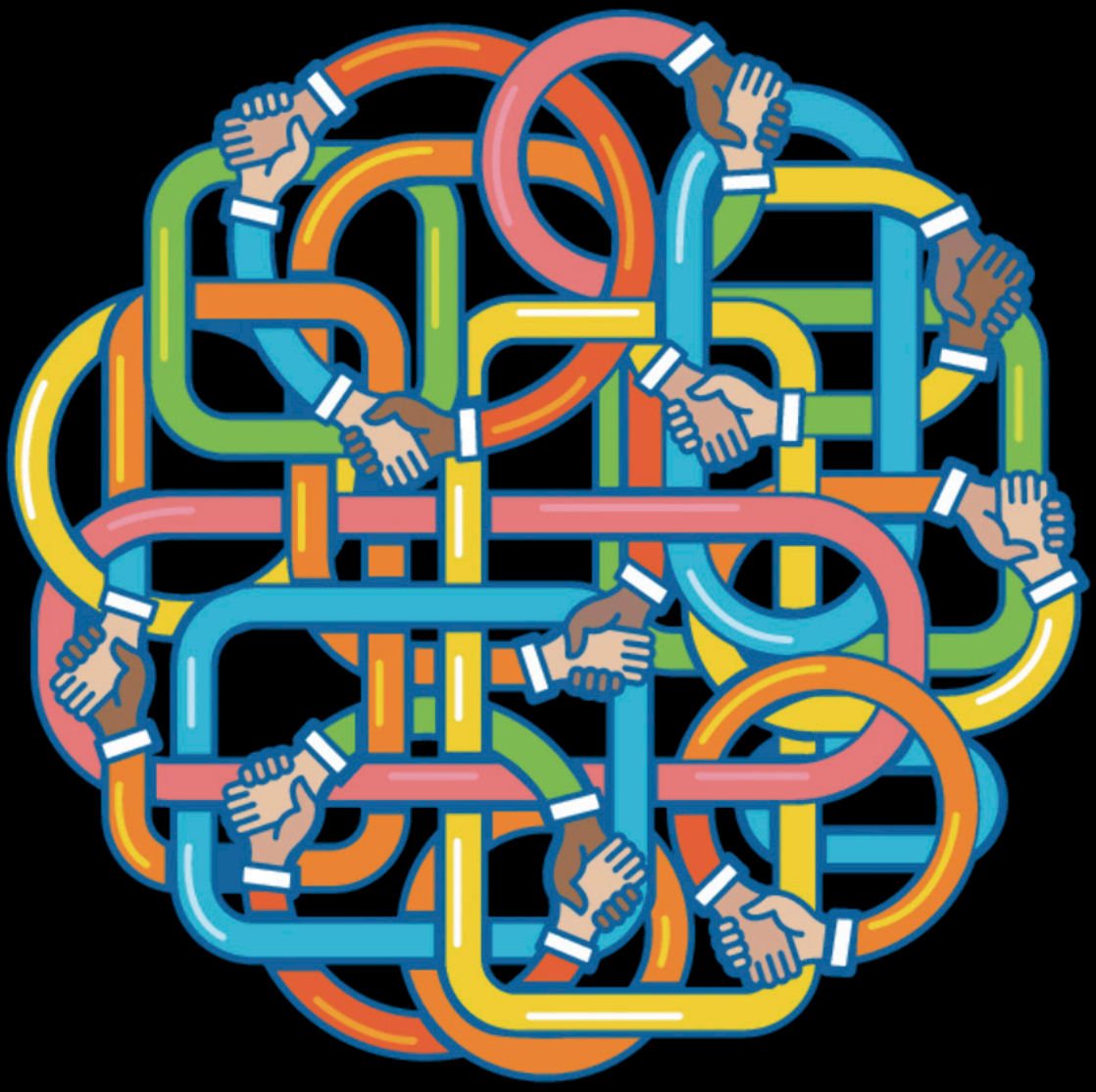
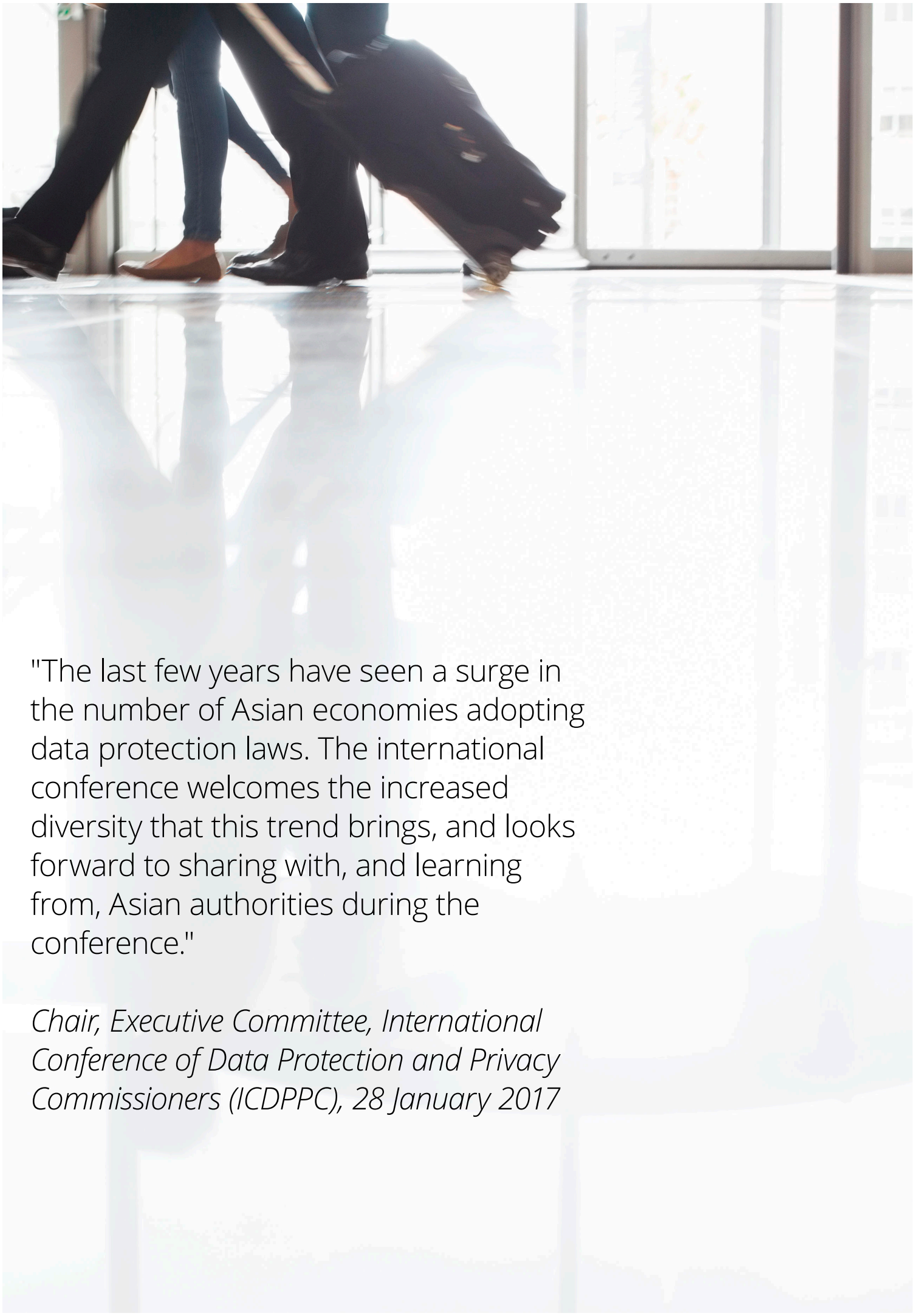
Deloitte.



