a) discloses any personal data of a data subject which was obtained from a data user without the data user's consent; and (b) the disclosure causes psychological harm to the data subject, the person commits an offence and is liable on conviction to a fine of up to HK$1,000,000 and to imprisonment for up to 5 years. A data user who fails to comply with Section 33 (not yet in force) without reasonable excuse will commit an offence under Section 64A of the PDPO which carries a fine of up to HK$10,000.

	The PDPO also imposes strict provisions in relation to the use of personal data in direct marketing, and a data user shall commit an offence if the data user fails: • to take certain actions before using personal data in direct marketing (liable on conviction to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to obtain the data subject's consent to use personal data in direct marketing (liable on conviction to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to notify the data subject when using personal data in direct marketing for the first time (liable on conviction to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to cease to use the personal data for direct marketing upon a data subject's request(liable on conviction to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to take certain actions before providing a data subject's personal data to another party for use by that other person in direct marketing (liable on conviction to a fine of up to HK$1,000,000 and to imprisonment for up to 5 years if for gain, and otherwise to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to obtain the data subject's consent to provide personal data to another party for use in direct marketing (liable on conviction to a fine of up to HK$1,000,000 and to imprisonment for up to 5 years if for gain, and otherwise to a fine of up to HK$500,000 and to imprisonment for up to 3 years); • to cease to provide personal data to another party for use in direct marketing upon a data subject's request(liable on conviction to a fine of up to HK$1,000,000 and to imprisonment for up to 5 years

	if for gain, and otherwise to a fine of up to HK$500,000 and to imprisonment for up to 3 years). Data subjects may also sue data users in breach of the PDPO directly for damages suffered, including injury to feeling.
How is electronic marketing regulated?	**In addition to the PDPO, unsolicited electronic messages are regulated under the Unsolicited Electronic Messages Ordinance (Chapter 593 of the Laws of Hong Kong).** In addition to the PDPO and the regulation of direct marketing through electronic means of communication, Unsolicited electronic messages are regulated under the Unsolicited Electronic Messages Ordinance (Chapter 593 of the Laws of Hong Kong) (UEMO). The UEMO prohibits the sending of "commercial electronic messages" (CEM) except in certain circumstances. Under the UEMO, a CEM is defined as an electronic message, the purpose or one of the purposes of which is (in the course of or in the furtherance of any business): • to offer to supply goods, services, facilities, land, or an interest in land; • to offer to provide a business opportunity or an investment opportunity; • to advertise or promote goods, services, facilities, land or an interest in land; • to advertise or promote a business opportunity or an investment opportunity; • to advertise or promote a supplier, or a prospective supplier, of goods, services, facilities, land or an interest in land; or • to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity.

	Under the UEMO, CEMs must not: • be sent unless the CEM includes accurate sender information; • be sent unless the CEM contains an unsubscribe facility; • be sent after an unsubscribe request is sent; • be sent to an electronic address listed in the do-not-call register; • use misleading subject headings; • be sent with calling line identification information concealed
Are there any recent developments or expected reforms?	**The Privacy Commissioner has recently issued a Guidance Note in relation to cross-border transfers of personal data, indicating another step towards bringing Section 33 of the PDPO into force.** Section 33 of the PDPO is not yet in force (and has not been brought into force for over 15 years). This is partly because, pursuant to Section 33, the Privacy Commissioner must prepare, among other things, a list of approved jurisdictions. However, the Privacy Commissioner has recently issued a Guidance Note in relation to Section 33 of the PDPO in relation to cross-border transfers of personal data, indicating another step towards bringing this long-dormant provision into force.

Contact Information

Charmaine Koo charmaine.koo@deacons.com.hk **David Swain** David.swain@deacons.com.hk	**Deacons** Alexandra House 5th Floor Central Hong Kong Tel 852.2825.9211

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

India

Prepared by Shardul Amarchand Mangaldas & Co, Lex Mundi member firm for India

Key Legislation Overview	
What is the Key Legislation?	**The Information Technology Act, 2000 (as amended in 2008) ("IT Act") read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Privacy Rules") deal with certain aspects of protection of personal data.** India does not have a specific legislation dedicated to data protection. At present, the IT Act read with the Privacy Rules recognizes the concept of personal information and sensitive personal data and to that limited extent govern the aspects of data protection and privacy in India. a) The IT Act extends to the whole of India. b) It is also applicable to any offense or contravention committed outside India by any person irrespective of its nationality if the act or conduct constituting the offence or contravention involved a computer, computer system or computer network located in India. c) Through an amendment in 2008 , a few provisions relating to the protection of personal data were introduced into the IT Act: The notable changes are embodied by Section 43A and Section 72A . Section 43A provides for compensation in instances where there has been a failure to protect sensitive personal data and information. Section 72A prescribes punishment for disclosure of information which is in breach of a lawful contract.

d) On April 11, 2011, the Central government announced the Privacy Rules. These rules represent an important advancement in the regulation of data privacy. They impose stringent obligations on corporations for the implementation of adequate steps which protect personal information and sensitive personal data or information ("SPDI").

e) The Privacy Rules contain detailed provisions relating to protection of data such as:

   (i) collection and use of personal information and SPDI;
   (ii) mandatory publication of privacy policy for corporations that collect personal information;
   (iii) technical requirements for security practices and procedures; and
   (iv) disclosure as well as transfer of personal information and SPDI.

f) In addition to the aforesaid provisions in the IT Act, the right to privacy has been recognized by numerous decisions of the Supreme Court of India as well as various High Courts. They have consistently recognized the same as a part of the Fundamental Rights guaranteed by Article 21 of the Indian Constitution, which aims at protecting life and personal liberty.

g) Various other Indian statutes such as, (i) Indian Contract Act, 1872 ; (ii) Indian Penal Code, 1860 ; (iv) Specific Relief Act, 1963 ; (v) Copyright Act, 1957 etc. also contain provisions, which directly or indirectly protect against breaches of confidentially and unauthorised disclosure of personal data.

Key Data Protection Provisions	
What data is protected?	**The Privacy Rules provide for the protection of - 'personal information' and SPDI.** The provisions of the IT Act read with the Privacy Rules provide for the protection of Personal Information and SPDI. 'Personal information' is defined as: *"any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying that person."* It is to be noted that this definition specifically applies to natural persons and not corporate entities or other legal persons. “SPDI” is defined as: *"personal information that consists of information relating to passwords; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical history and records; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise."* **Note:** Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 shall not be regarded as SPDI.

Who is subject to privacy obligations?	**The Privacy Rules only apply to bodies corporate or persons located in India as is clear from the 24 August 2011 Press Note issued by the Ministry of Communication and Information Technology.** Bodies Corporate and persons located in India are subject to the Privacy obligations. A body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. A press note dated 24 August 2011 clarifies, that the a body corporate which provides services relating to collection, storage, dealing or handling of SPDI under a contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6 of the Privacy Rules.
How is the collection of personal data regulated?	**The entity which seeks to use personal data or information cannot collect the same unless it obtains the prior consent of the provider of such data or information.** The personal data including SPDI should be collected : a) only for a lawful purpose; b) when the collection is necessary for that purpose. The information collected must be used only for the purpose for which it has been collected. c) The providers of information must be informed of the purpose for which the Sensitive Data is being collected and their consent must be obtained. Note: The Press Note dated August 24, 2011 makes it clear that the consent under Rule 5(1) includes consent given by any electronic communication. d) While collecting information directly from the person concerned, the body corporate or any person on its

	behalf must ensure that the person concerned has knowledge of — • the fact that the information is being collected; • the purpose for which the information is being collected; • the intended recipients of the information; and • the name and address of — i. the agency that is collecting the information; and ii. the agency that will retain the information. **Withdrawal of Consent** - The providers of information must be given an option to not provide the Sensitive Data sought or collected and also, to subsequently withdraw his / her consent given earlier.
How are the use and disclosure of personal data regulated?	**Subject to specific exceptions, a body corporate may only use or disclose personal information /SPDI for the purpose for which it was collected.** **Disclosure of SPDI by a body corporate to any third party requires prior permission from the provider of such information.** --- The Privacy Rules disallow the disclosure of any collected SPDI to a third party without the prior permission of the provider **except** when the disclosure is : i. in terms of a contract between the body corporate and the provider of the information; ii. necessary for compliance with a legal obligation; and iii. to government agencies mandated under law to obtain information for the purposes of verification of identity, prevention, detection, investigation of cyber incidents, prosecution and punishment of offences.

	A third party which receives any SPDI through the above explained mechanism is disallowed from disclosing it further.
How are storage, security and retention of personal data regulated?	**The Privacy Rules state that a body corporate holding SPDI shall not retain such information for longer than is required for the lawful purpose which requires the usage of such information. Further, body corporate is required to comply with reasonable security practices and procedures.** **Storage and Retention** The entity which seeks to use SPDI cannot store it for longer than is required for any lawful use, or as otherwise required under any other law. The IT Act also prescribes the manner in which documents or records are to be retained in electronic form, if the same is required by any other applicable law. It requires that- a. The information retained should be accessible for any subsequent reference; b. The record should be retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately, the information originally generated, sent or received; and c. The information regarding the origin, destination, date and time of dispatch or receipt of the electronic record are available in the electronic record. **Security** The Privacy Rules require that body corporates adopt reasonable security practices and standards and that they have a comprehensive documented information security programme and information security policies. The international standard IS/ISO/IEC 27001 on "Information Technology-Security Techniques-Information Security

	Management System-Requirements" is an example of the above mentioned standard. The adopted measures should be designed to protect SPDI from “unauthorized access, damage, use, modification, disclosure or impairment” and can be specified by an agreement between the parties or a law. If such specification is absent, such practices can be prescribed by the Central Government.
Are there rights of access to and correction of personal data?	**The providers of information have the right to review the information provided, and to ask for inaccurate or deficient information to be corrected.** **Information retained should be accessible for any subsequent reference.** The personal information and SPDI should be made available to the providers of information for review and modification, as and when requested by them. This is to allow the providers of information to correct the personal information or SPDI, if it is found to be inaccurate or deficient in any manner.
Are there restrictions on cross border data transfers?	**India permits the transfer of data to other jurisdictions for performance of a lawful contract between the body corporate or any person on its behalf and the provider of information (data subject) or in cases where the data subject has consented to the transfer.** At present, there are no specific restrictions or requirements under Indian Law for cross border transfers of personal information/ SPDI. Similarly, onward transfers of the data will continue to be governed by the contractual provisions between the parties. Unless the contract otherwise specifies, the transfer of SPDI including any information is subject only to two restrictions -

	a) The entity receiving the information must ensure the same level of data protection, as provided under the Privacy Rules. b) The transfer should be necessary for the performance of a lawful contract between the body corporate and the provider of information or the provider should have consented to such transfer.
Are there any notification requirements for data breaches?	**The Central Government has been empowered by Section 70B of the IT Act to appoint an agency called the Indian Computer Emergency Response Team ("Cert-In").** **This agency would provide forecast and alerts of cyber security incidents, provide emergency measures for handling such incidents, coordinate cyber incident response activities, and collect, analyse and disseminate information on cyber incidents.** Service providers, intermediaries, data centres and corporate entities are required to mandatorily notify the occurrence of certain 'cyber security incidents', under the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**Cert-In Rules**"). The CERT-In serves as a national agency and performs the functions listed in Section 70B(4) of the IT Act. These functions are: a) collection, analysis and dissemination of information on cyber incidents; b) forecast and alerts of cyber security incidents; c) emergency measures for handling cyber security incidents; d) coordination of cyber incidents response activities; e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, presentation, response and reporting of cyber incidents;

	f) Such other functions relating to cyber security as may be prescribed. The Cert-In functions at Department of Information Technology, Ministry of Communications and Information Technology and is located at “Electronics Niketan”, 6, CGO Complex, Lodhi Road, New Delhi – 110003. CERT-In is required to operate an Incident Response Help Desk on a 24 hours basis every day, including Government and other public holidays, in order to facilitate the reporting of cyber security incidents. Any individual, organization or corporate affected by cyber security incidents may report the incident to CERT-In. The occurrence of the following types of cyber security incidents trigger the notification requirements under the Cert-In Rules: • Targeted scanning/ probing of critical networks/ systems • Compromise of any critical information/ systems • Unauthorized access of IT systems/ data • Defacement of websites or intrusion into websites & unauthorized changes such as inserting malicious codes, links to external websites • Malicious code attacks such as spreading viruses, worms/ Trojans/ Botnets/ Spyware • Attacks on servers such as Database, Mail and DNS & Network devices such as Routers • Identity theft, Spoofing and phishing attacks • Denial of service (DoS) & Distributed Denial of service (DDoS) attacks • Attacks on critical infrastructure, SCADA systems and wireless networks • Attacks on Application such as E-governance and E-commerce etc.

Who is the privacy regulator?	**There is no regulator responsible for the enforcement of the data protection rules.** **The Ministry of Communications and Information Technology ("IT Ministry") is empowered to make rules under Section 43A of the IT Act.** --- The IT Ministry has the power to issue rules under the IT Act. While there exists no regulator for the enforcement of the Privacy Rules, there are government agencies which issue guidelines on behalf of the government, within the scope of the powers granted by the IT Act. One such agency is the Department of Electronics and Information Technology (**DeitY**), a division of the IT Ministry.
What are the consequences of a privacy breach?	**The IT Act and the Privacy Rules prescribe remedies in the nature of a claim for damages for the negligent acts of corporate bodies.** **If the negligence leads to wrongful loss or gain for any person, Section 43A of the IT Act allows for compensation claims up to INR 5,00,00,000.** **Similarly, Section 72A of the IT Act prescribes the punishment for any person including an intermediary who intentionally discloses personal information without the consent of the data subject, or in breach of a lawful contract. Such persons can be imprisoned for a period up to 3 years, or be fined up to INR 5,00,000, or both.** **Further, a penalty up to INR 25,000 has been prescribed for a contravention of the Privacy Rules.** --- Section 43A of the IT Act requires a corporate body corporate which possesses, deals or handles SPDI in a computer resource owned, controlled or operated by it to implement and maintain reasonable security practices and procedures.

	Wrongful loss or wrongful gain to any person due to non-compliance with the above requirements would result in the body corporate being liable to pay damages by way of compensation to the person affected. Section 72 of the IT Act also prescribes the penalty for the breach of confidentiality and privacy by a person who discloses any electronic records, books, registers, correspondences, information, documents or any other material without the consent of the concerned person. Those punished under this provision can be imprisoned up to two years or fined up to INR 1,00,00 or both. The IT Act separately deals with the disclosure of personal information which is in breach of a lawful contract. Under Section 72A, such disclosure is a punishable offence when done intentionally, or with the knowledge that it is likely to cause wrongful gain or loss. The punishment prescribed for the same is imprisonment up to three years or a fine up to INR 5,00,000, or both. For invoking the above provision, the following conditions need to be satisfied: • Access to any material containing personal information; • Existence of an intention or knowledge of causing wrongful loss or wrongful gain; • Disclosure without consent of the person concerned, or in breach of a lawful contract Penalties under the IT Act apply to “any offence or contravention thereunder committed outside India by any person”. The IT Act clarifies that this provision is applicable only if the “act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India”.

How is electronic marketing regulated?	**The IT Act does not explicitly refer to electronic marketing.** **However, the Telecom Regulatory Authority of India (TRAI) effectively enforces the Do Not Call (DNC) Registry.** The right to "opt out" of email marketing has been guaranteed by the Privacy Rules. They also require that companies address marketing and information collection practices in their privacy policies. Additionally, TRAI effectively enforces the Do Not Call (DNC) Registry. Repeated violations of the DNC norms can lead to tele-marketing companies losing their licenses. The protection of privacy from unsolicited commercial calls has to a great extent been guaranteed by the Telecom Unsolicited Commercial Communications Regulation, 2007. The National Do Not Call Register is periodically updated by service providers. Customers can choose to register for the same, and can also revoke an earlier registration. The register is centrally maintained by the NIC. The Department of Telecommunications has sought to improve accountability by requiring all telemarketers to register with it.
Are there any recent developments or expected reforms?	**The Government has signalled an intent to replace the existing privacy regime. However, the Privacy and Personal Data Protection Bills are yet to be released for public consideration.** While numerous legislation aimed at strengthening the privacy regime in India have been drafted, from information available in public domain it is discernible that none of them have even been introduced in the parliament.

	The salient features of these legislation (The Privacy Protection Bill, 2013 and The Personal Data Protection Bill, 2014) included- 1. The right to demand destruction of the data which is unnecessary for the purpose for which it is collected. 2. The requirement of consent for disclosure of personal data and not just SPDI. 3. The exemption from prior consent required for the disclosure of personal data being restricted to specific grounds such as national security, defence, public order and so on. 4. The continuing liability of entities after they transfer data to others. 5. Notification obligations for corporates, if the confidentiality, integrity or safety of personal data has been violated due to enumerated reasons. Additionally, the recently passed Aadhar (Target Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 provides for the protection of various information collected in furtherance of providing individuals with the Aadhar Unique Identification Number. It provides for the protection of biometric information such as an individual's finger prints, iris scans and other biological identifiers (specified by regulations). This information can only be used for Aadhaar enrolment and authentication. Further, it cannot be shared with anyone, or displayed publicly, except for the purposes enumerated by the regulations. Section 37 of the Aadhar Act penalizes the illegal disclosure of information with imprisonment up to three years or a fine up to ten thousand rupees, or both. In the case of a company, the fine can extend up to one lakh rupees. However, this legislation is currently being challenged before the Supreme Court of India.

Contact Information

Tejas Karia tejas.karia@AMSShardul.com	**Shardul Amarchand Mangaldas & Co** Amarchand Towers New Delhi India 110 020 Tel 91.11.4159.0700

References

1. Section 75 of IT Act: Act to apply for offence or contravention committed outside India- (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
   (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.
2. The amendments to IT Act have come into effect from October 28, 2009.
3. **43A. Compensation for failure to protect data.--**
   Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
   Explanation.-- For the purposes of this section,--
   (i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
   (ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
   (iii) "Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
4. ***72A. Punishment for disclosure of information in breach of lawful contract.--***
   Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that his likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.
5. *Kharak Singh v State of UP* AIR 1963 SC 1295, *Gobind v State of M.P.* (1975) 2 SCC 148, *State v Charulata Joshi* (1999) 4 SCC 65, *R. Rajagopal v State of Tamil Nadu* AIR 1995 SC 264.
6. Section 73 & 74 of the Contract Act deal with remedies for contractual damages by way of compensation for violation of terms of the contract or non-performance of the obligations.
7. Section 406: Criminal Breach of Trust (imprisonment up to three years or fine and/or both), Section 420: Cheating (imprisonment up to seven years imprisonment or fine and/or both).
8. Specific Performance for breach of contract.
9. Section 2(1)(i), Privacy Rules.
10. Section 3, Privacy Rules
11. https://www.dsci.in/sites/default/files/Government%20Clarification%20on%20notified%20Rules%20under%20sec%2043A%20of%20IT%20(Amendment)%20Act%202008.pdf (last visited on 04/04/2016)
12. Explanation (i), Section 43A, IT Act.
13. Ibid
14. Rule 5(3)
15. Rule 5 (7)
16. Rule 6
17. Rule 6(4)
18. Sub Clause (4) of Rule 5 of the Privacy Rule
19. Section 7 of the IT Act
20. Rule 8 of Privacy Rules
21. Section 43A(ii), IT Act.
22. Rule 5(6) of Privacy Rules
23. Rule 7, Privacy Rules
24. Rule 12(1)(a) of Cert-In Rules
25. Section 43 A
26. Section 1(2), IT Act
27. Section 75(2), IT Act
28. http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/consultion.pdf (Last visited on 4/4/2016)

29. Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorized under this Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Indonesia

Prepared by Ali Budiardjo, Nugroho, Reksodiputro, Lex Mundi member firm for Indonesia

Key Legislation Overview	
What is the Key Legislation?	**There is no dedicated law/ regulation pertaining to data privacy, but data privacy provisions can be found in regulations for specific fields of business.** Despite no specific law/regulation on data privacy, there are various provisions in laws and regulations that relate to privacy and data protection. They apply to specific fields of business, trade and industry, including the banking sector, the telecommunications sector, the medical services sector and the electronic transactions. The specific regulations are as follow: 1. Human Rights Law Under Article 29 (1) of the Law No. 39 of 1999 concerning Human Rights ("**Human Rights Law**"), everyone has the right to protection of his ***privacy***, family, honour, dignity and rights of ownership. Furthermore, Article 32 of the Human Rights Law states that freedom and confidentiality in correspondence, including communication through electronic telecommunications means may not be interfered with, except upon the order of a court or other legitimate authority according to the prevailing laws and regulations. 2. Banking & Financial Services Law As provided under Article 40 of Law No. 7 of 1992 as amended by Law No. 10 of 1998 concerning Banking Law ("**Banking Law**"), banks in Indonesia are prohibited from disclosing information regarding their customers to third parties, except on certain conditions explicitly mentioned in

	the Banking Law, such us for taxation purposes, debt settlement which has been delegated to Debt and Auction Affair Agency, criminal proceeding purposes, civil lawsuit between the bank and its customer, interbank information exchange, and inheritance. In regard to Financial Services, pursuant to Article 31 of Financial Services Authority ("Otoritas Jasa Keuangan" or "OJK") Regulation No. 1/POJK.07/2013, dated 26 July 2013, concerning Consumer Protection in the Financial Services Sector ("**Regulation No. 1/2013**"), financial services business actors are prohibited from providing third parties with data and/or information regarding their own consumers except where (i) the consumer concerned has given his/her/its written approval for such purpose; and/or (ii) the provision of the data and/or information is required under the prevailing regulation. Further, based on Bank Indonesia Regulation No. 16/1/PBI/ 2014 concerning payment system services consumers protection ("**Regulation No. 16/2014**"), the provider of payment system services must keep the confidentiality of consumers' data and/or information. In order to keep the confidentiality of consumers' data and/or information, the provider must have and implement policies on the protection of consumers' data and/or information. Article 15 of Regulation No. 16/2014 also stipulates that providers are prohibited to provide consumers' data and/or information to other parties, except in the event that the provider has obtained prior written approval from the consumer and/or it is required by the prevailing law and regulations. Regulation No. 16/2014 defines the "*provider of payment system services*" as a bank or non-bank institution that provides payment system services with a permit from Bank Indonesia. Regulation No. 16/2014 also limits the payment system services to the following fields: (i) issuance of instrument to transfer funds and/or withdraw funds; (ii) transfer of funds; (iii) payment instrument through card; (iv) electronic money; (v) provisioning and/or depositing Rupiah; and (vi) other

	payment system operations as regulated under the Bank Indonesia's rules 3. Telecommunications Law Article 42 Paragraph 1 and 2 of the Law No. 36 of 1999 concerning Telecommunications ("**Telecommunications Law**") requires a telecommunications service operator to keep confidential the information transmitted and/or received by a telecommunications services subscriber through telecommunications networks and/or telecommunications services that it is providing, except for the purposes of criminal proceedings. 4. Health Law Article 57 of the Law No. 36 of 2009 concerning Health ("**Health Law**") provides that every person has the right to his/her confidential personal health conditions that have been disclosed to the health care providers, unless for certain condition in which the confidentiality requirements may be exempted. 5. Electronic Information and Transaction Law Article 26 Paragraph 1 of the Law No. 11 of 2008 concerning Electronic Information and Transactions ("**EIT Law**") stipulates that, unless provided otherwise by relevant laws and regulations, use of any information through electronic media that involves personal data of a person must be made with the consent of the person concerned. 6. Public Information Disclosure Law Pursuant to Article 2 paragraph (4) of Law No. 14 of 2008 concerning Public Information Disclosure ("Public Information Disclosure Law"), certain information are exempted from the mandatory disclosure, which include personal data of a person.

	7. Indonesian Criminal Procedural Law Per Article 47 Paragraph 1 of Law No. 8 of 1981 concerning Criminal Procedure ("**Criminal Procedure Law**"), an investigator has the right to retrieve/open, examine and confiscate other documents sent through the post and telecommunication office, communication or transportation agency or enterprise, if the objects concerned are, for a good reason, suspected of having a connection with a criminal case currently being examined, with a special approval issued for such purpose by the head of the district court.
Key Data Protection Provisions	
What data is protected?	**The data subject to protection is different depending on the relevant regulation.** As the data protection regulation is different for each type of field, the object of data protection regulation is also different for each type of field. 1. Banking & Financial Services Law Based on Bank of Indonesia Regulation No. 7/6/PBI/2005 concerning Transparency of Bank Product Information and Customers Personal Data Utilization, Customers Private Information includes all data and information given by the customers at the early step of registration as a customer. Based on OJK Circular Letter No. 14/SEOJK.07/2014 concerning Confidentiality and Security of Data and/or Personal Information of Customers ("**SEOJK 14/2014**"), Personal Data and/or Information shall include: i. Individual: a) name; b) address; c) date of birth and/or age; d) phone number; and/or

	e) name of biological mother. i. Corporation a) name; b) address; c) phone number; d) composition of board of directors and commissioners including their document of identity; e) composition of shareholders. 2. Telecommunication Law Every information being transmitted and/or received by a telecommunications services subscriber through telecommunications networks and/or telecommunications services shall be considered as confidential information. 3. Health Law In general, the Health Law provide protection to customers of health services, especially regarding their identities and medical conditions, in which also including information contained in their medical records. 4. Electronic Information and Transaction Law The EIT law does not provide detailed description on what kind of data is considered as personal data. The protection of personal data is part of privacy rights that include the following definitions: i. the right to enjoy personal life, free from any disturbance; ii. the right to communicate with others without spying others; and iii. the right to observe access to information on personal life or privacy

	5. Public Information Disclosure Law According to Public Information Disclosure Law, the following information shall be categorized as confidential personal data: i. History and condition of family member; ii. History, condition and treatment, medication of physical and psychological health, of a person; iii. Financial condition, asset, revenue, and bank account of a person; iv. Evaluation result in relation with a person's capability, intellectuality, and recommendation on his/her ability; and/or v. personal record of a person in relation with formal and informal educational level activity;
Who is subject to privacy obligations?	**Subject to each relevant regulation.** The relevant party that is subject to privacy obligation also depends on the relevant type of field. 1. Banking & Financial Services Law As provided under SEOJK 14/2014 and Regulation 16/2014, the institutions that are subject to the privacy obligation are banks, payment system service providers and other financial institutions (including insurance and reinsurance company, financing company, security company, pledge company, stock exchange, investment consultant, etc.) 2. Telecommunications Law Article 42 Paragraph 2 of the Telecommunications Law requires telecommunications service operators to keep the confidentiality of information transmitted by their customers. 3. Health Law

	Pursuant to Article 70 paragraph (4) of Law No. 36 of 2014 concerning Medical Workers ("Medical Workers Law"), Medical Workers are obliged to maintain the confidentiality of medical records of the customers/patients. In this case, medical workers include every person that dedicate themselves in health services and have the knowledge and/or skill from education in the medical fields. 4. Electronic Information and Transaction Law The obligation to maintain confidential information transmitted or contain through electronic system, is imposed on Electronic System Provider. In this case, the Electronic System Provider shall include individual, state administrator, corporate body and the public that provides, processes and/or operates an electronic system either individually or jointly for its own interest and/or for other parties' interest to the electronic system users. 5. Public Information Disclosure Law As the Public Information Disclosure Law is designed to regulate Public Institutions, the subject of the privacy obligations are every state administrator institutions, corporations, independent institutions established based on law to undertake activities of public service and other legal entity solely established to undertake activities of public service. 6. Criminal Procedural Law Based on article 48 Paragraph 3 of Criminal Procedure Law, an investigator is obligated to truly maintain the confidentiality of the contents of the documents.

How is the collection of personal data regulated?	**Collection of Personal Data must be done based on the consent of the data owner or the authorized person.** Every data must be obtained from the rightful owner or authorized person based on mutual agreement, except for those regulated by the Criminal Procedural Law. In this case, the data owner must be fully informed on what data is being collected, how the data will be collected, and the purpose of collection of the personal data. In general, under the EIT Law, the use of any information through electronic media that involves personal data of a person must be made with the consent of the person concerned.
How are the use and disclosure of personal data regulated?	**Similar to the collection of personal data, the data owner or the authorized person must be fully informed and consented with the use and disclosure of data. However, the disclosure of personal data may only be done without consent of the data owner or the authorized person under certain circumstances as provided by law.** Other than consent from the individual concerned on the use, disclosure and/or transfer of personal information, the Indonesian laws and regulations are silent on the procedures to be followed for the disclosure of "personal information" However, as noted above, the EIT Law stipulates a definition of "privacy rights" that includes as follows: 1. The right to enjoy personal life, free from any disturbance; 2. The right to communicate with others without spying others; 3. The right to observe access to information on personal life or privacy.

	The disclosure of personal data may only be conducted upon consent of the data owner or authorized person, except in the event of: 1. as required by law; 2. order of the court; 3. for the purpose public interest (usually required authorization from certain government institution); 4. for the purpose of the relevant data owner interest (in the event of health related personal data).
How are storage, security and retention of personal data regulated?	**Generally, all electronic system providers must provide reasonable storage and security system to make the personal data accessible and safe from harm.** There are some general provisions on the obligation of personal data protection under the Indonesian laws and regulations. In general, the responsibility to maintain the security and retention of personal data is held by the institutions that collect and obtain such personal data. Article 26 of EIT Law stipulates that any utilization of information through electronic media regarding personal data must obtain prior consent from the related person. The elucidation of Article 27 of EIT Law further stipulates that personal data protection is a part of privacy rights, as being described in the previous section. In addition to the above, pursuant to article 15 of Government Regulation No. 82 of 2012 on Electronic System and Transaction Operation ("**Regulation 82/2012**"), an operator of an electronic system must: 1. keep the confidentiality, integrity and availability of personal data managed; 2. ensure that the usage and utilization of personal data is based on an agreement with the owner of the

	personal data, except as otherwise stipulated by the law and regulations; and 3. ensure that the use or disclosure of data is based on an agreement with the data owner and accords with the purpose specified to the personal data owner at the time of acquiring the data. Article 22 of Regulation 82/2012 further provides that an operator of an electronic system must safeguard the confidentiality, integrity, authenticity, accessibility, availability and tractability of electronic information and/or electronic documents in accordance with laws and regulations.
Are there rights of access to and correction of personal data?	**The provision on this matter in general can be found under the EIT Law, in which the Electronic Systems Provider is obliged to guarantee the accessibility of the Electronic Information.** As provided under the EIT Law, Electronic System Providers are obliged to guarantee the confidentiality, integrity, authenticity, accessibility, availability, and traceability of the Electronic Information and/or Electronic Documents (which also include any personal data contained therein). On correction of personal data, an Electronic Systems Provider must provide certain features in the respective electronic system, at least to: 1. perform correction; 2. cancel command; 3. give confirmation and reconfirmation; 4. make a choice of continue or stop performing next action; 5. check delivered information on form of contract offer or advertisement; 6. check the status of transaction succession or failure;

	7. read the agreement before continuing with the transaction.
Are there restrictions on cross border data transfers?	**The restriction on cross border data is only regulated for specific field, i.e., banking.** There is no specific provision on cross border data transfer under the Indonesian laws and regulations. However, specifically for the field of banking and finance, pursuant to Bank Indonesia Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilization of Information Technology ("**Regulation No. 9/2007**"), any operation of data centre and/or disaster recovery centre that is performed outside the territory of Indonesia, must obtain prior consent from Bank Indonesia by fulfilling certain requirements. The reason for this is that the operation of a data centre or disaster recovery centre can only be held within the territory of Indonesia. Under Regulation No. 9/2007, data centre is defined as a main facility of the processing of bank's data to support continuous operational activities of a bank, while disaster recovery centre is a replacement facility of data centre in the event of any errors or interruption.
Are there any notification requirements for data breaches?	Under Article 39 of Regulation 82/2012, an electronic system provider is obligated, among others, to have a policy and procedure and its implementation to take any necessary action in the event the data indicated has been hacked or stolen.