Building trust across cultures

Privacy and data protection

Cyber Risk



"The last few years have seen a surge in the number of Asian economies adopting data protection laws. The international conference welcomes the increased diversity that this trend brings, and looks forward to sharing with, and learning from, Asian authorities during the conference."

Chair, Executive Committee, International Conference of Data Protection and Privacy Commissioners (ICDPPC), 28 January 2017

Contents

Introduction

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
Partner, Australia

March 2017

As the Asia Pacific region embraces rapid development and growth **'a more competitive Asia is roaring back'.**

In a recent Deloitte **Voice of Asia**[1] report, Deloitte's top regional economists determined that 'a more competitive Asia is roaring back', driven by strong policy action and accelerated reform. Over the last 12 months, this has meant an influx of data protection regulation in the Asia Pacific region at a local, regional and international level.

In response, many countries in the region have introduced, and are introducing, new privacy rules.

The outsourcing industry, which continues to achieve profitable growth for organisations across sectors, is now exposed to increased privacy risks around how privacy is viewed. When it comes to transferring individuals' data across the region, it is important to better understand these risks in order to avoid data breaches. To do so requires a shift from a privacy and data protection approach that focuses solely on compliance with existing and emerging regulations, to one that also considers the region's culture and individual expectations, and so builds trust with both individuals and regulators.

Embracing cultural differences

Given the cultural diversity in the Asia Pacific region among people, regulators and organisations, getting it right can deliver a competitive edge. An organisation's proactive approach to understanding and embracing difference will augment its sensitivity to nuanced privacy and data protection risks.

This sensitivity lays the groundwork for greater organisational sustainability, as well as the opportunity for immediate accountability in an organisation's culturally diverse operations. In this way, an organisation can adhere to global and regional regulatory change with a local approach—'glocalising' its privacy risk management, as it were.

Emerging regulation pushing for regional collaboration

At a local level, countries such as the Philippines and Chinese Mainland have introduced stronger laws governing the use of information about individuals. A common set of principles introduced by the Asia Pacific Economic Corporation's (APEC) Privacy Framework encourages the harmonisation of privacy and data protection rules across our region. Although the Framework now includes cross border transfer rules and while the Framework is non-binding, it is a step towards assisting organisations to take a regional approach to privacy risk management. Finally, the impact of the European Union's General Data Protection Regulation demonstrates the extra-territoriality of global regulations affecting the Asia Pacific.

This report

Trust across cultures and the risk of losing trust are core strategic risks that need to be managed—particularly given the trend to expand the territorial scope of regulation beyond the country of origin. This includes balancing the expectations of regulators and individuals.

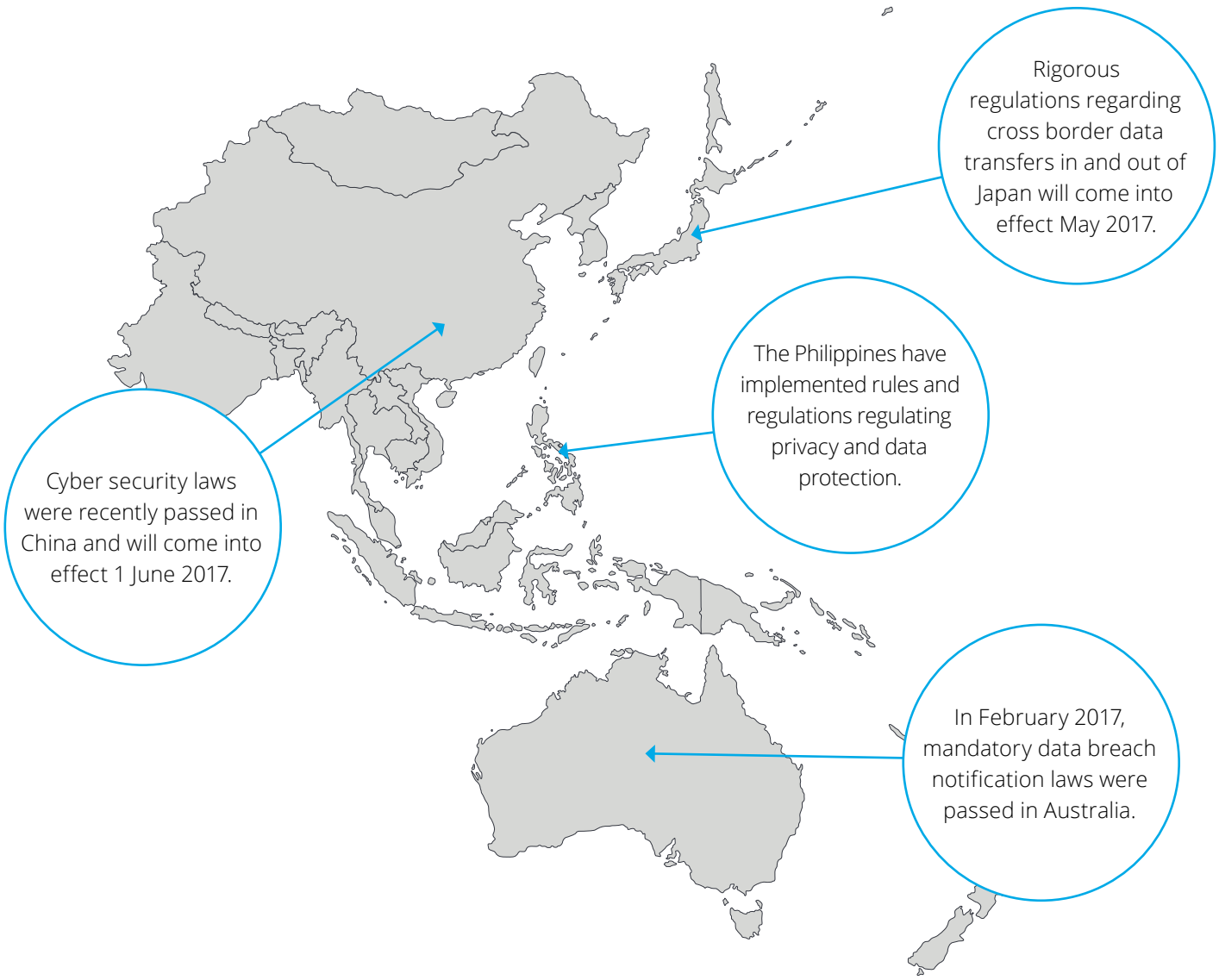
This report highlights the major considerations and developments in the Asia Pacific region and is aimed at starting a broader conversation about privacy and data protection.

We look forward to working together to address the many challenges to come.

1. Deloitte's top regional economists identify and analyse pressing economic and regulatory issues, calling out their impact on the region's governments and businesses

Asia Pacific at a glance

In the last twelve months our region has seen significant change in privacy and data protection laws



'A new and optimistic generation is taking its place in driving the direction of their economies: one that is technologically savvy, comfortable with the borderless consumerism of the global middle class, and yet imbued with the consumption-smoothing instincts of its parents and grandparents.