Who is the privacy regulator?	**Subject to the relevant regulation, as each regulation determines different regulator for each relevant field.** 1. Banking & Financial Services Law Previously, banking institution is subject to Bank Indonesia as the authorized regulator institution. However, as per the establishment of Financial Services Authority (Otoritas Jasa Keuangan/"**OJK**"), all regulatory and supervision to banking and non-banking financial institution is currently under the authority of OJK. 2. Telecommunications Law and EIT Law Privacy-related regulator for telecommunication and EIT field is under the authority of Ministry of Telecommunication and Information Technology ("**MCIT**"). Specifically, on the telecommunications business, the authority is under the Director General of Post and Information Technology Procurement. For the EIT business, it is under the authority of Director Information Application. 3. Health Law As provided under Medical Workers Law, the regulation is under the authority of Ministry of Health. 4. Public Information Disclosure Law As provided under Article 23 of Public Information Disclosure Law, the implementation of the Public Information Law shall be under the authorization of an Information Committee, an independent institution established based on the Public Information Law itself. The Information Committee consists of a Central Information Committee, Provincial Information Committee, and, if required, Regency/Municipality Information Committee.

What are the consequences of a privacy breach?	**The sanction for breach of privacy is regulated specifically for each relevant field.** 1. Banking & Financial Services Law Based on Article 47 of Banking Law, any members of Board of Commissioners, Board of Directors, bank employees or other affiliated parties who intentionally disclose an information which confidentially must be maintained pursuant to Article 40 of Banking Law, will be sentenced by a maximum 2 (two) year imprisonment and/or charged with a maximum fine of Rp. 200,000,000.00 (two hundred million Rupiah). Further, Article 53 of Regulation No. 1/2013 stipulates that any violation to the provisions contained in Regulation No. 1/2013 will be imposed with administrative sanctions in the form of: a) Written warning; b) Penalty; c) Limitation of business activities; d) Cessation of business activities; e) Revocation of business license. As mentioned previously, Article 31 of Regulation No. 1/2013 stipulates that financial services business actors are prohibited from providing third parties with data and/or information regarding their own consumers except for matters that are explicitly mentioned in this regulation. Thus, any violation to this provision will be imposed with the foregoing administrative sanctions. 2. Telecommunications Law Pursuant to Article 57 of the Telecommunications Law, any telecommunication service operator that breaches the requirement of keeping confidential information as set out in Article 42 of Telecommunications Law will be sentenced by a maximum imprisonment of 2 (two) years and or charged with

	a maximum fine of Rp. 200,000,000.00 (two hundred million Rupiah). 3. Health Law Article 82 paragraph (2) of Health Law stipulates that any medical service facility that fails to comply with the provision of Article 70 paragraph (4) on the obligation of maintaining the confidentiality of medical records of the customers will be imposed with administrative sanctions in the form of (i) verbal warning (ii) written warning (iv) administrative penalty, and/or (v) license revocation. Medical service facility is defined as an equipment and/or place which are utilized to operate a medical service effort, either promotive, preventive, curative, or rehabilitative conducted by the Government, Regional Government, and/or society. 4. Electronic Information and Transaction Law Under EIT Law, it is not explicitly regulated on how a breach of privacy will be sanctioned. However, any person whose rights are violated in relation to the use of personal data may file a claim for any damages or loss arising from the unauthorized use of personal data based on EIT Law. 5. Public Information Disclosure Law Pursuant to Article 17 of to Public Information Disclosure Law, there is some information that is exempted from public information category, including confidential personal data. Any violation shall be subject to 2 (two)-year imprisonment and/or charged with a maximum fine of Rp. 10,000,000.00 (ten million Rupiah).

How is electronic marketing regulated?	**There is no specific regulation on electronic marketing. However, the recipient must grant consent to any marketing method. The contents of the electronic marketing material are subject to the Consumer Protection Law.** Article 9 of EIT Law provides that any product marketing through an electronic system must provide complete and true information in relation to the contracts, the producers, and the offered product. Article 20 of EIT Law further provides that an electronic transaction is deemed to occur when the offer has been sent by the sender and accepted by the recipient. Such acceptance must be conducted through an electronic receipt. There are also some restrictions on how a product is offered and/or marketed pursuant to Article 9 of Law No. 8 of 1999 on Consumer Protection ("**Consumer Protection Law**"). The marketing of a product must not: 1. be misleading, as if the product (i) has a specific quality, price, characteristics, history, or purpose (ii) product is in a good condition, (iii) product has obtained a specific sponsor, consent, equipment, benefit, working characteristics, or accessory, (iv) the product is manufactured by a sponsored company; (v) the product is available; (vi) the product does not have any hidden defects, (vii) the product is a part of certain products; (viii) the product is originated from a certain place; or 2. directly or indirectly discriminate other products; 3. use any hyperbolic words; 4. Offer any uncertain promises.

Are there any recent developments or expected reforms?	**The MCIT is currently preparing a draft regulation on the Data Privacy. This regulation is expected to provide protection on data privacy, to balance the development of electronic systems in Indonesia.** The draft of MCIT Regulation concerning protection on data privacy in electronic systems ("**Draft Regulation on Data Privacy**") is expected to provide integrated protection on data privacy. In this matter, in the drafting process, the MCIT takes on board the Director General of Immigration, National Archive, OJK, Bank Indonesia, Indonesian Consumer Agency Foundation, and Ministry of Health. Under the Draft Regulation on Data Privacy, the confidential nature of every personal data is determined by the data owner, unless stipulated otherwise under the laws and regulations. In general, based on the Draft Regulation on Data Privacy, protection of personal data will be provided in the process of: 1. collection of data 2. processing and analysis of data; 3. data storage; 4. data presentation, publication, transmission, dissemination, and/or access opening; and 5. destruction/deletion of personal data. The Draft Regulation on Data Privacy still emphasizes the importance of consent in the collection and utilization (including publication and dissemination) of personal data. Other notable provision under the Draft Regulation on Data Privacy is that the Electronic System provider is obliged to store the collected personal data at least 5 years, unless otherwise stipulated under each specific relevant laws and regulations.

Contact Information

Agus Ahadi Deradjat aderadjat@abnrlaw.com **Kevin Omar Sidharta** ksidharta@abnrlaw.com	**Ali Budiardjo, Nugroho, Reksodiputro** Graha CIMB Niaga, 24th Floor Jakarta Indonesia 12190 Tel 62.21.250.5125

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Japan

Prepared by Nishimura & Asahi, Lex Mundi member firm Japan

Key Legislation Overview	
What is the Key Legislation?	**The Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI) provides general minimum rules concerning the protection of personal information and defers to guidelines to be established by various ministries for the details of measures to be taken for the implementation of and compliance with the APPI.** The key legislation governing privacy in Japan is the Act on the Protection of Personal Information (Act No. 57 of 2003) (**APPI**). The APPI provides the general rules concerning the protection of personal information in the private sector and regulates the handling (acquisition, use, transfer, retention, etc.) of personal information. The APPI defers to guidelines to be established by various ministries for the details of measures to be taken for the implementation of and compliance with the APPI. Since the guidelines are not laws, they are not legally binding instruments by themselves. However, the guidelines set forth the criteria to be used by the competent ministers when enforcing the APPI, and the competent ministers consider whether an entity has implemented measures set forth in the relevant guidelines when determining whether the APPI has been violated. For example, the Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information established by the Ministry of Economy, Trade and Industry (**METI**) and the Ministry of Health, Labor and Welfare (**Economic and Industrial Sectors Guidelines**) state that noncompliance with the

	provisions of those Guidelines that contain mandatory language can be deemed a violation of the APPI by METI.
Key Data Protection Provisions	
What data is protected?	**The APPI protects Personal Information, being information about a living individual that can be used to identify the specific individual through the name, date of birth or other description contained in such information (including such information that will allow easy reference to other information and will thereby enable identification of the specific individual).** Personal Information is protected under the APPI. In addition, under the APPI, two categories of Personal Information are established: "Personal Data"; and "Retained Personal Data." These three terms are defined in the APPI as follows: • Personal Information: information about a living individual that can be used to identify the specific individual through the name, date of birth or other description contained in such information (including such information that will allow easy reference to other information and will thereby enable identification of the specific individual) • Personal Data: Personal Information contained within a Personal Information Database. A Personal Information Database is a collection of information including Personal Information as set forth below: (i) a collection of information systematically arranged in such a way that specific Personal Information can be retrieved by a computer; or (ii) any other collection of information designated by Cabinet Order as being systematically arranged in such a way that specific Personal Information can be easily retrieved. Specifically, the Cabinet Order designates any information

	systematically arranged in such a way that specific Personal Information can be easily retrieved by (a) organizing the Personal Information contained in it according to certain rules and (b) including a table of contents, an index, or other arrangements that aid retrieval. • Retained Personal Data: Personal Data for which a Business Operator Handling Personal Information has the authority to disclose, correct, add or delete content, discontinue utilization, erase, or discontinue provision to a third party, excluding (i) data specified by Cabinet Order as data the knowledge of which would be harmful to the public interest or other interests and (ii) data that will be erased within six months.
Who is subject to privacy obligations?	**The APPI's provisions apply to any "Business Operator Handling Personal Information" that has held in its database the Personal Information of more than 5,000 persons on any given day in the past six months. Operator Handling Personal Information."** The APPI applies to a "Business Operator Handling Personal Information." Under the APPI, a "Business Operator Handling Personal Information" is defined as any person using a Personal Information Database for business other than the following entities: (i) state organs; (ii) local governments; (iii) incorporated administrative agencies and the like; (iv) local independent administrative institutions; and (v) entities specified by Cabinet Order as having little likelihood of harming the rights and interests of individuals considering the volume and the manner of utilization of personal information they handle (i.e., Small Business Operators). Article 2 of the Cabinet Order defines "Small Business Operator" as an entity that has a Personal Information Database that is used for its business containing a combined total number of unique

	individuals not exceeding 5,000 on any given day in the past six months.
How is the collection of personal data regulated?	**Personal Information must not be collected by deception or other wrongful means. Generally, once a Business Operator Handling Personal Information has collected Personal Information, it must notify the individual of or publicly announce the Purpose of Use.** The following restrictions apply to the collection of Personal Information: • Proper Acquisition A Business Operator Handling Personal Information must not acquire Personal Information by deception or other wrongful means. • Notice of the Purpose of Use at the Time of Acquisition Once a Business Operator Handling Personal Information has acquired Personal Information, it must notify the individual of or publicly announce the Purpose of Use, except in cases where the Purpose of Use has already been publicly announced or where any of the following requirements is met: • where the notification or public announcement of the Purpose of Use is likely to cause harm to the life, body, or property or to any rights or interests of an individual or a third party • where the notification or public announcement of the Purpose of Use is likely to harm the rights or legitimate interests of the Business Operator Handling Personal Information

	• where cooperation with a state agency, local government or a third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and where the notification or public announcement of the Purpose of Use is likely to impede the execution of such affairs • where the Purpose of Use is evident from the situation surrounding the collection of the Personal Information The Economic and Industrial Sectors Guidelines provide the following as examples of methods of the public announcement of the Purpose of Use: announcement via the website of the business or display in an easily viewable location within a place of business.
How is the use and disclosure of personal data regulated?	**When handling Personal Information, a Business Operator Handling Personal Information must specify the Purpose of Use of Personal Information to the extent possible and must not use Personal Information beyond the scope necessary to achieve the Purpose of Use without obtaining the individual's prior consent. As a general rule, a Business Operator Handling Personal Information may not[Ed: "shall not" or "must not"] provide Personal Data to a third party without obtaining the individual's prior opt-in consent.** --- • Restriction by the Purpose of Use When handling Personal Information, in addition to specifying the Purpose of Use of Personal Information (see above), a Business Operator Handling Personal Information is required to comply with the following rules: • A Business Operator Handling Personal Information must not change the Purpose of Use beyond the scope that is reasonably related to the Purpose of Use before the change.

	• As a general rule, a Business Operator Handling Personal Information must not use Personal Information beyond the scope necessary to achieve the Purpose of Use without obtaining the individual's prior consent. Exceptions to the general rule apply in the following cases: - where the handling of Personal Information is required by laws and regulations - where the handling of Personal Information is necessary for the protection of the life, body, or property of an individual and where obtaining the person's consent is difficult - where the handling of Personal Information is necessary for the improvement of public health or promotion of the sound growth of children and where obtaining the person's consent is difficult - where cooperation with a state agency, local government or a third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and where obtaining the person's consent is likely to impede the execution of the affairs concerned • Disclosure or sharing of Personal Data with third parties As a general rule, a Business Operator Handling Personal Information may not provide Personal Data to a third party without obtaining the individual's prior opt-in consent. Exceptions to the general rule apply in the following cases: • where the handling of Personal Data is required under laws and regulations • where the handling of Personal Data is necessary for the protection of the life, body, or property of an individual and where obtaining the person's consent is difficult

	• where the handling of Personal Data is necessary for the improvement of public health or promotion of the sound growth of children and where obtaining the person's consent is difficult. • when cooperating with a state agency, local government or a third party commissioned by a state or local agency to conduct certain affairs specified by the laws and regulations and obtaining the person's consent is likely to impede the execution of the affairs concerned • Opt-out option: A Business Operator Handling Personal Information may provide Personal Data to a third party without obtaining the individual's prior consent if the Business Operator Handling Personal Information, in advance, notifies the individual of the following information or makes the information "readily available" to the individual: (i) the fact that the provision to a third party is a Purpose of Use; (ii) the items of the Personal Data to be provided to a third party; (iii) the means or method of provision to a third party; and (iv) the fact that the provision of such Personal Data as will lead to the identification of the individual to a third party will be discontinued at the request of the individual to opt out. • If the Personal Data are transferred as a result of a merger, acquisition, or similar succession transaction, the recipient of Personal Data is not deemed a "third party." • Service provider exception: If the Personal Data are transferred as a result of a commission of a third party service provider by a Business Operator Handling Personal Information for all or part of the processing of the Personal Data that is necessary to achieve the Purpose of Use, and the service provider does not

	process the data for its own Purpose of Use, such service provider is not deemed a "third party." • If a Business Operator Handling Personal Information either notifies an individual in advance of the following information, or ensures that the information is made readily available for the individual in advance, the Business Operator Handling Personal Information may use Personal Information jointly with another specific individual or entity without the individual's prior consent: i. The fact that Personal Data may be shared with and used jointly by specific individuals or entities; ii. the items of the Personal Data used jointly; iii. the scope of the joint users; iv. the purpose for which the Personal Data is used; and v. the name of the individual or business operator (from among the joint users) that is responsible for the management of the Personal Data.
How are storage, security and retention of personal data regulated?	**Business Operators Handling Personal Information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the Personal Data.** Under the APPI, Business Operators Handling Personal Information are required to take security control measures concerning Personal Data. The APPI imposes a broadly stated obligation on Business Operators Handling Personal Information to "take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the Personal Data." There are no concrete measures specified in the APPI for satisfying this requirement. However, it is generally understood that security control measures required by the APPI include: (i)

	organizational measures; (ii) employee-related measures (e.g., training of personnel); (iii) physical measures; and (iv) technical measures. Concrete actions under each type of measure are stipulated in the guidelines established by various ministries. Neither the APPI nor the guidelines set out specific time limits for the retention of Personal Data.
Are there rights of access to and correction of personal data?	**A Business Operator Handling Personal Information must make certain matters accessible to individuals whose Retained Personal Data is retained. An individual may request a Business Operator Handling Personal Information to disclose, correct or stop using, etc. relevant Personal Data in certain circumstances.** A Business Operator Handling Personal Information must comply with the following rules: • A Business Operator Handling Personal Information must make the following details accessible to individuals whose Retained Personal Data is retained: (1) the name of the Business Operator Handling Personal Information; (2) the Purpose of Use (except in specified circumstances); (3) procedures for requesting a correction to Retained Personal Data or to stop the use or sharing of, or to erase, Retained Personal Data, as well as procedures for other requests; and (4) other matters, as specified by Cabinet Order, that are necessary to ensure the proper handling of Retained Personal Data. • When an individual requests that a Business Operator Handling Personal Information disclose whether it has any Retained Personal Data that could lead to the identification of that individual (or if the individual requests notification that the Business Operator Handling Personal Information holds no such Personal Data), the Business Operator Handling Personal

	Information must disclose any relevant Personal Data without delay. • When an individual requests that a Business Operator Handling Personal Information correct, add to, or delete Retained Personal Data of the individual because they are inaccurate, the Business Operator Handling Personal Information must investigate the issue without delay. Based on the result of the investigation, the Business Operator Handling Personal Information must correct, add to, or delete the Retained Personal Data concerned. The Business Operator Handling Personal Information must notify the individual of its response to the request. • If an individual requests that a Business Operator Handling Personal Information stop using or disclosing Retained Personal Data on the basis that the Business Operator Handling Personal Information is violating certain provisions of the APPI, the Business Operator Handling Personal Information must stop using or disclosing the Retained Personal Data concerned if the request is reasonable.
Are there restrictions on cross border data transfers?	**none** None; however, please see section 13.
Are there any notification requirements for data breaches?	**A notification or other measures where a security breach has occurred are not required under the APPI; however, some guidelines require notification of the individual concerned, as well as reporting to the competent minister.** A notification or other measures where a security breach has occurred are not required under the APPI; however, some guidelines require notification of the individual concerned, as well as reporting to the competent minister. For example, the Guidelines Targeting Financial Sectors Pertaining to the

	Protection of Personal Information established by the Financial Services Agency (**FSA**) state that if a leak of personal information occurs, the Business Operators Handling Personal Information should report to the FSA immediately and promptly make a public announcement containing information such as the facts concerning the leak and measures to be taken to prevent a recurrence of the incident.
Who is the privacy regulator?	**The ministries enforce the APPI relating to the particular industries they regulate.** The ministries enforce the APPI concerning the particular industries they regulate. The majority of Japanese businesses are regulated by the Ministry of Economy, Trade and Industry (METI); the Ministry of Health, Labour and Welfare (MHLW); the Financial Services Agency (FSA); the Ministry of Internal Affairs and Communications (MIC); and the Ministry of Land, Infrastructure and Transport (MLIT)
What are the consequences of a privacy breach?	**The ministries may request reports on the handling of Personal Information, and they may issue recommendations or corrective orders. A breach of a corrective order is a criminal offense, punishable by imprisonment with work for not more than six months, or a fine of not more than 300,000 yen, or both.** Under the APPI, the ministries may request reports on the handling of Personal Information, and they may issue recommendations or corrective orders if a Business Operator Handling Personal Information breaches an individual's privacy and violates the APPI. Prior to issuing a corrective order, the ministries may take an incremental approach and instruct, advise, and make recommendations to the Business Operator Handling Personal Information. A breach of a corrective order is a

	criminal offense, punishable by imprisonment with work for not more than six months, or a fine of not more than 300,000 yen, or both (not only shall the performer be punished, but also the company shall be subject to a fine of not more than 300,000 yen). If an individual's privacy is violated due to a privacy breach, the individual may have a tort claim or breach of contract claim against the Business Operator Handling Personal Information.
How is electronic marketing regulated?	**The Act on Specified Commercial Transactions and the Act on the Regulation of Transmission of Specified Electronic Mail** **prohibit a company from transmitting e-mail as a means of advertisement without the customer's prior request or consent.** --- • The Act on Specified Commercial Transactions (Act No. 57 of 1975)(**ASCT**). Under the ASCT, in principle, a company must not provide advertisement of its sales terms by e-mail without the customer's prior request or consent. When a company provides such advertisement by e-mail with the customer's consent, the company must record and preserve the consent. The ASCT also contains rules for other forms of marketing, such as telemarketing, mail order sales, multilevel marketing, and offers for the provision of certain long-term services. • The Act on the Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002) (**Specified E-Mail Act**)

	The Specified E-Mail Act regulates the transmission of e-mail as a means of the advertisement of sales activities (**Specified E-mail**). Under this law, a company, in principle, must not transmit Specified E-mail without the customer's prior request or consent. The content of the regulation is similar to the ASCT.
Are there any recent developments or expected reforms?	**A bill to amend the APPI was passed in September 2015. The amended APPI will come into effect as of the date specified by Cabinet Order within a period not exceeding two years from the date of issue (September 9, 2015).** A bill to amend the APPI was passed in September 2015, and the Personal Information Protection Commission (**PPC**) was established on January 1, 2016. The amended APPI will come into effect as of the date specified by Cabinet Order within a period not exceeding two years from the date of issue (September 9, 2015). The amended main provisions with special reference to the above questions are as follows (however, please note that details about the provisions of the amendment will be provided by Cabinet Order or the Rules of the PPC that will be issued later (hopefully later this year)): • Question 2 "WHAT DATA IS PROTECTED?" Information, including a "Personal Identification Code," will be added to the definition of Personal Information. Personal Identification Code means a code, including characters, numerical characters and marks, that can be used to identify the specific individual and which will be specified in a Cabinet Order (e.g., biometric identifiers, such as fingerprint data or face recognition data, a passport number and license number, etc.). In addition, the amended APPI will contain provisions regarding the processing method and handling of

	"Anonymized Processed Information," which is information about an individual obtained by processing personal information so as not to identify the specific individual and not to restore such personal information pursuant to the APPI and the Rules of the PPC. • Question 3 "WHO IS SUBJECT TO PRIVACY OBLIGATIONS?" As stated in Question 3, the APPI's provisions apply to any "Business Operator Handling Personal Information" that has held in its database the Personal Information of more than 5,000 persons on any given day in the past six months. However, the amended APPI will remove this number requirement. • Question 4 "HOW IS THE COLLECTION OF PERSONAL DATA REGULATED?" A Business Operator Handling Personal Information must not obtain Sensitive Information without the individual's prior consent. (The "Sensitive Information" will be specified in the Cabinet Order.) • Question 5 "HOW ARE THE USE AND DISCLOSURE OF PERSONAL DATA REGULATED?" If a Business Operator Handling Personal Information provides Personal Data to a third party, it must prepare a record of the date the data was provided, the third party's name, and the matters specified in the Rules of the PPC pursuant to the Rules of the PPC. On the other hand, if a Business Operator Handling Personal Information receives Personal Data from a third party, it must confirm (i) the third party's name and address, the representative's name, and (ii) how the third party obtained the Personal Data, and record the date the data was provided and the matters regarding such confirmation and the matters specified by the Rules of the PPC, pursuant to the Rules of the PPC.

	• Question 8 “ARE THERE RESTRICTIONS ON CROSS-BORDER DATA TRANSFERS?“ A Business Operator Handling Personal Information must not provide Personal Data to a third party (excluding those operators with a management system conforming to the standards set forth in the Rules of the PPC) in a foreign country (excluding countries which are specified by the Rules of the PPC as those that have an equivalent system for the protection of Personal Information as the system under Japanese law) without the individual’s prior consent • Question 10 “WHO IS THE PRIVACY REGULATOR?” and Question 11 “WHAT ARE THE CONSEQUENCES OF A PRIVACY BREACH?” After the amended APPI comes into effect, the PPC will enforce the law in the private sector; and the PPC may not only request reports and issue recommendations and orders, but also conduct on-the-spot inspections.

Contact Information

Ms. Hitomi Iwase h_iwase@jurists.co.jp	**Nishimura & Asahi** Otemon Tower Tokyo Japan 100-8124 Tel 81.3.6250.6200

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Korea

Prepared by Lex Mundi member firm tbc

Key Legislation Overview	
What is the Key Legislation?	**The Personal Information Protection Act is the comprehensive general data protection law, and there exists several sector-specific laws that regulate the handling of personal data in certain industries.** In South Korea, the collection and processing of personal data is governed by the Personal Information Protection Act (PIPA), the comprehensive general data protection law. In addition, there are a number of sector-specific laws that regulate the handling of personal data in certain industries including: • Act on the Promotion of Information and Communications Network Utilization and Information Protection (Network Act); • Utilization and Protection of Credit Information Act (Credit Information Act); • Act on the Protection and Use of Location Information; and • Electronic Financial Transactions Act. Practically, because of the complexity of the rules, there are many difficulties in determining which acts will apply to a specific case. In this regard, we will focus our description on the PIPA.

Key Data Protection Provisions	
What data is protected?	**The PIPA protects personal data – i.e., information relating to a living natural person from which a specific individual can be identified.** The PIPA protects personal data. Personal data means any information relating to a living natural person (such as individual customers of a company) from which the individual can be identified through one's name, resident registration number, visual image and so on (including any information which, if not by itself, can be easily combined with other information to identify a specific individual). Also, certain information such as (i) Particular Identification Data (i.e. resident registration numbers, passport numbers, driver's licence numbers and alien registration numbers) or (ii) Sensitive Data, which refers to information which, if divulged, may considerably infringe upon the data subject's privacy (for example, bio-data or criminal records) require stronger protection.
Who is subject to privacy obligations?	**Data controllers** The PIPA applies to data controllers – i.e., a public institution, corporate body, organisation or individual that processes data directly or via another person/entity to administer personal data files(defined as "a collection of personal data in which personal data is systematically organised pursuant to certain rules for easy search/use") as part of its duties.

How is the collection of personal data regulated?	In principle, prior opt-in consent of the data subject is required
	Data controllers must obtain the data subject's prior opt-in consent in order to collect/use the data subject's personal data. Also, when seeking consent from a data subject, data controllers must inform the data subject of the following: • purposes of collection/use of personal data; • items of personal data to be collected; • duration of retention/use of personal data; and • the fact that the data subject has the right to refuse to give consent to such collection/use, and disadvantages, if any, to the data subject which may result due to such refusal. However, personal data may be collected/used without the data subject's consent in the following cases: • If the collection/use is specifically required or permissible under other applicable laws and regulations, or is necessary to comply with the data controller's obligations under other applicable laws and regulations; • If the collection/use is necessary to enter into and perform a contract with the data subject; • If there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party, and the consent to the collection/use of personal data cannot be obtained in an ordinary manner because the data subject (or his/her legal guardian) cannot express his/her intent, or his/her address is unknown; or • If the collection/use is necessary to achieve a legitimate interest of the data controller where such interest clearly overrides the rights of the data subject, provided that the collection/use will be substantially relevant to the legitimate interest of the data controller,

	and that such collection/use is performed only to a reasonable extent.
How are the use and disclosure of personal data regulated?	**In principle, prior opt-in consent of the data subject is required** Data controllers must obtain the data subject's prior opt-in consent in order to use the data subject's personal data. Also, separate consent must be obtained for transferring personal data to a third party. When seeking consent from a data subject regarding the transfer of personal data, the data controller must inform the data subject of the following: • the identity of the third party recipient of the personal data; • the third-party recipient's purpose of use of the personal data; • items of personal data to be provided to the third-party recipient; • duration of retention/use of personal data by the third-party recipient; and • the fact that the data subject has the right to refuse to give consent to the contemplated transfer, and disadvantages, if any, to the data subject which may result due to such refusal. However, personal data may be transferred without the data subject's consent in the following cases: • If the transfer is specifically required or permissible under other applicable laws and regulations, or necessary to comply with the data controller's obligations under other applicable laws and regulations; and • If there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party and the consent to the transfer of personal data cannot be obtained in an ordinary

	manner because the data subject (or his/her legal guardian) cannot express his/her intent or because his/her address is unknown.
How are storage, security and retention of personal data regulated?	**Personal data may only be stored after obtaining the data subject's consent or pursuant to a statutorily permitted purpose and data controllers are legally required to implement detailed security measures when storing personal data** The duration of the data retention period must be set out in (a) the data controller's notice for the data subject's informed consent to collection/use of personal data, and (b) the data controller's privacy policy. If the personal data are no longer necessary upon (i) the passage of the duration of retention or (ii) the achievement of the professed purposes of the processing of personal data, or for other reasons, the data controller must without delay destroy the personal data unless any other law or regulation requires it to keep them. The PIPA sets forth very specific security requirements with respect to the security of personal data. For instance, the PIPA requires data controllers to implement the following safeguards: • Establish and implement an internal administrative plan for the safe processing of personal data; • Implement measures to place restrictions on the access to personal data and the access authority; • Apply encryption technology to the personal data or take other equivalent measures to ensure the secure storage and transmission of the personal data. • Maintain access logs/records and take measures to prevent the forgery or falsification of such records, in order to be able to effectively respond to an intrusion incident.

	• Install and update security programs for the protection of personal data and implement physical measures, such as setting up separate storage facilities for storing the personal data securely or installing security locks. The implementing regulations of the PIPA (e.g., the Enforcement Decree, Official Notices, etc.) set forth such measures in greater detail.
Are there rights of access to and correction of personal data?	**Data subjects are guaranteed the right of access, the right to request rectification/erasure, and the right to request suspension of processing** The data subject is entitled to the following rights against the data controller: • Right of access - the data subject has the right to request access to his/her personal data that is being processed by the data controller; • Right to request rectification, erasure - once the data subject accesses his/her personal data, the data subject has the right to request rectification or erasure of his/her personal data; and • Right to request suspension of processing - the data subject has the right to request suspension of the processing of his/her personal data.
Are there restrictions on cross border data transfers?	**The consent of data subject may be required** The PIPA regulates cross-border transfers of personal data involving the transfer of personal data to third parties located overseas, so a data controller is still bound by the general regulations on the provision of personal data to third parties. However, the outsourcing of processing of personal data to an outsourced processor located overseas is treated in the same way as a domestic outsourcing.

	However, in cases where the Network Act applies, the consent of the data subject might still be required for the transfer of personal data across national borders for the purpose of outsourcing the processing of personal data.
Are there any notification requirements for data breaches?	**In the event of a data security breach, the data controller must notify the relevant data subjects and report the breach to the competent regulatory authority.** The data controller must notify data subjects of the following without delay: • The items of personal data that were the subject of the breach; • The time of the breach and the reasons for the breach; • Information concerning measures that can be taken by the data subject to minimize damages resulting from the breach; • Countermeasures taken by the data controller and procedures for providing redress to the data subject; and • Contact information of its pertinent department for reporting damages incurred by the data subject. Also, whenever there is a data breach involving the personal data of 10,000 or more data subjects, the data controller must (1) report to the competent regulatory authority without delay (i) the fact that it informed its data subjects of the breach, and (ii) the measures it took to minimise damages to the data subjects, and (2) disclose certain statutorily-prescribed information on its internet homepage for at least 7 days.

Who is the privacy regulator?	**The Ministry of Interior is the government agency responsible for enforcing the PIPA** As explained above in our response to Question 1, South Korea's data protection laws are divided into one general comprehensive law (i.e., the PIPA) and several sector-specific laws. Each of these sector-specific laws is enforced by a different regulatory agency. In the case of the PIPA, the Ministry of the Interior is the government agency responsible for its enforcement.
What are the consequences of a privacy breach?	**Criminal, administrative penalties and/or civil liabilities** The PIPA sets forth detailed penalties for each type of violation. A data controller that commits a material violation of the PIPA may be subject to imprisonment of up to ten years or a fine of up to KRW 100 million and a penalty surcharge of up to 3% of the revenue generated from the data controller's relevant service(s). For other minor violations, the data controller may simply be ordered to take corrective measures or be subject to an administrative fine of up to KRW 50 million. Data subjects who suffer damages from the data breach are entitled to seek compensation from the data controller.
How is electronic marketing regulated?	**In principle, the consent of recipient is required.** In general, electronic marketing is regulated by the Network Act. Under the Network Act, in principle, direct marketing (i.e., the transmission of for-profit advertisements) is only allowed if the recipient's explicit consent was obtained in advance. (Only a few limited exceptions are recognised.)