These new consumers are exactly what Asia and the world need right now. They're inherently optimistic and incredibly open to innovation and new ideas. They'll make enthusiastic importers as well as formidably competitive exporters. And yet, like consumers everywhere, they will be a stabilising force in their giant economies. That means they're likely to play an anchor role for 2017 regardless of other developments.'

Voice of Asia, Deloitte 2017

Australia

Type of information protected under legislation

In Australia, privacy is regulated nationally by the Privacy Act 1988 through the Office of the Australian Information Commissioner (OAIC). The types of information protected includes:

- Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained
- Sensitive information is considered a subset of personal information to which more stringent protections apply

Specific industry considerations

The Privacy Act is supplemented by industry specific regulatory regimes that apply to:

- The health industry
- Credit providers and credit reporting bodies
- Telecommunications and media

Did you know?

Assessments of organisation by the OAIC have increased in frequency, reflective of the growing awareness of privacy from Australian consumers, with 94% prioritising trust over ease of use when accessing websites.

Deloitte Australian Privacy Index 2016

Considerations

There are thirteen Australian Privacy Principles that apply to Australian government agencies, most large private sector organisations, direct marketers, data brokers and all private health service providers nationally. In some circumstances there is an exemption for small businesses and private sector employment records.

Credit providers and credit reporting bodies have additional obligations regarding consumer credit reporting information. This regulates the types of personal information that can be included in a credit report, who can access those reports and why, and imposes obligations to ensure that the information is accurately maintained.

Recently introduced mandatory data retention laws require telecommunications and internet service providers to securely retain telecommunications metadata.

The OAIC conducts and publishes assessments of organisations. A new mandatory data breach notification law was passed in February 2017. The new law obliges organisations to notify individuals and the OAIC of suspected or actual breaches of personal information that is likely to result in serious harm.

Chinese Mainland

Type of information protected under legislation

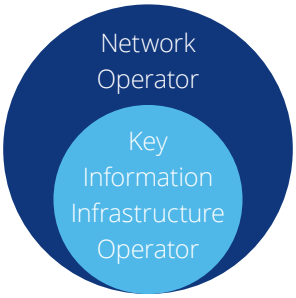
China Cyber Security Law protects all kinds of 'important' business information, including personal information, recorded electronically or otherwise, that can be used to independently identify or be combined with other information to identify a natural person.

Personal information includes, but is not limited to a natural person's name, date of birth, ID number, biologically identified personal information, address and telephone number.

Specific industry considerations

Data privacy laws are supplemented by industry specific regulatory regimes. In the financial services industry, regulations require that financial institutions store and process personal financial information collected and produced during operations within the territory of China.

If it is necessary to transfer personal financial information to overseas parties, financial institutions must ensure contractual provisions are in place, guaranteeing the protection of personal financial information.



Did you know?

China's cyber security law is relatively new and applies broadly.

There is further scope to broaden the laws to incorporate industry specific and Key Information Infrastructure (KII) specific requirements. Sectors this could apply to include public services, energy, media, government, health care, finance, transportation, telecommunication and manufacturing.

Considerations

	To collect and use personal information, network operators shall clearly express the purposes, means and scope of collecting and using the information, and obtain the consent of the individuals whose data is collected.
	KII operators must store personal information and important business information within Chinese Mainland. If it is necessary to provide the information to overseas parties then a security assessment must be conducted. The scope of KII is still pending definition by the State Council.
	Network operators shall not divulge, distort or damage the personal information they have, and must not provide it to others without their consent.
	If personal information has, or may have been compromised, network operators must take measures immediately to inform users and report the breach to the relevant departments.
	'Measures for Network Products and Services' introduced on 2 May 2017 require all 'important network products and services for networks and information systems that are pertinent to national security' to be subject to a security assessment.

Hong Kong

Type of information protected under legislation

Personal data is regulated under the Personal Data (Privacy) Ordinance (PDPO) and is administered by the Office of the Privacy Commissioner for Personal Data.

Personal data is defined as information which relates to a living person that can be used to identify that person, and exists in a form in which access or processing is practicable.

Specific industry considerations

While the Privacy Commissioner has primary responsibility for personal data regulation in Hong Kong, the Hong Kong Monetary Authority has also issued guidance to deposit-taking institutions specific to customer data protection.

Did you know?

In 2015, public complaints to the Privacy Commissioner's office in Hong Kong increased by almost 20% to 1,971. Of those complaints, 74% were made against the private sector, mostly in the financial sector.

Hong Kong Privacy Commissioner, Annual Report 2015

Considerations

	The PDPO contains six Data Protection Principles with which data users must comply.
	Specific requirements are imposed on the management of identity card numbers, customer credit information and human resource related information.
	The Privacy Commissioner can conduct an investigation of a complaint about any possible breach of the PDPO.
	Non-compliance with the Data Protection Principles can result in an enforcement notice served by the Commissioner or legal proceedings resulting in a monetary fine and/or imprisonment.
	The PDPO Cross-Border Data Transfer provision is not yet effective, but a guidance note has been issued. When effected, it will prohibit the transfer of personal data outside of Hong Kong subject to specific circumstances.

India

Type of information protected under legislation

India does not currently have any specific privacy law. However, information technology, including some interpretable aspects of data privacy, are governed by the IT Act 2000, its Amendment in 2008, and subsequent IT Rules, which were released in 2011. It defines personal information 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 such a person.

The Information Technology Rules 2011 further defines Sensitive Personal Data or Information (SPDI) as information that attracts additional restrictions and obligations. It includes passwords, banking and financial information, health and mental health records, and biometric information.

Specific industry considerations

Some industries in India are subject to additional legal obligations. These include a code that applies to medical information, regulation for telecommunication information and the outsourcing of banking operations overseas.

Credit information companies and credit institutions (including banks) must also comply with credit information regulations. These are not prescribed by law or by the regulator, but must be framed by the relevant credit information companies and institutions.

Did you know?

Generally, the IT Rules apply to individuals or 'data subjects' located in India. This means that the IT Rules may not apply to data processing that takes place in India if the 'data subjects' are located overseas.

Considerations

	Organisations must publish a privacy policy that outlines the types of information that it collects and the reasons for collection, who it is disclosed to and any steps it takes to keep the information secure.
	Personal information can only be collected if the individual concerned has provided consent, and the organisation must provide the individual with appropriate notification.
	The information can be used only for the purpose for which it was collected and it can generally only be retained for as long as that use remains valid. The individual can review information that is held about them and ask that it be corrected if it is wrong.
	There are restrictions on transferring SPDI that must be considered before an entity discloses the information to any third party, whether in India or overseas.
	There are penalties for entities who fail to comply with the data protection provisions, including fines and imprisonment.

Indonesia

Type of information protected under legislation

The primary data protection laws are the Electronic Information and Transaction Law (EIT Law) and the Government Regulation No. 82 on the Implementation of Electronic System and Transaction (GR 82/2012).

These laws define personal data as certain personal information that is kept and maintained, and its accuracy and confidentiality protected.

Specifically, GR 82/2012 introduces the term Electronic System Operator (ESO) which means any person, state administrator, business or public entity that provides, manages, or operates an electronic system in its own interest or that of another party.