	Additionally, the Network Act provides for certain information that must be included in the for-profit advertisements (e.g., the name and contact details of the sender), and specifies certain acts that the sender is prohibited from engaging in (e.g., finding methods to prevent the recipient's refusal to receive marketing communications).
Are there any recent developments or expected reforms?	**Regulatory guidelines on de-identification measures and proposed amendments to the Network Act were announced recently** Korean data protection laws and regulations have been undergoing frequent changes as of late. Among these changes, the most notable one is the recent announcement of the "Guidelines on De-identification Measures" ("Guidelines") and the "Comprehensive Guide to Data Protection Laws and Regulation" ("Comprehensive Guide") on June 30, 2016. The Guidelines and the Comprehensive Guide specify the criteria for determining what qualifies as personal data, thereby reducing the ambiguity associated with the concept of personal data and also prescribe the specific de-identification measures necessary to transfer personal data without having to resort to legally required consent under the PIPA and other sector-specific data protection requirements. Another notable change is the proposed amendments to the Network Act announced on September 23, 2016. Once the National Assembly approves this proposed amendment and the relevant provisions take effect, the implementing regulations of the Network Act are expected to be relaxed significantly.

Contact Information

Kwang Bae Park kwangbae.park@leeko.com **Sunghee Chae** sunghee.chae@leeko.com	**Lee & Ko** 63 Namdaemun-ro, Jung-gu Seoul, South Korea Tel +82 2-772-4000

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Macau

Prepared by MdME l Lawyers l Private Notary, Lex Mundi member firm for Macau

Key Legislation Overview	
What is the Key Legislation?	**Law No. 8/2005 (the "Data Protection Law"), which sets the legal regime for collecting, processing and transferring personal data.** This piece of legislation provides for regulation in respect of the collection, treatment and transfer of personal data. It advances the basic definitions in respect of personal data and establishes requirements and sanctions in respect of data privacy and protection issues.
Key Data Protection Provisions	
What data is protected?	**Personal Data, being information about an identifiable individual.** The data protected by the Data Protection Law is "personal data" which is is defined as "any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person". Information considered as sensitive, such as health, sexual, political and genetic information is subject to particular protection in terms of requirement for treatment and safety.

Who is subject to privacy obligations?	**Any individual or collective persons wishing to collect, treat and/or transfer personal data** These subjects are divided into the more specific categories of: Controller: The individual or collective person which "alone or jointly with others determines the purposes and means of the processing of personal data". Processor: The individual or collective person "which processes personal data on behalf of the controller". Third party: The individual or collective person "other than the data subject, the controller, the processor and the persons under the direct authority of the controller or the processor, which are qualified to process the data".
How is the collection of personal data regulated?	**Generally, personal information must be collected from the individual concerned and must only be collected for a lawful purpose connected with a function or activity of the person/ entity collecting/ treating the personal data. The individual must be made aware of certain matters before collection.** Under the Data Protection Law, namely Article 6, collection and treatment of personal data is only admissible if its data holder provides his unambiguous consent to said treatment of if the processing of personal data is required for: a) for the performance of a contract or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate; b) for compliance with a legal obligation to which the controller is subject;

	c) in order to protect the vital interests of the data subject if the latter is physically or legally incapable of giving his consent; d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or e) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject. As a general rule, the collection, treatment and transfer of personal data is subject to the issuance of a notice to the MDPO whereby the entity proposing to carry out these activities declares its intention to collect, treat and/or transfer personal data, within 8 days after the commencement of treatment of personal data (Article 21). Moreover, certain types of data collection and treatment (e.g. sensitive data for the purposes of Article 7 or combination of data for the purposes of Article 9) are subject to prior authorization by the MDPO, in accordance with Article 22 of the Data Protection Law. However, there are certain cases where due to the recurrence and necessity of treatment of certain personal data, the legal requirements of notification to the MDPO are waived. Among these cases, we would note the following exemptions: a. Authorization No. 01/2007, dated 30 November, 2007, which creates an exemption of obligation of notification for "Data Processing Relating to Remunerations, Payments and Welfare Benefits";

	b. Authorization No. 02/2007, dated 30 November, 2007, which creates an exemption of obligation of notification for "Data Processing Relating to Administration of Employees and Service Providers"; c. Authorization No. 01/2008, dated February 22, 2008, which creates an exemption of the obligation of notification for “Personal Data Processing Relating to Billing and Contact Information of Clients, Suppliers and Service Providers”; d. Authorization No. 01/2011, dated November 7, 2011, which creates an exemption of the obligation of notification for the “Processing of Recruitment Data”; and e. Authorization No. 01/2013, dated April 19, 2011, which creates a simplification of the obligation of notification for the “Processing of Personal Data by Video Surveillance System for Security Purposes”.
How are the use and disclosure of personal data regulated?	**Subject to specific exceptions, persons/entities covered by these provisions may only use or disclose personal information for the purpose for which it was collected.** Controllers and persons who obtain knowledge of the personal data processed in carrying out their functions are bound by professional secrecy, even after their functions have ended. However, this duty does not exclude the duty to supply mandatory information according to the law, except when it is contained in filing systems organized for statistical purposes.

	Moreover, personal data may be disclosed to third parties in cases of explicit consent of data subjects or where the personal data: 1) is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; 2) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party; 3) is necessary or legally required on important public interest grounds, or for the establishment, exercise of defiance of legal claims; 4) is necessary in order to protect the vital interests of the data subject; 5) is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.
How are storage, security and retention of personal data regulated?	**Personal information must be protected from unauthorised loss, use, modification or disclosure with reasonable security safeguards. persons/entities covered by these provisions must not keep personal information for longer than is required** According to Article 15 of the Data Protection Law, entities collecting and processing personal data are required to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration,

	unauthorized disclosure or access, thus ensuring appropriate levels of security and protection of the processed data. Moreover, where sensitive data is treated, the Data Protection Law requires that special measures be taken to: 1) prevent unauthorized persons from entering the premises used for processing such data (control of entry to the premises); 2) prevent data media from being read, copied, altered or removed by unauthorized persons (control of data media); 3) prevent unauthorized input and unauthorized obtaining of knowledge, alteration or elimination of personal data input (control of input); 4) prevent automatic data processing systems from being used by unauthorized persons by means of data transmission premises (control of use); 5) guarantee that authorized persons may only access data covered by the authorization (control of access); 6) guarantee the checking of the bodies to whom personal data may be transmitted by means of data transmission premises (control of transmission); 7) guarantee that it is possible to check a posteriori , in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are input, when and by whom (control of input); 8) in transmitting personal data and in transporting the respective media, prevent unauthorized reading, copying, alteration or elimination of data (control of transport).

Are there rights of access to and correction of personal data?	**An individual is entitled to have access to any personal information about them held by persons/entities covered by these provisions. An individual may request correction/ amendment/ reply of personal information.** Articles 10 to 14 of the Data Protection Law set out the rights of the data holder, which must be ensured by the entity collecting and treating personal data in Macau, namely: a) Right to Information (Article 10): holders of personal data are entitled to receiving a number of information regarding the data they provide , namely: i. The identity of the entity collecting and treating the data and of his representative, if any; ii. The purposes of the processing; iii. Other information such as: 1) The recipients or categories of recipients; 2) Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply; 3) The existence and conditions of the right of access and the right to rectify. b) Right of Access (Article 11): Data holders are entitled (i) without constraints; (ii) at reasonable intervals and (iii) without excessive delay or expense incurred to: i. Confirmation as to whether or not data relating to them are being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;

	ii. Communication in an intelligible form of the data undergoing processing and of any available information as to their source; iii. Knowledge of the reason involved in any automatic processing of data concerning them; iv. The rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Act, in particular because of the incomplete or inaccurate nature of the data; v. Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with iv. above, in which case the third parties are required to rectify, erase or block the data accordingly, unless this proves impossible, or would involve a disproportionate effort. f) Right of Objection (Article 12): Data holders have the right to object at any time (based on legitimate reasons) to the processing of part or all of their data. g) Right not to be subjected to automated individual decisions (Article 13): not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, in particular his performance at work, creditworthiness, reliability or conduct. h) Right to indemnification (Article 14): If an illicit treatment of personal data causes damages to the

	data holder, he shall be entitled to reparation for the damages sustained.
Are there restrictions on cross border data transfers?	**Persons/entities covered by these provisions wishing to transfer personal information out of Macau must still comply with certain information privacy principles.** Persons/entities covered by these provisions wishing to transfer personal information out of Macau must still comply with certain information privacy principles.
Are there any notification requirements for data breaches?	**There are no mandatory reporting requirements for data breaches** There are no mandatory reporting requirements for data breaches
Who is the privacy regulator?	**The Macau Data Privacy Office (the "MDPO")** The public regulatory entity charged with monitoring and enforcing the compliance with the provisions of the Data Protection Law is the Macau Data Protection Office, created under the Chief Executive's Dispatch No. 83/2007. The MDPO is charged with, inter alia, with: • Promoting data privacy; • Creating codes of conduct; • Enforcing the provisions of the Data Protection Law; and • Conducting inspections and administrative procedures with a view to applying fines and sanctions under the Data Protection Law.

What are the consequences of a privacy breach?	**The Data Protection Law sets out in Articles 30 to 43 the applicable administrative and criminal sanctions applicable to infractions of the Data Protection Law.** **From an administrative perspective, these infractions may entail fines ranging from MOP$2,000.00 to MOP$200,000.00, depending on the nature of the infractions.** **Moreover, conducts such as intentionally omitting the requests for authorization required under the Data Protection Law, may result in prison sentences of up to 2 years or a fine of up to 240 days (a day is equivalent to an amount between MOP$50.00 and MOP$5,000.00, determined on a case to case basis by the Courts in view of the defendant's economic situation).** **Moreover, the Data Protection Law sets out additional penalties such as (i) temporary prohibition of collection of treatment of personal data; (ii) order to partially or fully erase the unduly collected data; (iii) publication of the judgment against the infringing entity in the Macau newspapers and/or (iv) public warning or censure of the infringing entity.** --- The Data Protection Law sets out in Articles 30 to 43 the applicable administrative and criminal sanctions applicable to infractions of the Data Protection Law. From an administrative perspective, these infractions may entail fines ranging from MOP$2,000.00 to MOP$200,000.00, depending on the nature of the infractions. Moreover, conducts such as intentionally omitting the requests for authorization required under the Data Protection Law, may result in prison sentences of up to 2 years or a fine of up to 240 days (a day is equivalent to an amount between MOP$50.00 and MOP$5,000.00, determined on a case to

	case basis by the Courts in view of the defendant's economic situation). Moreover, the Data Protection Law sets out additional penalties such as (i) temporary prohibition of collection of treatment of personal data; (ii) order to partially or fully erase the unduly collected data; (iii) publication of the judgment against the infringing entity in the Macau newspapers and/or (iv) public warning or censure of the infringing entity.
How is electronic marketing regulated?	**No specific regulation at this stage, direct marketing is subject to specific restrictions** There are no specific regulations on electronic marketing from a data privacy perspective. However, data subjects are entitled to (i) object to processing of data for the purposes of direct marketing or market research and (ii) to be informed of data is disclosed to third parties for said purposes, prior to disclosure.
Are there any recent developments or expected reforms?	**Changes in MDPO framework; envisaged changes to Data Protection Law** It is envisaged that the MDPO will be converted into a more comprehensive entity, with expanded powers of supervision and enforcement. The Data Protection Law is slated to be revised to address challenges of the digital age, safe harbor issues, etc. However, the director of the MDPO has stated that these changes are not likely to take place until next year (2017).

Contact Information

Jose Leitao jleitao@mdme.com.mo	**MdME l Lawyers l Private Notary** Avenida da Praia Grande, 409 Macau Macau Tel 853.2833.3332

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Malaysia

Prepared by Skrine, Lex Mundi member firm for Malaysia

Key Legislation Overview	
What is the Key Legislation?	**The Personal Data Protection Act 2010 governs the processing of personal data in respect of commercial transactions. The Act contains principles on consent, notice, disclosure, security, data retention, data integrity and access.** The key legislation governing data protection in Malaysia is The Personal Data Protection Act 2010 (PDPA). The PDPA came into force on 15 November 2013 and it sets out 7 key principles in the processing of personal data by a data user. Five further pieces of subsidiary legislation have been enacted pursuant to the PDPA to further facilitate the enforcement of the PDPA. Recently, the Personal Data Protection Standard 2015 ("**PDP Standards**") was issued by the PDP Commissioner. The PDP Standards spell out three main standards namely: Security Standards, Retention Standards and Data Integrity Standards which have application to both personal data which are processed both electronically and non-electronically.
Key Data Protection Provisions	
What data is protected?	**Personal data protects information in respect of a commercial transaction from which an individual is identified or identifiable.** "personal data" means any information in respect of commercial transactions, which—

	a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. Examples of what would be considered personal data includes name and contact details. “sensitive personal data” means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette. Examples of sensitive personal data would include data concerning an individual's health, political opinions, religion, as well as arrests and convictions for criminal offences.
Who is subject to privacy obligations?	**The PDPA applies to any person who processes or has control over the “processing” of any personal data. (data user)** “data user” means a person who either alone or jointly or in

	common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor. "Processing" carries wide meaning under the PDPA and means "in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including— a) the organization, adaptation or alteration of personal data; b) the retrieval, consultation or use of personal data; c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or d) the alignment, combination, correction, erasure or destruction of personal data". There is also a category referred to as "data processors" which carry the following meaning:- "data processor", in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes. A data user would be ultimately responsible for any data processors it utilises. The PDPA does not apply to personal data processed outside Malaysia unless the data is intended to be further processed in Malaysia and it also does not apply to a data user who is not established in Malaysia unless that person uses equipment in Malaysia to process personal data (save where it is only for purposes of transit).

	The Malaysian Federal and State Government are also exempt from the PDPA. Data users who fall within certain sectors are required to register with the PDP Commissioner. The sectors which have been specified are: • Communications • Banking and Financial Institutions • Insurance • Health • Tourism and Hospitalities • Transportation • Education • Direct Selling • Services, namely organisations carrying on the following businesses: legal, audit, accountancy, engineering or architecture, retail or wholesale dealing as defined under the Control Supplies Act 1961, private employment agencies. • Real Estate • Utilities
How is the collection of personal data regulated?	**The PDPA prohibits a data user from processing personal data without the consent of a data subject and the PDPA requires a data user to inform a data subject of various matters relating to the information of a data subject, which is being processed by or on behalf of that data user.** The General Principle of the PDPA prohibits a data user from processing personal data without the consent of the data subject unless it is for the following reasons: for the performance of a contract to which the data subject is a party;

	a) for the taking of steps at the request of the data subject with a view to entering into a contract; b) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract; c) in order to protect the vital interests of the data subject; d) for the administration of justice; or e) for the exercise of any functions conferred on any person by or under any law. The Notice Principle of the PDPA requires a data user to inform a data subject by written notice of the following, in both the national language (Malay) and English: a) that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject; b) the purposes for which the personal data is being or is to be collected and further processed; c) of any information available to the data user as to the source of that personal data; d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data; e) of the class of third parties to whom the data user discloses or may disclose the personal data; f) of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data; g) whether it is obligatory or voluntary for the data subject to supply the personal data; and

	h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data. Notice has to be provided as soon as practicable which means:- a) when the data subject is first asked by the data user to provide his personal data; b) when the data user first collects the personal data of the data subject; or c) in any other case, before the data user— (i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or (ii) discloses the personal data to a third party.
How are the use and disclosure of personal data regulated?	**Data user cannot disclose any personal data of a data subject for any purpose other than the purpose disclosed (and directly related purpose) and to any party other than the class of third parties to the data subject. (Disclosure Principle of the PDPA)** However, disclosure of personal data is permitted where: a) consent has been given by the data subject b) the disclosure is necessary to prevent or detect crime, or for the purpose of investigations c) the disclosure is required or authorised by law or order of the court d) the data user had acted under the belief that he has a legal right to disclose the data to another person e) the data user had acted under the reasonable belief that he would have received the consent of

	the data subject if the data subject had known of the disclosure and the circumstances of such disclosure; or f) the disclosure was justified as being in the public interests in circumstances as determined by the Minister.
How are storage, security and retention of personal data regulated?	**A data user is obligated to take specified measures to protect personal data from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction during its processing. (Security Principle) A data user must also not retain longer than is necessary of any data for the fulfilment of the purpose for which it is processed and requires the data user to destroy or permanently delete all personal data, which is no longer required for the purpose for which it was processed. (Retention Principle)** Where data is being processed, the data user themselves or the data user on behalf of the data processor must take into account the following security factors: a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction; b) the place or location where the personal data is stored; c) any security measures incorporated into any equipment in which the personal data is stored; d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and e) the measures taken for ensuring the secure transfer of the personal data.

	The PDP Standards also which provides certain measures which have to be complied with under the Security Standards. Where a “data processor” is used, the Security Standards stipulate that the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor— a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and b) takes reasonable steps to ensure compliance with those measures. The Retention Principles stipulates that personal data must not be retained longer that is necessary for the fulfilment of the purpose for which it is processed. The PDP Standards also contains the Retention Standards which specify the measures which have to be taken in terms of retention of data.
Are there rights of access to and correction of personal data?	**The Access Principle confers the right on a data subject to access his personal data and to correct the same if it is inaccurate, incomplete, misleading or outdated.** A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under the PDPA. The PDPA also grants rights to data subjects to request for access to and/or correction of personal data. The PDPA

	prescribes the procedures and there are also timelines which would have to be complied by a data user where there is an access and/or correction request. The PDPA also provides the grounds on which such data access request may be refused such as where the burden or expense of providing access is disproportionate to the risks to the data subject's privacy in relation to the personal data in the case in question or where the data user cannot comply with the data access request without disclosing personal data relating to another individual, among other factors. A data correction request may also be turned down where the data user is not supplied with such information as he may reasonably require to ascertain in what way the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date or where the data user is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date, among other factors.
Are there restrictions on cross border data transfers?	**A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette.** No permitted place/country has been specified in the Gazette at present. Notwithstanding the prohibition, a data user may transfer any personal data to a place outside of Malaysia if: a) the data subject has given his consent to the transfer; b) the transfer is necessary for the performance of a contract between the data subject and the data user;

	c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which— (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; e) the data user has reasonable grounds for believing that in all circumstances of the case— (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA; g) the transfer is necessary in order to protect the vital interests of the data subject; or h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

Are there any notification requirements for data breaches?	**There are no breach notification requirements in the PDPA**
Who is the privacy regulator?	**A "Personal Data Protection Commissioner" will be appointed by the minister to carry out the functions and the powers assigned to the Commissioner by the PDPA. There is currently a Personal Data Protection Commissioner appointed and also a Personal Data Protection Department which has been set up.** The functions of the Commissioner includes: a) to advise the Minister on the national policy for personal data protection and all other related matters; b) to implement and enforce the personal data protection laws, including the formulation of operational policies and procedures; c) to promote and encourage associations or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of the PDPA; d) to cooperate with bodies corporate or government agencies for the purpose of performing his functions; e) to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act; f) to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to their personal data;

	g) to monitor and supervise compliance with the provisions of the PDPA, including the issuance of circulars, enforcement notices or any other instruments to any person; h) to promote awareness and dissemination of information to the public about the operation of the PDPA; i) to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data; j) to represent Malaysia through participation in events that relate to personal data protection as authorized by the Minister, whether within or outside Malaysia; and k) to carry out such activities and do such things as are necessary, advantageous and proper for the administration of this Act, or such other purposes consistent with the PDPA as may be directed by the Minister.
What are the consequences of a privacy breach?	**Breaches of the provisions of the PDPA will result in a fine or imprisonment or both.** Failure to comply with the provisions in the PDPA may amount to a criminal offence: a) Breach of any of the seven data protection principles attracts a fine up to RM 300,000 and / or to two years imprisonment, or both b) Unlawful collection, disclosure and sale of personal data attracts a fine up to RM 500,000 and / or to three years imprisonment, or both If a body corporate is found to have committed an offence, the officers of such body corporate are deemed to have

	committed the offence personally. However the officer(s) of such body corporate may not be found to have committed the offence if he / they can prove the offence was committed without his / their knowledge or consent and he / they had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.
How is electronic marketing regulated?	**There are no specific rules on electronic marketing under the PDPA however the PDPA has a general provision on section on processing of personal data for direct marketing.** "Direct marketing" is defined in the PDPA as "the communication by whatever means of any advertising or marketing material which is directed to particular individuals". This would be wide enough to encompass electronic marketing. The PDP stipulates that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. Where the data subject is dissatisfied with the failure of the data user to comply with the notice, whether in whole or in part, the data subject may submit an application to the Commissioner to require the data user to comply with the notice. Where the Commissioner is satisfied that the application of the data subject is justified, the Commissioner may require the data user to take such steps for complying with the notice. A data user who fails to comply with the requirement of the Commissioner under subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding two

	hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both. There was a Proposal Paper for a Guide in Dealing with Direct Marketing which was issued by the PDP Department in 2013 which covered both conventional and electronic direct marketing, however such proposal paper has been discontinued after feedback was obtained from the relevant stakeholders.
Are there any recent developments or expected reforms?	**The PDP Standards was issued by the PDP Department in late December 2015. It is also expected that Codes of Practice for various industries will issued by the PDP Commissioner after discussions with the various sectors involved.** The PDP Standards came into force in late December 2015 and outline three main standards namely: Security Standard, Retention Standard and Data Integrity Standard which have application to personal data processed both electronically and non-electronically. The PDP Standards are stated to be “a minimum requirement” and will apply to all data users, meaning any person who processes, has control of or allows the processing of any personal data in connection with a commercial transaction. The PDPA Commissioner may designate a body as a data user forum in respect of a specific class of data users for the purposes of the PDPA and such data user forum may develop may prepare a code of practice on its own initiative; or upon request by the Commissioner. The PDP Commissioner has been in discussions with the various data user forums on the development of codes of practice for different sectors.

Contact Information

Jillian Chia jc@skrine.com	**Skrine** Unit.No. 50-8-1, 8th Floor, Wisma UOA Damansara Kuala Lumpur Malaysia 50490 Tel 60.3.2081.3999

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

New Zealand

Prepared by Simpson Grierson, Lex Mundi member firm for New Zealand

Key Legislation Overview	
What is the Key Legislation?	**The Privacy Act 1993 governs the collection, storage and security, accuracy, retention, use and disclosure of personal information. Privacy Codes apply to particularly industries, sectors or contexts.** The key legislation governing privacy in New Zealand is the Privacy Act 1993 (Privacy Act). The Privacy Act sets out twelve Information Privacy Principles (IPPs) that govern the collection, storage and security, accuracy, retention, use and disclosure of personal information. The IPPs are not intended to operate as a rigid set of rules, but rather as a set of guidelines to protect an individual's right to privacy. The Privacy Act allows the Privacy Commissioner to issue codes of practice which modify the operation of the Privacy Act in relation to particular industries, sectors or context (Privacy Codes). A Privacy Code may modify the application of any of the IPPs, for example, by prescribing standards that are more stringent, or less stringent, than the standards prescribed under the Act. A Privacy Code can be issued in respect of specified information or classes of information, specified agencies or classes of agency, an industry or profession or class of industries or professions. Currently, the following Codes of Practice are in force in New Zealand: • Civil Defence National Emergencies (Information Sharing) Code 2013; • Credit Reporting Privacy Code 2004; • Health Information Privacy Code 1994;

	• Justice Sector Unique Identifier Code 1998; • Telecommunications Information Privacy Code 2008; and • Superannuation Schemes Unique Identifier Code 1995.
Key Data Protection Provision	
What data is protected?	**The Privacy Act protects personal information, being information about an identifiable individual.** Personal information is protected by the Privacy Act. Personal information is "any information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Birth, Deaths and Marriages Registration Act 1995, or any former Act". Examples of what would be considered personal information includes information concerning an individual's health, sex, political, philosophical and religious views and affiliation, as well as arrests and convictions for criminal offences.
Who is subject to privacy obligations?	**The Privacy Act applies to public and private sector agencies.** The Privacy Act applies to "agencies", which includes public and private sector organisations. Agency is defined broadly under the Privacy Act to mean "any person or body of persons, whether corporate or unincorporated, and whether in the public sector or in the private sector; and, for the avoidance of doubt, includes a department". There are a number of exceptions to the definition of "agency" including the Governor-General, the Parliamentary

	Service Committee, Ombudsmen and any news medium in relation to its news activities.
How is the collection of personal data regulated?	**Generally, personal information must be collected from the individual concerned and must only be collected for a lawful purpose connected with a function or activity of the agency. The individual must be made aware of certain matters before collection, if it is reasonably practicable.** The Privacy Act sets out certain requirements in relation to the collection of personal data. Generally personal information should not be collected by any agency unless: • the information is collected for lawful purpose connected with a function or activity of the agency; and • the collection of the information is necessary for that purpose. Where an agency collects personal information, the information should be collected directly from the individual concerned. There are a limited number of exceptions to this rule. These exceptions include where: • the information is publicly available information; • the individual agrees that it can be collected from someone else; • non-compliance will not prejudice the interests of the individual concerned; • non-compliance is necessary for the maintenance of the law by a public sector agency, for law enforcement, protection of public revenue or for the conduct of legal proceedings before any court or tribunal; • compliance would prejudice the purpose of the collection or is not reasonably practical; or

	• the information will not be used in a form in which the individual concerned is identified or will be used for statistical or research purposes and will not be published in a form that could reasonably identify the individual. When collecting personal information strictly from the individual concerned, an agency must take reasonable steps (before collecting the information) to ensure the individual is aware of certain matters, including: • that the information is being collected; • the purpose of the collection; • the intended recipients of the information; • the name(s) and address(es) of the agency (or agencies) that is (or will) be collecting and holding the information; • if the collection of the information is authorised or required by law (and if so the particular law and whether supply of the information is voluntary or mandatory under that law); • the consequences of not providing the information; and • the rights of access to, and collection of, personal information by the individual. These steps should be taken before the information is collected if this is reasonably practicable. There are a number of exceptions to this requirement such as where non-compliance is authorised by the individual concerned, compliance would prejudice the purposes of collection, non-compliance would not prejudice the individual concerned or the information will not be used in a form in which the individual is concerned is identifiable. In addition, personal information must not be collected by unlawful means or by means that are, in the circumstances, unfair or intrude to an unreasonable extent on the personal affairs of the individual concerned.

How are the use and disclosure of personal data regulated?	**Subject to specific exceptions, an agency may only use or disclose personal information for the purpose for which it was collected.** Generally, an agency should only use personal information that it holds for the purpose for which it was obtained and the agency must not use the information for any other purpose. There are a number of exceptions to this general principle, including instances where: • the agency believes the proposed other purpose is a directly related purpose; • the source of the personal information is a publicly available information; • non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, for law enforcement, protection of public revenue, or for the conduct of any legal proceedings; • the use of the information is necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life or health of an individual; • the individual has authorised the use of the information for the other purpose; or • the information is to be used in a form in which the individual is not identified or is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned. An agency should also take reasonable care to ensure that personal information is accurate, current, complete, relevant and not misleading before the information is used. There is also a general principle against the disclosure of personal information. However, an agency may disclose personal information in certain circumstances, including where it believes, on reasonable grounds:

	• that the proposed disclosure is one of the reasons why the information was obtained, or is for a directly related purpose; • the source of the information is publicly available information; • the agency is authorised to do so by the individual concerned; • the disclosure is to the individual concerned; • that non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, for law enforcement, protection of public revenue, or for the conduct of legal proceedings; • that the disclosure is necessary to prevent or lessen a serious and imminent threat to public health or safety or the life and health of the individual concerned; • the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or • the information is to be used in a form in which the individual concerned is not identified or is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual.
How are storage, security and retention of personal data regulated?	**Personal information must be protected from unauthorised loss, use, modification or disclosure with reasonable security safeguards. Agencies must not keep personal information for longer than is required.** In terms of the storage and security of personal information an agency that holds personal information is required to ensure that: • the information is protected, by such security safeguards as is reasonable in the circumstances to take, against unauthorised loss and access, use, modification or disclosure; and

	• if it is necessary for the information to be given to a service provider to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information. The Privacy Act also requires that an agency must not keep personal information it holds for longer than is required for the purposes for which that information may be lawfully used.
Are there rights of access to and correction of personal data?	**Subject to specific grounds for withholding access, an individual is entitled to have access to any personal information about them held by an agency. An individual may request correction of personal information.** Where an agency holds personal information in a way that is readily retrievable, an individual is entitled to obtain confirmation from the agency whether or not the agency holds personal information about the individual and to have access to that information. Where access is given, the individual must also be advised that she/he may request the correction of that information. This general right of access to personal information is subject to provisions in the Privacy Act setting out grounds on which a request for access may be refused and procedural provisions relating to access to, and correction of, personal information. Good reasons for withholding access to personal information requested by an individual include reasons of national security and Government international relationships as well as the protection of trade secrets, the privacy of the affairs of other individuals, legal professional privilege and where the information is evaluative material.

	Where an agency holds personal information about an individual, the individual is to be entitled to: • request correction of the information; • request that, if a correction sought is not made, a statement of the correction sought is attached to the information.
Are there restrictions on cross border data transfers?	**Agencies transferring personal information out of New Zealand must still comply with certain information privacy principles. The transfer of personal information out of New Zealand can be prohibited in certain circumstances.** The Privacy Act does not purport to have extraterritorial effect on persons outside of New Zealand. However, where an agency subject to the Privacy Act transfers personal information outside of New Zealand, or the information is transferred outside of New Zealand on the agency's behalf, the agency is still required to comply with the Information Privacy Principles dealing with storage and security, accuracy, retention, use and disclosure. The IPPs in relation to an individual's right to access and require collection of their personal information will also apply to personal information held by an agency offshore. In addition, the Privacy Act gives the Privacy Commissioner the power to prohibit the transfer of personal information from New Zealand to another State if the Commissioner is satisfied, on reasonable grounds, that: • the information received in New Zealand from another State will likely be transferred to a third State where the information will not be subject to a law providing comparable safeguards to the Privacy Act; and • the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines Governing the

	Protection of Privacy and Transborder Flows of Personal Data.
Are there any notification requirements for data breaches?	**There are no mandatory reporting requirements for data breaches, however it is anticipated that this may form part of proposed reforms.** There are currently no requirements under the Privacy Act for mandatory data breach notification. However, the Privacy Commissioner has issued a Data Safety Toolkit which sets out voluntary guidelines on how to deal with data breaches. The Data Safety Toolkit includes guidance as to matters to consider in assessing whether notification of the breach should be given to the individuals affected, the Privacy Commissioner and/or any other authorities or third parties. In addition, in 2014 the Government signalled its intention to replace the Privacy Act with mandatory data breach reporting being identified as one of the matters to be introduced in the new legislation. Draft legislation has still to be released for public comment. Cabinet Social Policy Committee Reforming the Privacy Act 1993 (13 March 2014).
Who is the privacy regulator?	**The Privacy Act 1993 establishes the office of the Privacy Commissioner. The functions of the Privacy Commissioner range from promoting privacy to investigating complaints of interference with privacy.** The Privacy Commissioner has a range of functions under the Privacy Act in relation to the promotion of privacy. These functions include undertaking compliance audits at the request of an agency, undertaking educational programmes, providing advice on matters relating to the operation of the

	Privacy Act and reporting to the Prime Minister on matters relating to privacy. The Privacy Act also gives the Privacy Commissioner the power to issue codes of practice that may modify the application of any one or more information privacy principles in respect of certain personal information (or classes of personal information, agencies, activities or industries or professions. The current privacy codes in effect are: • Civil Defence National Emergencies (Information Sharing) Code 2013; • Credit Reporting Privacy Code 2004; • Health Information Privacy Code 1994; • Justice Sector Unique Identifier Code 1998; • Telecommunications Information Privacy Code 2008; and • Superannuation Schemes Unique Identifier Code 1995. If a person believes there has been a breach of any information privacy principle or code of practice in respect of a person, and that person has suffered (or may suffer) loss, detriment, damage or injury, a complaint may be made to the Privacy Commissioner. The Privacy Commissioner's functions are then to investigate the completing, act as a conciliator or refer the matter on to either an ombudsman or other official if the Privacy Commissioner considers the complaint is more appropriately addressed under the jurisdiction of that other official. The Privacy Commissioner does have the discretion to take no action in relation to a complaint.