If your business is an ESO it may need to pay particular attention to the regulatory requirements.

Specific industry considerations

There are a number of other laws in Indonesia that regulate the collection of personal information, particularly in relation to banking and finance activities and healthcare.

Considerations

	ESOs can be public or non-public services. ESOs providing public services are required to be registered whilst those in non-public services may choose to be registered.
	The key principle in handling personal data in Indonesia is to obtain the consent of the individual to whom the data pertains.
	There are no specific standards or expectations about transparency, retention, correction or deletion of personal data. However, the government is reportedly considering a new and more detailed Personal Data Protection Bill to govern personal information held in electronic systems.
	ESOs are required to notify individuals in the event of a breach of personal data, but there is no further explanation in the regulation as to how and when any notification should be made.
	The Ministry of Communications and Informatics (MCI) is responsible for administering the data protection regime. The MCI can investigate matters involving unlawful handling of personal and confidential information, that could result in penalties, including fines and imprisonment.

Japan

Type of information protected under legislation

Japan's amended Personal Information Protection Act (PIPA) will be fully effective as of 30 May 2017. PIPA applies to data controllers, which are considered to be entities handling personal information databases for business purposes, and are not state institutions or local public entities.

Personal information regulated by PIPA includes any information relating to a living individual that can be used to identify them, either alone or in combination with other easily accessible information.

In addition, Special Care-required Personal Information includes racial, religious, medical and other sensitive information, and consent is received for it to be collected or processed.

Specific industry considerations

Particular industries, including financial, medical and telecommunication services are subject to additional guidelines implemented by the Personal Information Protection Commission (PPC).

Businesses that deal with big data containing personal information can create and provide to a third party *Anonymously Processed Information* in accordance with the standard set by the PPC.

Did you know?

The amended PIPA requires that businesses keep records of how and from where it collected personal information. More information about the record keeping requirements is available from the PPC.

Considerations

	The PIPA established the PPC which monitors and supervises businesses as an independent authority over all data controllers who have a presence in Japan. The PPC currently has limited supervisory power but is soon expected to be the central regulatory authority over business operators handling personal information.
	There are some exemptions for using personal information for journalism, literary work, academic studies, and religious and political activities.
	The PIPA requires that consent be obtained before personal information about an individual can be transferred by a data controller to a third party in a foreign country if the recipient does not have a data protection system that conforms to standards prescribed by the PPC.
	Businesses are required to record provision and receipt of personal information to or from a third party as well as to have prior consent.
	Improper use of personal information databases, such as data theft or providing information to third parties for wrongful gain can result in criminal penalties.

Korea

Type of information protected under legislation

The Korean Personal Information Protection Act (the PIPA) applies to personal information that pertains to a living person, including full name, Resident Registration Number, or any information by which the individual in question can be identified.

It includes information that might not immediately be identifiable, but could help to identify someone by combining it with other information.

Specific industry considerations

Businesses should be aware that there are some specific industry regulations that apply in certain sectors. In particular, the following industries have legislation to supplement the PIPA:

- Banking
- Health
- Employment/ industrial relations

Considerations

	The PIPA applies to Data Handlers which are considered to be any agency, company, organisation or individual that by itself or through a third party, handles personal data in the course of or in relation to its business activities.
	The PIPA contains eight privacy principles with which both public and private sector data handlers must comply, regardless of their size.
	In 2016, punitive damages and statutory damages were newly introduced by PIPA. Civil damages are provided for personal information loss, theft, leak, or falsification, caused by wilful misconduct or gross negligence of the data processor. Victims will also be able to claim punitive damages of up to three times the amount of civil damages.
	The Korean government is allowed to process health-related personal data or electronic medical records, through a Cloud Communication System from 6 August 2016.
	From June 2016, every enterprise which had sales of no less than KRW 15 billion in the previous year must obtain the Certification of Information Security Management System (the ISMS).

Malaysia

Type of information protected under legislation

Malaysia's Personal Data Protection Act 2010 (PDPA) regulates the collection, storage, processing and use of personal data by data users. It also requires any person who processes, has control over or authorises the processing of personal data with respect to commercial transactions, to comply with requirements issued by the Personal Data Protection Commissioner.

Personal data is generally considered to be information that relates to a data subject who is identifiable from that information.

Specific industry considerations

Certain classes of Data Users are required to register with the Department of Personal Data Protection, including accounting, auditing, legal, engineering, architecture and housing developers, as well as medical and dental services.

Did you know?

Unless a specific exemption applies to countries specified and published by the relevant Minister, data users are generally not permitted to transfer personal information outside Malaysia.

Considerations

	The PDPA contains seven high level principles, including a general data protection principle and principles related to notice and choice, disclosure, security, data retention, data integrity and data access.
	The PDPA does not apply to Malaysian government agencies or to personal data processed outside of Malaysia. However, it does apply to foreign entities that are not located in Malaysia but use equipment there for processing personal data.
	The PDPA framework also includes subsidiary regulations and standards that have been issued by the Personal Data Protection Commissioner since the PDPA was implemented. Data users should consider these regulations with respect to their particular organisation.
	The Personal Data Protection Standards 2015 comprises of a set of standards relating to security, retention and data integrity of both electronic and non-electronic personal data. The Standards specify minimum requirements for electronic personal data that include registration of employees involved in processing of personal data, identity management, password protection, malware protection, and restrictions on the use of removable media devices and cloud computing.
	The Personal Data Protection (Compounding of Offences) Regulations 2016 specifies the types of offences against the PDPA that may be compounded.

Mauritius

Type of information protected under legislation

The Data Protection Act 2004 and Data Protection Regulations 2009 are administered by the Data Protection Office (DPO). The regulatory regime provides protections for personal data and sensitive personal data managed by both the public and private sector.

Types of information protected under the legislation includes:

- Personal data is information which relates to an individual, including an opinion forming part of database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.
- Sensitive data is personal information concerning a data subject and consisting of information relating to race, ethnicity, political opinions, religious beliefs, membership to a trade union, physical or mental health, sexual preferences, commission or alleged commission of an offence and proceedings for an offence committed or alleged to have been committed.

Did you know?

The DPO website has some resources that can help data controllers perform a privacy self-assessment.

Considerations

There are eight Data Protection Principles (DPPs) in the Data Protection Act that regulate the collection, processing, integrity, security and cross border transfer of personal data.

While there is no specific legislative requirement for an organisation to have a Data Protection Officer, common practice has led to the establishment of a personal data compliance officer in most organisations.

All data controllers need to be registered with the DPO and the register is made available on the DPO website.

Registrations with the DPO have an expiry date and will need to be renewed at least a month before they end.

There is currently no scheme monitoring data breach notifications but the DPO encourages data controllers to be proactive – to notify the affected individuals where there is a risk of harm and report material breaches to the Commissioner.

Mongolia

Type of information protected under legislation

Under the Organisation Secrets Act 1995, sometimes called the Organisation Privacy Act, a company can determine by itself what type of information is considered confidential in Mongolia.

The Act refers to information, technical solutions or designs, research materials and technologies and equipment, which if disclosed may have adverse impacts on the dominant position in the market.

Specific industry considerations

The Banking Act 2010 imposes fines on any person who discloses confidential information held by a bank, but like the Organisation Secrets Act it allows the bank to decide what information is deemed confidential.