What are the consequences of a privacy breach?	**A failure to comply with the information privacy principles may be an actionable interference with privacy if harm is caused to the individual. The Privacy Commissioner has the power to investigate interferences with privacy but cannot make binding decisions. Complaints may be referred to the Human Rights Review Tribunal which has jurisdiction to order a range of remedies, including awarding damages of up to NZD200,000.** A failure to comply with any of the requirements of the IPPs may be an interference with the privacy of the individual concerned and could be the subject of a Privacy Act complaint made to the Privacy Commissioner if harm is caused. The Privacy Commissioner may investigate complaints and endeavour to secure settlements between the parties to a complaint. If a settlement is not reached, the matter may become subject to civil proceedings before the Human Rights Review Tribunal (HRRT). The proceedings could be issued by the Director of Human Rights Proceedings or by the aggrieved individual. The Privacy Commissioner may also refer a complaint to an Ombudsman, the Health and Disability Commissioner, the Inspector General of Intelligence and Security or to an overseas privacy enforcement authority if the Privacy Commissioner determines that such persons or authority should deal with the complaint. Where Privacy Commissioner is unable to secure a settlement for claim of interference with privacy, the matter could become the subject of proceedings before the HRRT. The remedies, if a breach of privacy is found by the HRRT, can include one or more of the following: • a declaration; • an order restraining the defendant from continuing or repeating the interference;

	• damages; • an order requiring the defendant to perform specified acts with a view to remedy the interference, or redressing any loss or damage suffered by the aggrieved individual; or • such other relief as the HRRT thinks fit. The HRRT has jurisdiction to make awards of up to $200,000. The Privacy Commissioner also has a policy pursuant to which the Privacy Commissioner's Office may name agencies who have breached the Privacy Act in public reports in appropriate cases. Agencies may be named where, on balance, the Privacy Commissioner considers that the agency ought to be named for the purpose of giving effect to the Privacy Act. Civil rights of action may also be available if there is a privacy breach, for example, claims for breach of confidence, breach of privacy or intrusion in the right to seclusion. An action is an interference with the privacy of an individual if: a) in relation to that individual: i. the action breaches an IPP; or ii. the action breaches a code of practice; or iii. the action breaches an IPP or code of practice as modified by an Order in Council; or iv. the provisions of an information sharing agreement approved by an Order in Council have not been complied with; or v. the provisions of Part 10 (information matching) have not been complied with; and b) the Privacy Commissioner is satisfied that the action:

	i. caused, or may cause loss, detriment, damage, or injury to that individual; or ii. has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations, or interests of that individual; or iii. has resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that individual.
How is electronic marketing regulated?	**Unsolicited commercial electronic messages are prohibited under the Unsolicited Electronic Messages Act 2007 (Anti-Spam Act).** Unsolicited commercial electronic messages are prohibited under the Unsolicited Electronic Messages Act 2007 (Anti-Spam Act).
Are there any recent developments or expected reforms?	**The Government has signalled an intent to repeal and replace the existing privacy regime.** Following recommendations arising from the 2011 Law Commission review into the Privacy Act, the Government has signalled its intent to repeal and replace New Zealand's existing privacy law regime in 2014. A draft Privacy bill has still to be released for public consideration but indications are that reforms will address matters such as: • mandatory breach notification; • the issue of compliance notices for Privacy Act breaches; • strengthened own motion investigations by the Privacy Commissioner and increased fines; • specific requirements in relation to cross-border outsourcing, disclosures and enforcement co-operation; and • streamlining the complaints procedure.

Contact Information

Karen Ngan Karen.Ngan@simpsongrierson.com **Jania Baigent** Jania.Baigent@simpsongrierson.com	**Simpson Grierson** Lumley Centre, 88 Shortland Street Auckland New Zealand 1141 Tel 64.9.358.2222

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Philippines

Prepared by Romulo Mabanta Buenaventura Sayoc & de los Angeles, Lex Mundi member firm for Philippines

Key Legislation Overview	
What is the Key Legislation?	**The Data Privacy Act of 2012 governs the processing of Personal Information and Sensitive Personal Information. Processing includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.** The Data Privacy Act protects Personal Information and Sensitive Personal Information from which the identity of an individual is apparent or can be reasonably and directly ascertained.
Key Data Protection Provisions	
What data is protected?	**The Data Privacy Act protects Personal Information and Sensitive Personal Information from which the identity of an individual is apparent or can be reasonably and directly ascertained.** The Data Privacy Act protects Personal Information and Sensitive Personal Information. Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. Sensitive personal information refers to personal information:

	• About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; • About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; • Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and • Specifically established by an executive order or an act of Congress to be kept classified.
Who is subject to privacy obligations?	**The Data Privacy Act applies to any natural and juridical person involved in personal information processing.** The Data Privacy Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.

How is the collection of personal data regulated?	**Generally, personal information must be collected from the individual who has given their consent. [Sec. 12(a)] The processing of personal information is allowed if collected for specified and legitimate purposes and processed fairly and lawfully.** The Data Privacy Act states that personal information must, be: • Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only; • Processed fairly and lawfully; • Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted; • Adequate and not excessive in relation to the purposes for which they are collected and processed; • Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and • Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, that personal information collected for other purposes may be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

	The personal information controller must ensure implementation of personal information processing principles set out herein. Moreover, the processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: • The data subject has given his or her consent; • The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract; • The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; • The processing is necessary to protect vitally important interests of the data subject, including life and health; • The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or • The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. Furthermore, the processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: • The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case

	of privileged information, all parties to the exchange have given their consent prior to processing; • The processing of the same is provided for by existing laws and regulations: Provided, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; • The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing; • The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, that such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing; • The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or • The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

How are the use and disclosure of personal data regulated?	**Subject to specific exceptions, the use and disclosure of personal data is permitted for the purpose for which it was collected. Such as, when necessary to the fulfilment of a contract, for compliance with a legal obligation, to protect vitally important interests of the data subject, to comply with the requirements of public order and safety.** Please refer to the discussion in Question number 4 for the regulation of the use of personal information and sensitive personal information. Generally, personal information and sensitive personal information cannot be disclosed without the consent of the data subject or without being authorized by the Data Privacy Act or any existing law. However, the following are not included in the scope of the Data Privacy Act: • Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including: 1. The fact that the individual is or was an officer or employee of the government institution; 2. The title, business address and office telephone number of the individual; 3. The classification, salary range and responsibilities of the position held by the individual; and 4. The name of the individual on a document prepared by the individual in the course of employment with the government; • Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

	• Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit; • Personal information processed for journalistic, artistic, literary or research purposes; • Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions; • Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with the Anti-Money Laundering Act and other applicable laws; and • Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.
How are storage, security and retention of personal data regulated?	**The personal information must be protected against any accidental or unlawful destruction, alteration and disclosure, accidental loss or destruction, as well as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.** For the security of the storage of personal information, the personal information controller must observe the following: • Implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and

	disclosure, as well as against any other unlawful processing. • Implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. • Further ensure that third parties processing personal information on its behalf shall implement the security measures required by the Data Privacy Act. Also, in determining the appropriate level of security, the following factors should be considered: the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. The security measures to be implemented must include the following, which are subject to guidelines that the National Privacy Commission may issue: • Safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability; • A security policy with respect to the processing of personal information; • A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach, and • Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

	Moreover, the employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information is not intended for public disclosure. This obligation shall continue even after leaving the public service, the transfer to another position, or upon termination of their employment or contractual relation.
Are there rights of access to and correction of personal data?	**The rights of the data subject, among others, include reasonable access to contents of his or her personal information and to correct it immediately and accordingly if there is dispute in the accuracy.** The Data Privacy Act provides that the data subject is entitled to: • Be informed whether personal information pertaining to him or her shall be, are being or have been processed; • Be furnished with the information before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity. The data subject is also allowed reasonable access to, upon demand, the following: • Contents of his or her personal information that were processed; • Sources from which personal information were obtained; • Names and addresses of recipients of the personal information; • Manner by which such data were processed; • Reasons for the disclosure of the personal information to recipients;

	• Information on automated processes where the data will or likely be made as the sole basis for any decision significantly affecting or will affect the data subject; • Date when his or her personal information concerning the data subject were last accessed and modified; and • The designation, or name or identity and address of the personal information controller; The data subject may dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, that the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject. In addition, the data subject may suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information.
Are there restrictions on cross border data transfers?	**The Data Privacy Act applies to those entities engaged in and outside of the Philippines if the processing relates to personal information about a Philippine citizen or a resident, even if the processing is done outside of the Philippines as long as it is about Philippine citizens or**

	residents. The Data Privacy Act applies to an act done or practice engaged in and outside of the Philippines by an entity if the act, practice or processing relates to personal information about a Philippine citizen or a resident. Moreover, the Data Privacy Act applies if the entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: • A contract is entered in the Philippines; • A juridical entity unincorporated in the Philippines but has central management and control in the country; and • An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and Also, the Data Privacy Act applies if the entity has other links in the Philippines such as, but not limited to: • The entity carries on business in the Philippines; and • The personal information was collected or held by an entity in the Philippines.
Are there any notification requirements for data breaches?	**The personal information controller must notify the Commission and affected data subjects when there is a breach in processing sensitive personal information or other information believed to have been acquired by an unauthorized person.** The Data Privacy Act states that the personal information controller shall promptly notify the Commission and the affected data subjects when it has reasonable belief that

	sensitive personal information or other information has been acquired by an unauthorised person, and that: • Such personal information may, under the circumstances, be used to enable identity fraud, and • The Personal Information Controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with the provisions of the Data Privacy Act and the existence of good faith in the acquisition of personal information. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Who is the privacy regulator?	**The Data Privacy Act created an independent body known as the National Privacy Commission. The Commission is tasked to administer and implement the provisions of the Data Privacy Act, and to monitor and ensure compliance of the country with international standards set for data protection.** The National Privacy Commission is tasked to administer and implement the provisions of the Data Privacy Act, and to monitor and ensure compliance of the country with international standards set for data protection. The Data Privacy Act also provides that the National Privacy Commission, shall have the following functions: • Ensure compliance of personal information controllers with the provisions of the Data Privacy Act; • Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report; • Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest; • Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy; • Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to the Data Privacy Act; • Coordinate with other government agencies and the private sector on efforts to formulate and implement

	plans and policies to strengthen the protection of personal information in the country; • Publish on a regular basis a guide to all laws relating to data protection; • Publish a compilation of agency system of records and notices, including index and other finding aids; • Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of the Data Privacy Act; • Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers; • Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person; • Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of the Data Privacy Act and other data privacy laws; • Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary; • Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection; • Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws; • Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and • In general, perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

What are the consequences of a privacy breach?	**Depending on the breach committed, the offender may suffer a penalty of imprisonment ranging from six months to six years and a fine of Php 100,000 up to 5,000,000.** The Department of Justice, upon recommendation of the National Privacy Commission, shall prosecute violations of the Data Privacy Act which are punishable with criminal sanctions. The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty: • The unauthorized processing of personal information or sensitive personal information: 1. without the consent of the data subject or without being authorised by the Data Privacy Act or any existing law, or 2. for purposes not authorised by the data subject or otherwise authorised under the Data Privacy Act or under existing laws • Accessing or providing access to personal information or sensitive personal information due to negligence and without being authorised under the Data Privacy Act or any existing law • Knowingly or negligently disposing, discarding or abandoning the personal information or sensitive personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection • Processing personal information or sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Data Privacy Act or under existing laws. • Knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in

	any way into any system where personal and sensitive personal information is stored. • Concealment of security breaches involving sensitive personal information after having knowledge of the security breach and of the obligation to notify the National Privacy Commission pursuant to Section 20(f) of the Data Privacy Act. • Disclosing personal information or sensitive personal information without the consent of the data subject and without malice or bad faith by any personal information controller or personal information processor or any of its officials, employees or agents, to a third party. • Disclosing, with malice or in bad faith, of unwarranted or false information relative to any personal information or personal sensitive information obtained by any personal information controller or personal information processor or any of its officials, employees or agents. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under the Data Privacy Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of the Data Privacy Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

How is electronic marketing regulated?	**The Implementing Rules of the Electronic Commerce Act of 2000 ensures the protection of users, in particular with regard to privacy, confidentiality, anonymity and content control.** The Implementing Rules of the Electronic Commerce Act of 2000 ensures the protection of users, in particular with regard to privacy, confidentiality, anonymity and content control. The Electronic Commerce Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic documents related to such activities and to promote the universal use of electronic transactions in the government and by the general public. Electronic Commerce Act shall apply to any kind of electronic data message and electronic document used in the context of commercial and non-commercial activities to include domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information.
Are there any recent developments or expected reforms?	**The Data Privacy Act remains to largely unenforced due to the lack of specific implementing rules and regulations.** The Data Privacy Act specifically placed the National Privacy Commission (NPC) as an attached unit under the Department of Information and Communications (DICT); however, since the DICT has yet to be created, the NPC necessarily fell under the jurisdiction of the Office of the President (OP). The OP has not appointed all the members

	of the NPC, and to date, no draft rules and regulations to implement the law has been issued.

Contact Information

Herminio Ozaeta Herminio.Ozaeta@Romulo.com	**Romulo Mabanta Buenaventura Sayoc & de los Angeles** 21st Floor, Philamlife Tower Makati City Philippines 1226 Tel 632.555.9555

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Singapore

Prepared by Rajah & Tann Singapore LLP, Lex Mundi member firm for Singapore

Key Legislation Overview	
What is the Key Legislation?	**Personal Data Protection Act 2012 ("PDPA").** The PDPA regulates the collection, use, disclosure and processing of personal data in Singapore. The PDPA also provides for the establishment of a Do-Not-Call ("**DNC**") Registry, which allows individuals to opt out of marketing messages that are sent by way of voice calls, text messages or fax messages, by registering their Singapore telephone numbers in the three (3) DNC registries (for voice calls, texts and faxes) (the "**DNC Provisions**"). The DNC Provisions would need to be strictly complied with as a breach is a criminal offence. The Personal Data Protection Commission ("**PDPC**") was established to administer and enforce the PDPA. There are various subsidiary legislation such as the Personal Data Protection Regulations 2014. The PDPC has also issued several guidelines to provide guidance on the PDPA, although these do not have the force of law and will not bind the PDPC in its administration and enforcement of the PDPA.
Key Data Protection Provisions	

What data is protected?	**Any data that identifies or potentially identifies an individual (whether living or deceased)** The PDPA regulates the processing of personal data. "personal data" is defined as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.
Who is subject to privacy obligations?	**All organizations (includes individuals, companies, associations or body of persons) regardless of size** The data privacy obligations are imposed on any "organization", which is broadly defined under the PDPA to include any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore. This definition means that the PDPA has significant extraterritorial effect.
How is the collection of personal data regulated?	**Personal data of an individual cannot be collected and processed for any purpose unless at or prior to collection, the organisation notifies the individual of the purposes for which the personal data is collected, and obtains consent from the individual.** Generally, an organisation will be prohibited from collecting an individual's personal data, unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. Such consent must be 'valid' and the PDPA sets out additional obligations that

	organisations must comply with when obtaining consent, for example, prohibiting organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices. There is a limited list of exceptions for when an organisation may collect personal data about an individual without the consent of the individual. Further, the personal data must only be collected for purposes that a reasonable person would consider appropriate in the circumstances.
How are the use and disclosure of personal data regulated?	**Personal data of an individual cannot be used or disclosed for any purpose unless the organisation had notified the individual of the purposes for which the personal data will be used or disclosed, and obtained consent from the individual.** Generally, an organisation will be prohibited from using or disclosing an individual's personal data, unless the individual gives, or is deemed to have given, his consent for the use or disclosure of his personal data. Such consent must be 'valid' and the PDPA sets out additional obligations that organisations must comply with when obtaining consent, for example, prohibiting organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices. There is a limited list of exceptions for when an organisation may use or disclose personal data about an individual without the consent of the individual. Further, the personal data must only be used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances.

How are storage, security and retention of personal data regulated?	**Personal data must be protected from unauthorised access, collection, use, disclosure, etc. through security arrangements that are reasonable and appropriate in the circumstances.** **Organisations must not retain personal data where the purpose of collection is no longer relevant and there is no legal or business purpose to retain the same.** In terms of storage and security, the PDPA requires an organisation to put in place reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. In terms of retention of personal data, the PDPA requires an organisation to destroy or anonymise personal data when the purpose for which that personal data was collected is no longer relevant and retention is no longer necessary for legal or business purpose.
Are there rights of access to and correction of personal data?	**An individual has the right to request access and correction to his personal data.** Upon request by an individual, an organisation must provide the individual within a specified time, with: a) personal data about the individual that is in the possession or under the control of the organisation; and b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

	There is a limited list of exceptions to the abovementioned access right. Upon a request for correction of personal data by an individual, an organization will be required to: a) correct the personal data within a specified time; and b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. There is a limited list of exceptions to the abovementioned access right.
Are there restrictions on cross border data transfers?	**An organisation is prohibited from transferring personal data of any individual out of Singapore unless certain conditions are met.** An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. The transferor must ensure that the recipient of the personal data in the country outside Singapore is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.
Are there any notification requirements for data breaches?	**No** There is no mandatory notification requirement for data breaches under the PDPA.

	However, the PDPC encourages notification. Further, it may be viewed as a point of mitigation.
Who is the privacy regulator?	**The Personal Data Protection Commission** The PDPA confers various powers on the Personal Data Protection Commission (PDPC), including powers of investigation, power to issue directions and penalties to non-compliant organisations, as well as the power to review an organisation's reply to a request made by an individual under the access and correction principles. It is important to note that the PDPC is empowered to issue fines of up to S$ 1 million per breach of the PDPA and that it may do so of its own accord.
What are the consequences of a privacy breach?	**The PDPC may issue the breaching organisation a fine of up to S$ 1 million per breach and/or issue relevant directions.** **Some breaches may amount to a criminal offence.** **Affected individuals have statutory rights under the PDPA to commence a lawsuit against the breaching organisation.** An individual may lodge a complaint to the organisation directly, or to the PDPC, if he or she is aware of non-compliance with the PDPA. The PDPC may conduct an investigation, either on its own accord or upon receiving a complaint from an individual or organisation, to determine if an organisation has complied with the PDPA.

	The PDPC is empowered to give directions to the organisation such as to : a) stop collecting, using or disclosing personal data in contravention of the PDPA; b) destroy the personal data collected in contravention of the PDPA; and/or c) pay a financial penalty of an amount not exceeding $1 million. Further, certain breaches of the PDPA may result in criminal liability. Breaches of the DNC Provisions amount to criminal offences. In addition, the PDPA provides individuals who suffer loss or damage as a result of a breach of the PDPA the right to commence civil proceedings in the courts against the organisation.
How is electronic marketing regulated?	**Organisations sending marketing messages will need to be aware of its obligations under the PDPA and Spam Control Act.** Electronic marketing is regulated under 2 main pieces of legislation : a) PDPA; and b) Spam Control Act (Cap. 311A) ("SCA"). • The DNC Provisions cover messages that contain marketing elements which can be received by recipients via: • voice calls; • smses / mmses (short message service / multimedia messaging service); and

	• facsimiles. One of the requirements of the DNC Provisions is that it requires a sender of such marketing messages to first check the respective DNC registry to ascertain whether the recipient's number is on the registry. If the recipient's number is on the registry, the sender must not send marketing messages to that number. This is unless the sender has received prior clear and unambiguous consent from the recipient. Other requirements are applicable as well. A breach of the DNC Provisions is criminal. The SCA was enacted to control email and mobile spam in Singapore. Under the SCA, marketers are under certain obligations when sending unsolicited communications through emails or text messages. Such obligations include providing a means to unsubscribe in the marketing message, and labelling the messages as advertisements with the <ADV> letters.
Are there any recent developments or expected reforms?	**There are no reform proposals currently in place.** There are no reform proposals currently in place.

Contact Information

Steve Tan steve.tan@rajahtann.com	**Rajah & Tann Singapore LLP** 9 Battery Road Singapore Singapore 049910 Tel 65.6535.3600

Lex Mundi World Ready

Lex Mundi Data Privacy Guide

Taiwan

Prepared by Tsar & Tsai Law Firm, Lex Mundi member firm for Taiwan

Key Legislation Overview	
What is the Key Legislation?	**Personal Data (Information) Protection Law ("PDPL").** The PDPL became effective on 1 October 2012. The PDPL contains privacy principles that generally conform to the OECD Guidelines, and imposes obligations on entities that collect, process and use personal data.
Key Data Protection Provisions	
What data is protected?	**Personal data** The PDPL provides a definition for personal data— name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and other information which may directly or indirectly be used to identify a living natural person.
Who is subject to privacy obligations?	**All private sectors and government agencies** The PDPL is a general data protection regulation and applies to all private sectors and government agencies.
How is the collection of personal data regulated?	**The data controller shall provide proper notice for the collection prior to or upon collection.** The data controller is permitted to collect and process personal data only if the data controller unambiguously

	informs the data subject of the following information prior to or upon the collection: • data controller's name; • purpose for collecting personal data; • categories of personal data; • period, area, recipients and means of using the data; • the data subject's rights and the methods by which the data subject may exercise those rights in accordance with the PDPL; and • where the data subject has the right to choose whether or not to provide the data, the consequences of not providing the data.
How are the use and disclosure of personal data regulated?	**Personal information collected should in principle only be used for the purpose notified and not for any other purpose.** Where the data collector wishes to use the personal data for any new purposes not previously notified or consented to by the data subject, the data collector must obtain the data subject's separate written consent for the new purpose.
How are storage, security and retention of personal data regulated?	**Proper security measures are required.** Data controllers should adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed. The central competent authority may request the data controller to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.
Are there rights of access to and correction of personal data?	**Yes** Under the PDPL, a data subject has the right to request the deletion of their personal information if the purposes of processing or use no longer exist.
Are there restrictions on cross border data transfers?	**Yes** In general, transfer of personal data abroad does not require

	approval from the authorities, unless the sector-based laws provide otherwise. For example, financial institution, in certain circumstances, are subject to approval requirements and shall obtain prior approval from the financial supervisory authority to transfer consumer personal data to an offshore third party.
Are there any notification requirements for data breaches?	**Yes** Where personal data is stolen, altered, leaked or the data subject's interests are otherwise compromised due to the data collector's failure to comply with the PDPL, the data collector is required to use appropriate methods to notify affected data subjects of the incident and the remedial measures that the data collector has adopted after investigating the incident.
Who is the privacy regulator?	**Various government authorities.** There is no single regulator or authority that oversees the PDPL. Industry sector regulators and local government authorities have separate responsibilities for the enforcement of the PDPL. The power to enforce the privacy law is shared by government authorities based on a sectoral basis.
What are the consequences of a privacy breach?	**Civil and criminal liabilities.** Liabilities for breach of the PDPL include fines of up to NT$1m (US$34,000), imprisonment of up to five years, compensation for civil damages claims of up to NT$20,000 (US$700) per claim and class action litigation up to a total of NT$200m (US$6.7m) per action.
How is electronic marketing regulated?	**An right to opt-out should be provided** The PDPL provides that when the data subject refuses the electronic marketing, the data controller should cease using such personal data. In addition, when making the first marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

Are there any recent developments or expected reforms?	**Yes** The PDPL was recently amended, enlarging the scope of personal information to be sensitive, and eliminating criminal liability for violations of the PDPL without a profit motive. The amendments came into force on March 15, 2016.

Contact Information

Eugenia Chuang eugeniachuang@TsarTsai.com.tw	**Tsar & Tsai Law Firm** 8th Floor, 245, DunHua S. Road, Section 1 Taipei Taiwan 106 Tel 886.2.2781.4111

Lex Mundi Data Privacy Guide

Thailand

Prepared by Tilleke & Gibbins, Lex Mundi member firm for Thailand

Key Legislation Overview	
What is the Key Legislation?	**Provisions of the Civil and Commercial Code and provisions of the Penal Code are generally applicable. In addition, some laws/regulatory notifications set out special protections for data in particular sectors and/or particular types of data.** At present, Thailand lacks a comprehensive data protection law. However, there are several industry-specific requirements, with certain as sectors such as telecommunications, banking/finance, insurance, securities, healthcare, consumer credit, and electronic payment services (collectively, "Specially-Protected Sectors"), all having separate approaches to personal data protection. There is a separate regime applicable to government entities, and there are also some laws/provisions which bind those individuals engaging in certain professions/occupations, such as medical practitioners, pharmacists, druggists, midwives, nursing attendants, priests, advocates, lawyers, or auditors, and assistants or trainees in such professions, as well as government officials. However, both within and outside the Specially-Protected Sectors, people who suffer damage due to unauthorized disclosure of their personal data may claim against the responsible party in tort (under the Civil and Commercial Code); criminal charges (under the Penal Code) may also be possible, depending on the circumstances (e.g. criminal defamation, etc.).

Key Data Protection Provisions	
What data is protected?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not specify which data is protected. Within the Specially-Protected Sectors, some of the regulatory notifications specify particular types of data that are protected.** For private sector companies outside the context of the Specially-Protected Sectors, the law does not specify which data is protected. Within the Specially-Protected Sectors, some of the regulatory notifications specify particular types of data that are protected. For example, regulations under the Telecommunications Business Act protect personal information of telecommunications subscribers (as specified therein) and the Credit Information Business Act protects credit information (as specified therein).
Who is subject to privacy obligations?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not specify who is subject to privacy obligations. Within the Specially-Protected Sectors, the parties subject to privacy obligations depend on the provisio** For private sector companies outside the context of the Specially-Protected Sectors, the law does not specify who is subject to privacy obligations. Within the Specially-Protected Sectors, the parties subject to privacy obligations depend on the provisions of each law/regulatory notification. For example, pursuant to regulations under the Securities and Exchange Act, licensees are obligated to address—as part of the application process—how they will protect personal data. Once approved, such effectively becomes a license condition. So, the licensee bears such obligation. Another example is under the National Healthcare Act. It provides that all persons are subject to the obligations restricting disclosure.

How is the collection of personal data regulated?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the collection of personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out requirements in respect of the collection of personal data.** For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the collection of personal data. Within the Specially-Protected Sectors, some regulatory notifications set out requirements in respect of the collection of personal data. For example, the Credit Information Business Act addresses this with specificity, in relation to the collection of credit information.
How are the use and disclosure of personal data regulated?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the use and disclosure of personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out requirements in respect of the use and disclosure of personal data.** For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the use and disclosure of personal data. Within the Specially-Protected Sectors, some regulatory notifications set out requirements in respect of the use and disclosure of personal data. For example, pursuant to regulations under the Telecommunications Business Act, the use and disclosure of personal information is restricted to those purposes set out in the regulatory notification. Similarly, under the Financial Institutions Business Act, information can only be disclosed for specified purposes.
How are storage, security and retention of personal data regulated?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the storage, security, and**

	retention of personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out requirements in respect of the storage, security, and retention of personal data. For private sector companies outside the context of the Specially-Protected Sectors, the law does not set out specific regulations for the storage, security, and retention of personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out requirements in respect of the storage, security, and retention of personal data. For example, regulations under the Computer Crimes Act impose requirements on service providers (as defined therein) in relation to retaining personal data of service users. They set out the specific categories of personal data that must be retained, as they enumerate requirements for how it should be stored. Another example is regulations issued under the Royal Decree on Electronic Payments. As part of the licensing process, an applicant for an electronic payment license must explain how it will protect information of service users. This includes how such information is stored, etc. Once approved, such becomes a license condition.
Are there rights of access to and correction of personal data?	**For private sector companies outside the context of the Specially-Protected Sectors, the law does not provide specific rights to access or correct personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out rights to access and correct personal data.** For private sector companies outside the context of the Specially-Protected Sectors, the law does not provide specific rights to access or correct personal data. Within the Specially-Protected Sectors, some laws/regulatory notifications set out rights to access and correct personal data. Examples include the Credit Information Business Act and regulations issued under the Telecommunications

	Business Act, each of which contain provisions for an access/correction mechanism.
Are there restrictions on cross border data transfers?	**For private sector companies outside the context of the Specially-Protected Sectors, statute does not prohibit the transfer of personal data to another country for the purposes of analysis thereof, and the law imposes no particular restrictions or conditions in respect of such transfers. As for the Specially-Protected Sectors, such requirements may exist, depending on the sector.** For private sector companies outside the context of the Specially-Protected Sectors, statute does not prohibit the transfer of personal data to another country for the purposes of analysis thereof, and the law imposes no particular restrictions or conditions in respect of such transfers. There is no governmental authority from which to seek approval for such transfers. As for the Specially-Protected Sectors, such requirements may exist, depending on the sector. For example, the Credit Information Business Act contains restrictions on the transfer of information abroad. Also, regulations issued under the Telecommunications Business Act specify that a further regulatory notification may be issued to impose restrictions on the transfer of information abroad (thus far, such has not been issued).
Are there any notification requirements for data breaches?	**For private sector companies outside the context of the Specially-Protected Sectors, statute does not require the provision of notification in respect of data security breaches. However, such requirements could be applicable in the Specially-Protected Sectors.** For private sector companies outside the context of the Specially-Protected Sectors, statute does not require the provision of notification in respect of data security breaches. Nevertheless, if such a breach occurs, and losses/damages to the data subjects can be mitigated by making such

	notification, then it would be advisable to do so. As for the Specially-Protected Sectors, such requirements may exist depending on the sector and the applicable provisions. For example, as part of the license application process under the Securities and Exchange Act, applicants must address how they will protect information of clients. This could include notification to affected clients when a breach occurs. Once the license application is approved, this would effectively become a license condition. Similar obligations exist for electronic payment licensees, under the Royal Decree on Electronic Payments.
Who is the privacy regulator?	**For private sector companies outside the context of the Specially-Protected Sectors, there is no specific privacy regulator. In the Specially-Protected Sectors, the regulators specific to those sectors may have some authority in respect of privacy matters in those sectors.** For private sector companies outside the context of the Specially-Protected Sectors, there is no specific privacy regulator. In the Specially-Protected Sectors, the regulators specific to those sectors would have some authority in respect of privacy matters in those sectors. For example, the Securities and Exchange Commission would have the authority to deal with noncompliance with license conditions that concern privacy. Another example is the Credit Information Protection Committee, which has the authority to deal with noncompliance with privacy obligations under the Credit Information Business Act.
What are the consequences of a privacy breach?	**A privacy breach can result in civil liability, criminal liability (including fines and/or imprisonment), and/or administrative action.** Both within and outside the Specially-Protected Sectors, people who suffer damage due to unauthorized disclosure of their personal data may claim against the responsible party in

	tort; criminal charges may also be possible, depending on the circumstances (e.g. criminal defamation, etc.). Laws/regulations applicable within the Specially-Protected Sectors set out other specific penalties for breach, which may include fines, imprisonment, or administrative action, such as loss of license.
How is electronic marketing regulated?	**Generally, privacy matters in the context of electronic marketing are regulated in the same manner as other data privacy matters. However, the Computer Crimes Act and the Telecommunications Business Act are also relevant.** Generally, privacy matters in the context of electronic marketing are regulated in the same manner as other data privacy matters. However, it is important to ensure that the relevant activities do not constitute a breach of the Computer Crimes Act or the Telecommunications Business Act. For example, they must not interfere with normal operation of the recipient's computer equipment, and they must not constitute illegal eavesdropping.
Are there any recent developments or expected reforms?	**There are multiple pending new laws and regulatory notifications.** There are a number of pending new laws that may come into effect at some point in the future, any of which would likely result in the need to revisit these issues. Such laws include: • Cyber Security Bill • Personal Data Protection Bill • Bill to Amend the Electronic Transactions Act • Bill to Amend the Computer Crimes Act

	In addition, a number of regulators in individual sectors have been working on upgrading regulation of data protection matters, within their regulatory domains. This will result in new regulatory notifications.

Contact Information

David Duncan David.D@tilleke.com **Jeffrey Blatt** Jeffrey.b@tilleke.com	**Tilleke & Gibbins** Supalai Grand Tower, 26th Floor Bangkok Thailand 10120 Tel 66.2653.5555

This guide is part of the Lex Mundi Global Practice Guide Series which features substantive overviews of laws, practice areas, and legal and business issues in jurisdictions around the globe. View the complete series of Lex Mundi Global Practice Guides at: www.lexmundi.com/GlobalPracticeGuides