Did you know?

Mongolia also has the Personal Secrecy Act 1995 that gives people the right to sue for breaches of personal privacy.

Considerations

	In Mongolia an organisation is free to determine what information it should keep confidential.
	An organisation is not allowed to keep confidential any information which contains evidence that the equipment and technologies being used are having an adverse impact on human health or the environment.
	An organisation is not allowed to keep any information confidential that relates to any crime.
	The laws of Mongolia do not provide any legal remedies for breaches of confidentiality. The Organisation Secrets Act provides that an organisation can file a petition with the courts and the dispute will be adjudicated in accordance with the contract signed between the parties.

New Zealand

Type of information protected under legislation

The Privacy Act in New Zealand protects information about identifiable individuals. What information makes an individual identifiable is left open to interpretation. It applies whether or not the information is true, and whether or not it is recorded in a material form.

The Act regulates all agencies, broadly defined as whoever who holds the personal information, irrespective of whether the entity is in the public or private sector. In some cases the Act even applies to individuals.

Specific industry considerations

Some industries are also subject to specific requirements related to:

- Health
- Credit reporting
- Telecommunications
- Media and broadcasting
- Employment

Did you know?

Any organisation working with or selling services to the public sector will be expected to be compliant with the New Zealand Information Privacy Principles.

Considerations

	The Act contains twelve Information Privacy Principles (IPPs) in three broad categories—collection, use, and disclosure. Where more specific standards are required, the Privacy Commissioner can issue specific codes of practice.
	Damages can be awarded for privacy violations. Those with a human rights component are treated as particularly serious, an approach that partially stems from New Zealand's Bill of Rights Act.
	The Privacy Act allows for Approved Information Sharing Agreements (AISA) as a legal mechanism to enable information sharing between or within agencies for the purposes of delivering public services. Private sector agencies are only allowed to be conditionally involved.
	Generally speaking, public sector agencies in New Zealand take their privacy obligations more seriously than the private sector and privacy is increasingly considered an essential factor in providing customer focused public services.
	The Minister of Justice recently indicated that reforms to New Zealand's privacy law are in the early stages of planning. The reforms may include changed information sharing arrangements between public sector agencies, and establishing a mandatory data breach notification scheme.

Papua New Guinea

While there is currently no legal framework for privacy and data protection in Papua New Guinea, the recent introduction of the Cybercrime Code Act 2016 regulates activities conducted through electronic systems and devices.

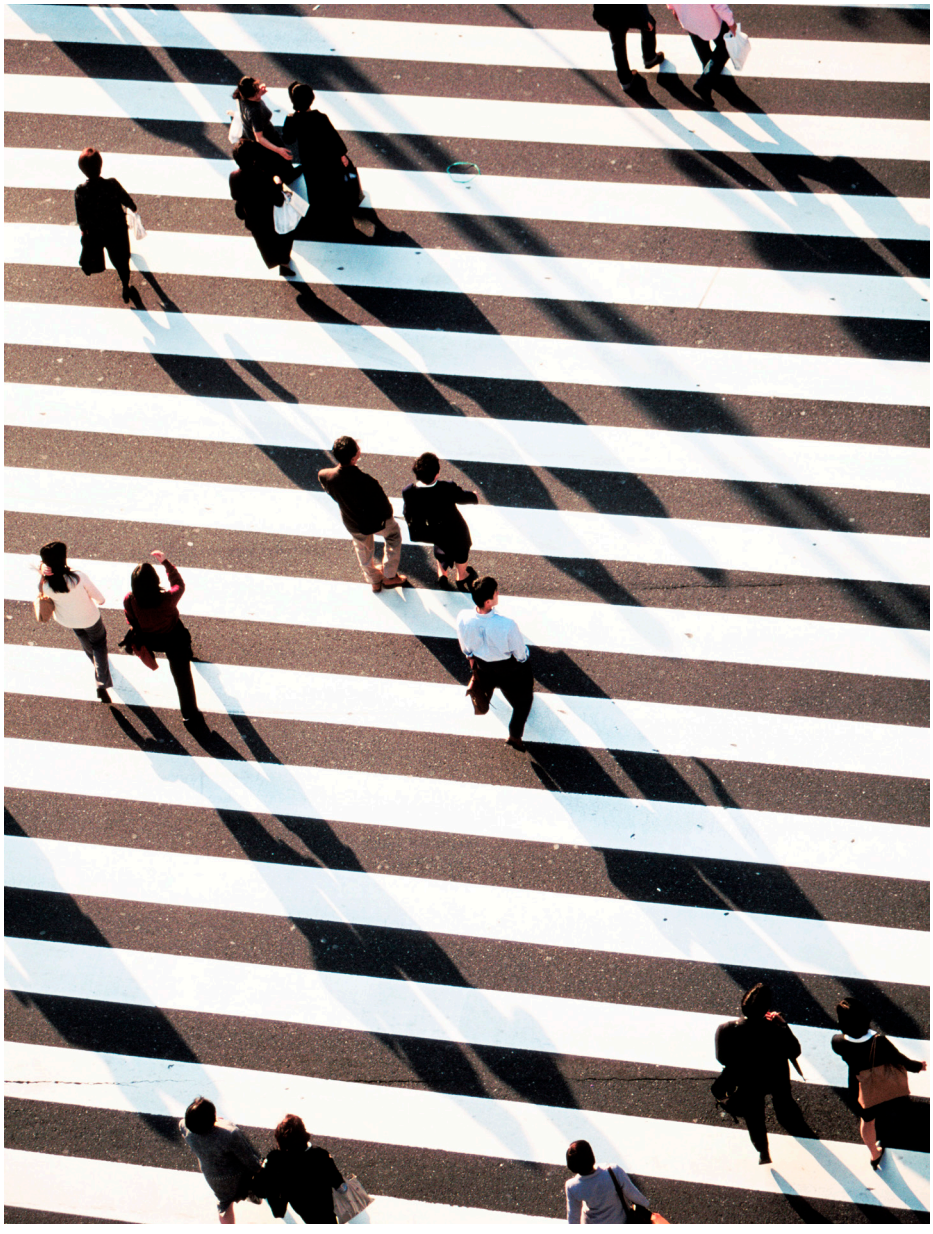
This Act is designed to prevent, or prosecute, crimes and offences committed against individuals, the public, government agencies or corporate entities, through the use of information and communication technologies (ICT).

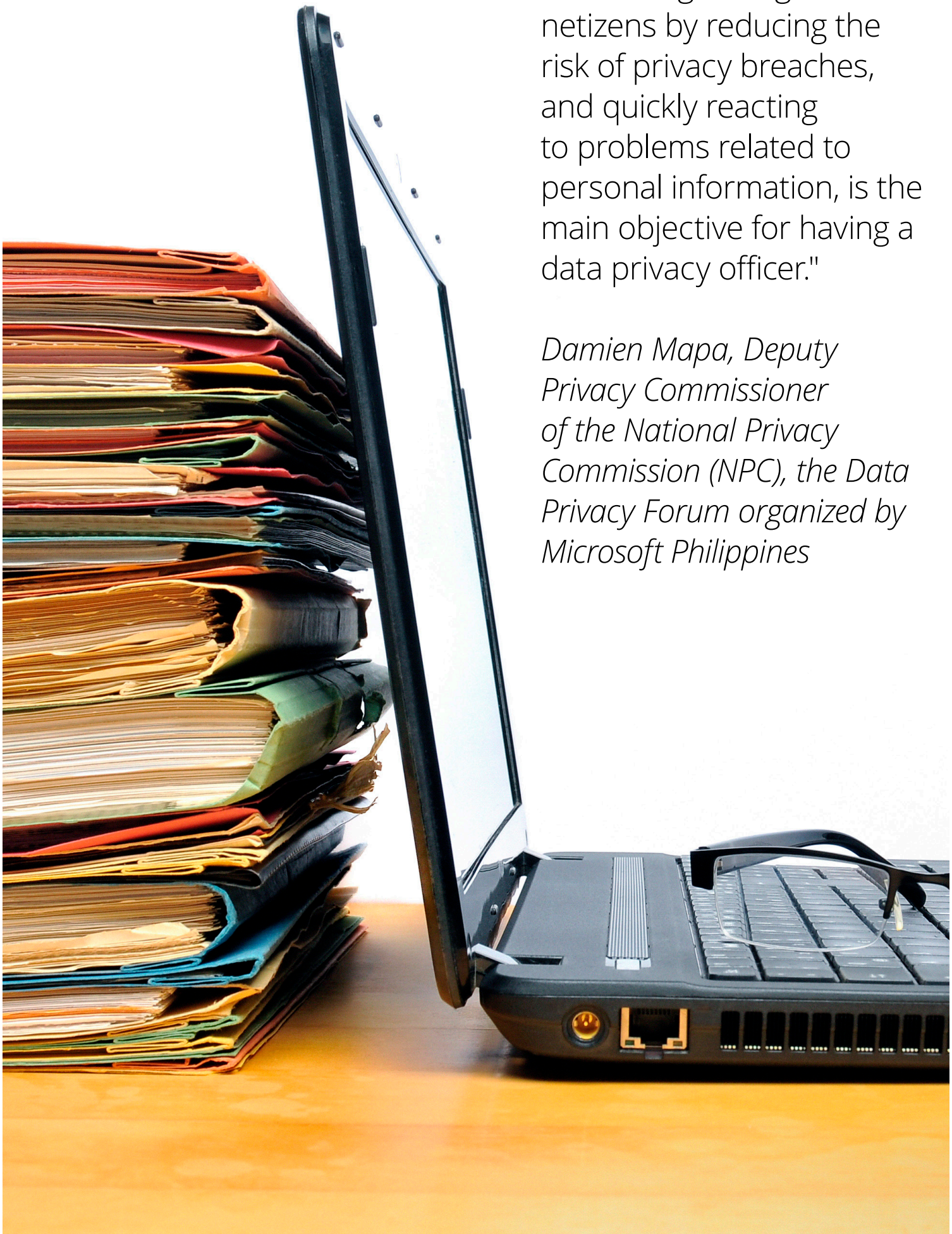
The Act regulates hacking, cyber bullying, child online grooming, unlawful advertising, cyber harassment, electronic fraud, forgery, gambling by children, identity theft, unlawful disclosure, infringement of intellectual property rights such as trademarks, copyright, patents and industrial designs, production, possession and publication of child pornography and animal pornography, the production and publication of adult pornography, the design and distribution of illegal devices and many other technical offences.

The Cybercrime Code Act provides mechanisms for law enforcement agencies to prevent, investigate and prosecute these kinds of cybercrimes. It also permits international cooperation between law enforcement agencies regarding cybercrime, where there may be criminal offences related to ICTs and the use of electronic systems and devices.

Private communications are protected under the Protection of Private Communications Act 1973. Private communications include any communications made by one person, meant for another, and precautions are taken to ensure they are not overheard.

The technology and media industry are most affected under this Act.





"Protecting the rights of netizens by reducing the risk of privacy breaches, and quickly reacting to problems related to personal information, is the main objective for having a data privacy officer."

Damien Mapa, Deputy Privacy Commissioner of the National Privacy Commission (NPC), the Data Privacy Forum organized by Microsoft Philippines

The Philippines

Type of information protected under legislation

The Data Privacy Act applies to personal information held by both public and private data controllers and processors.

In 2016, the National Privacy Commission issued Implementing the Rules and Regulations of the Republic Act No 10173 (the Rules or IRRs), which provides a practical framework for the Data Privacy Act.

Personal information means 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, or when put together with other information would directly and certainly identify an individual.

Did you know?

If you are operating in the Philippines, you may be required to submit an annual summary of security incidents and data breaches to the National Privacy Commission.

In certain circumstances some obligations might also apply outside of the Philippines. You should check whether these obligations apply to your activities.

Considerations

	The Rules have a significant impact on business in the Philippines, particularly the IT and Business Process Outsourcing industry, an industry reportedly worth over USD 20 billion in the Philippines and the largest contributor to the country's GDP.
	The Rules require that consumers be notified in a meaningful way whenever their personal information is collected.
	In the event of a data breach, if the information is sensitive or could be used for identity fraud, the Rules require that notification be provided to the Commission and to affected consumers often within 72 hours.
	The Rules contain a requirement to register data processing operations and to notify the Commission of automated processing operations in particular circumstances.
	There are penalties for improperly accessing and disposing of personal information, or processing personal information without the an individual's consent. These could include imprisonment and significant financial penalties.

Singapore

Type of information protected under legislation

The Singapore Personal Data Protection Act (PDPA) regulates personal information that identifies a person, either on its own or together with other information, whether true or not, whether sensitive or not, and whether electronic or not.

The PDPA excludes some information, including business contact information. Though data about deceased individuals is generally excluded, disclosure and protection obligations still apply to those individuals deceased ten years or less.

The Personal Data Protection Commission (PDPC) has been established by the Government to administer the PDPA.

Specific industry considerations

Accompanying the PDPA are advisory guidelines in a range of sectors including:

- Telecommunication
- Real estate
- Education
- Health care
- Social services

Did you know?

Organisations may still be able to use personal data collected before the PDPA came into effect in 2014, but if the data is to be used for a new purpose the organisation may have to seek a consent again.

Considerations

	The PDPA contains two main provisions—the Data Protection provision and the 'Do Not Call' provision (DNC).
	The Data Protection provision consists of nine key privacy obligations with which organisation must comply—consent, purpose limitation, notification, access and correction, accuracy, protection, retention limitation, transfer limitation and openness.
	An organisation must appoint a Data Protection Officer (DPO) to manage its data protection policies and ensure the organisation is compliant with the PDPA.
	Data intermediaries are organisations contracted to process personal data. They must comply with the same protection and retention obligations, meaning they need to ensure reasonable security measures are in place and that they do not retain the data if there is no longer a business or legal need to do so.
	The DNC provision prohibits organisations from sending certain marketing messages in the form of voice calls, text or fax messages to Singapore telephone numbers registered with the DNC Registry. Organisations that wish to send marketing messages must check with DNC registry or receive clear and unambiguous consent.

Sri Lanka

Type of information protected under legislation

The Information and Communication Technology Agency (ICTA) in Sri Lanka oversees a suite of e-laws that help to regulate electronic data and documents used in electronic transactions.

These laws enable smooth and easy domestic and international online transactions.

The Computer Crimes Act restricts anyone from modifying or deleting information without authority and makes it illegal to program a computer in such a manner so as to prevent authorised persons from obtaining access to it.

Specific industry considerations

Banks are regulated by several regulations. Organisations should check which regulations might apply to them.

Did you know?

In 2016 Sri Lanka introduced a Right to Information Act, giving citizens the right to seek access to information in the possession or control of a public authority. Sri Lanka also established an Information Commissioner's Office in December 2016.

Considerations

The ICT was vested with the National Certification Authority (NCA), making it the certification authority for the Electronic Transaction Act, governing all electronic contracts, e-commerce, e-business and e-Government activities.

The banking sector led the development of a digital certificate framework in Sri Lanka in order to have the appropriate information security safeguards in place and build customer confidence.

At present the government is considering implementing a Data Protection Act to help build a digitally inclusive Sri Lanka.

In May 2015, Sri Lanka adopted the Budapest Convention, making it a member of the Convention on Cybercrime. It adopted domestic legislation and has been cooperating with the Council of Europe in cybercrime matters.

The Computer Crimes Act creates offences for unauthorised modification, alteration or deletion of information and denial of access.

Taiwan

Type of information protected under legislation

The Personal Data Protection Act (PDPA) applies to all public entities, companies and also to individuals except where they are managing personal data purely for personal or family affairs.

Personal data is any information that is sufficient to directly or indirectly identify an individual.

Sensitive personal data includes a number of categories not limited to medical records, medical history, genetic information and criminal records.

Personal data can only be used for the purpose for which it was collected unless an exception in the PDPA applies. There are exceptions in the PDPA for personal data that is processed only for personal or family activities.

Did you know?

Any organisation operating in Taiwan can be prohibited by the regulatory authority from transferring any personal data overseas if it is deemed to be against the national interest, or if the overseas location does not have an adequate personal data protection regime.

Considerations

	Organisations that deal with personal information are required to provide adequate notice regarding the purpose and proposed use of the personal data to be collected.
	The PDPA gives individuals the right to review and request a copy of their personal information, to supplement or correct the information, to withdraw consent and have the collection and use of the personal information discontinued.
	Organisations that keep personal information must have proper security measures in place to prevent it being stolen, altered, damaged, destroyed or disclosed. When commissioning other organisations to collect, process or use personal information, the organisation must also properly supervise the commissioned agency.
	The PDPA provides for damages where an infringement of rights is deliberate or negligent.
	Several authorities are responsible for applying and enforcing the PDPA. The Ministry of Justice is responsible for drafting and interpretation of the PDPA, but industry regulators and local government authorities have responsibilities for enforcement in their particular areas.

Thailand

Type of information protected under legislation

There is no specific privacy law in Thailand though there are a number of laws that protect information in particular contexts.

The Trade Secret Act in Thailand protects significant trade information including formulas, programs, techniques, or processes. The Act specifically defines 'trade secret' and 'trade information' and provides penalties in cases of infringement.

Specific industry considerations

In some specific business areas including finance and telecommunications, there are laws that regulate the collection, use, disclosure and transfer of personal data.

Specific restrictions apply to sensitive personal information and businesses will require a person's consent before their data can be processed.

Did you know?

The right to privacy is enshrined in the constitution of the Kingdom of Thailand.

Considerations

	The Trade Secret Act is subject to the Central Intellectual Property and International Trade Court, a specialist court established to regulate intellectual property rights and trade in an accessible and user friendly way.
	The legislative definition of trade information is broad, including formula, form, compilations or assembled works, programs, methods, techniques, and processes.
	Civil remedies are available in case of disclosure of information without owner's permission. In some cases a criminal offence may also be imposed.
	In 2015, the Thai government approved a draft Personal Information Protection Act to reform the data protection regime but the Act is yet to be formally considered by the National Legislative Assembly.
	Thailand is currently considering a number of bills related to data protection and internet communications to support its growing digital economy.

Vietnam

Type of information protected under legislation

Vietnam's new Law on Cyber Information Security (CIS Law) is limited to the handling of personal information in commercial transactions in cyberspace.

It defines personal information as information associated with the identification of a specific person and includes a set of principles for data privacy protection that regulates collecting, editing, utilising, storing, providing, sharing or spreading the information.

The CIS Law also extends to protecting the private life of individuals, their family secrets, and personal and private information of both individuals and organisations.

Specific industry considerations

The new CIS Law is limited to the regulation of personal information in cyberspace. Other aspects of personal data protection in Vietnam are shared across a number of other sectoral, industry specific regulations.

Did you know?

CIS Law applies to individuals and organisations engaged in information technology application and development activities in Vietnam.

Considerations

	The recent introduction of the CIS Law, which encourages the strict and secure handling of personal information, provides the necessary regulatory framework for strong economic, social and political growth within Vietnam.
	Although consent is central to the CIS Law, there are provisions that strongly support national security. Sharing personal information without consent is permissible at the request of state agencies, and a cybersecurity service provider must cease their business for the sake of national security and public order if requested by a relevant government agency.
	The CIS Law does not contain any specific provisions for the transfer of personal data outside of Vietnam, nor does it include a data breach notification scheme.
	The main body responsible for enforcing data protection legislation is the Ministry of Information and Communications. It can conduct examinations and inspections, and examine complaints and other suspected data privacy violations.
	Organisations might be subject to a financial penalty, disciplinary action or a civil penalty for a personal information breach. Individuals may also seek compensation for any loss or harm suffered.

"Leveraging data for business opportunity and other competitive advantages does not happen by chance. One needs concerted effort and conscientious planning to design the business operations and organisational processes to collect and manage the data, and also protect it, before one can capitalise on data effectively for opportunities and growth. It starts with the people in our organisations – their awareness and their sense of ownership towards being custodians of data."

Dr Yaacob Ibrahim, Minister for Communications and Information at the Opening of the Fourth Personal Data Protection Seminar, 20 July 2016 Raffles City Convention Centre

Emerging trends across the region

Increasing opportunities and the use of data to drive business growth mean that organisations need to take a more proactive and localised approach to mitigating data privacy and protection risks; particularly as regulatory change occurs across the Asia Pacific region.

This exciting challenge demands increased collaboration across the region to stay ahead of this evolving landscape.

Trend 1: Regulators are taking a more pro-active approach to privacy and data protection

Regulators are responding proactively to shifting global and regional views, especially with evolving technologies and their impact on individuals.

Regulatory regimes are becoming stronger. And regulators are now performing reviews of organisations as part of their annual strategies. In some countries there are strict breach reporting requirements with penalties imposed for non-compliance.

In such a dynamic landscape, an organisation's privacy and data protection framework can quickly become outdated. If they fail, this may not only result in penalties, but also financial loss, loss of consumer trust, and damage to the reputation of an organisation.

How can you prepare?

Your action plan:

- Consider commissioning a privacy health check to understand how your privacy framework stacks up to the expectations of Regulators. Start by completing the checklist on page 26.

"By treating privacy as a complementary service or product feature, rather than a compliance issue, an organisation can build a better relationship with the consumer and make sure that their customers become a key part of building their brand."

Deloitte Privacy Index 2016

Trend 2: Building a sustainable privacy framework

Globalisation has meant it is no longer sufficient to manage privacy and data protection risk as a localised, compliance driven requirement on an ad hoc basis. Risk exposure needs to be continuously monitored to manage organisation, third party, regulator, individual, global and cultural expectations.

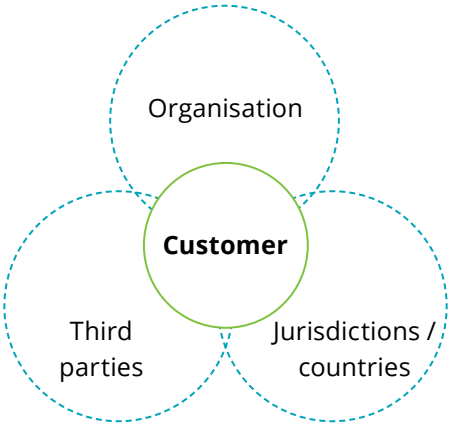
Privacy frameworks need to be resilient and be able to withstand regulatory change, regulator activity and the increased knowledge that individuals are developing about the potential use of their information.

Organisations must be able to adapt and build on their privacy and data protection programs to ensure that they are staying relevant to emerging risks. This will help to build trust not only within organisations, but also externally with consumers to be in line with their expectations.

How can you prepare?

Your action plan:

- Include a privacy and data protection review in your Internal Audit plan
- Implement a process to identify and assess the impact of new regulations or guidelines introduced by jurisdictions.
- Implement a data monitoring program to determine where you data are and monitor where they are moving to within the organisation and to external entities.
- Pro-actively build relationships with regulators outside of your jurisdiction.



Trend 3: Consumers understand more than you think···and are not telling you!

Consumers are learning about the consequences of providing information to organisations – and fast. This is driving organisations to understand and respond in a way that match their expectations.

Notwithstanding cultural differences, a clear similarity between all countries in the APAC region is that individuals rely on technology for all kinds of products and services – we all are in the same boat.

Ignorance of consumer and cultural expectations can cause individuals to be more wary of the information they provide to organisations. This can prevent organisations from achieving the intended strategic and commercial outcomes with the data provided. Individuals want to know that their information is protected. Trust is highly valued and without it, reputation may be compromised not only by the media and advocacy groups, but by those that sustain your organisation financially – your customers.

How can you prepare?

Your action plan:

- Be more transparent with your customers regarding how you use their data.
- Understand your customers perceptions of trust, data use and how far they will allow you to push the boundaries with innovation.
- Implement an external customer education program to manage expectations.

Trend 4: Third and x-party management

Organisations may outsource business functions to a third or even fourth party located in another country. The geographical location of these business functions may influence cultural and regulator sentiment emanating from these locations, and both may need to be key elements in a data protection risk management program.

In some jurisdictions, an "... organisation is responsible for [all] personal information in their custody; a responsibility that extends to those parties with whom the organisation shares such information. This means that organisations which use third parties to perform business functions are increasing their exposure to privacy and data protection risk by engaging with them."[1]

How can you prepare?

Your action plan:

- Assess your third party management program with a specific focus on privacy and breach management
- Obtain verified evidence on whether your third parties are compliant with your organisation's expectations

Trend 5: Overcoming the fear of transparency

There is a reluctance among organisations to be transparent regarding data use for fear of losing customers. It's sometimes perceived that transparency has the potential to draw unwanted attention to issues with an organisation's privacy and data protection framework, or to become a competitive differentiator.

Being clear and candid with your customers is critical to fostering trust, and ensuring customer commitment and growth.

The time taken by organisations to notify customers when information has been misused or compromised has a clear impact on brand perceptions and customer trust. This has been demonstrated by many public examples of breaches across APAC.

How can you prepare?

Your action plan:

- Review the notifications and any communication provided to customers to ensure they are in line with the activities that the organisation may perform using data
- Understand your risk culture – are your staff comfortable reporting breaches or potential changes to customer communications relating to data use?
- Review your data breach response plans to ensure that all relevant individuals can be mobilised to obtain all information required to conduct a risk assessment which the organisation can have confidence in.

1. https://www2.deloitte.com/au/en/pages/risk/articles/third-parties-part-first-line-defence.html

Have you considered...?

Each country in the Asia Pacific region regulates privacy and data protection a little differently. Organisations may need to consider the following:

- ☐ Do you know **how the regulations and regulators** of the country in which you're operating impact on your organisation?
- ☐ **Do you collect or store information that could identify an individual?**
- ☐ **Do you need to notify or receive consent** before collecting or using someone's personal information?
- ☐ Do you need to **consider the restrictions on transferring information across borders**? Some restrictions apply even if you are moving information within your own organisation.
- ☐ Do you **know where** your organisation stores data?
- ☐ Do you **know where your third parties store data**?
- ☐ **Are you transparent with your customers?** Do you tell them how you're managing their information?
- ☐ **Do you have policies** about how you manage personal information, and would they meet the expectations of your customers in each country?
- ☐ **Do you have an action plan** for when a data breach occurs? In some countries it is mandatory to promptly report data breaches to the regulator and to let your customers know what's happened.
- ☐ Is your organisation **ready for a risk culture change**? Consider the places your organisation operates and understand the culture, the changing economy and the impact these can have on staff understanding and behaviour when using personal information.

"...there has never been a more important time to ensure that privacy is built into the fabric of business and into every product and service development. In this era of a data driven economy, where innovation itself relies increasingly on using personal information in new technological contexts, businesses and agencies know that if they go down this path it will be essential that they get privacy right in order for long term success to follow. And privacy is also, very much, an international conversation."

Timothy Pilgrim – Australian Privacy Commissioner
Privacy Awareness Week Business Breakfast,
Sydney, 16 May 2016

Contacts

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
Tel: +61 428 200 542
Email: jamesnunnprice@deloitte.com.au

Marta Ganko
Asia Pacific Thought Leader
Tel: +61 2 9322 3143
Email: mganko@deloitte.com.au

Marta Ganko
Privacy & Data Protection Leader, Australia
Tel: +61 2 9322 3143
Email: mganko@deloitte.com.au

Shree Parthasarathy
Cyber Risk Leader, India
Tel: +91 98 7172 2243
Email: sparthasarathy@deloitte.com

Anu Nayar
Cyber Risk Leader, New Zealand
Tel: +64 2 1207 9573
Email: anayar@deloitte.co.nz

Young Soo Seo
Cyber Risk Leader, South Korea
Tel: +82 2 6676 1929
Email: youngseo@deloitte.com

Tonny Xue
Cyber Risk Leader, Chinese Mainland and Hong Kong
Tel: +86 10 8520 7315
Email: tonxue@deloitte.com.cn

Mitsuhiko Maruyama
Cyber Risk Leader, Japan
Tel: +81 90 6492 3648
Email: mitsuhiko.maruyama@tohmatsu.co.jp

Philip Chong
Data Privacy Leader, Southeast Asia
Tel: +65 6 224 8288
Email: pchong@deloitte.com

Chia-han Wu
Cyber Risk Leader, Taiwan
Tel: +886 2 4051 6888
Email: chiahwu@deloitte.com.tw

Haruhito Kitano
Cyber Risk, Japan
Tel: +81 80 3591 6426
Email: haruhito.kitano@tohmatsu.co.jp

Man Soo Han
Tax and Legal, South Korea
Tel: +82 2 6138 6710
Email: mshan@deloitte.com

Cheryl Khor
Cyber Risk, South East Asia
Tel: +60 3 7610 8888
Email: ckhor@deloitte.com

CQ-026EN-17