A QUICK GUIDE TO PHILIPPINE DATA PRIVACY LAW COMPLIANCE

The Philippines has always had privacy laws – from fundamental pronouncements in the Constitution, to specific protections for bank accounts, private conversations and privileged communications. But it was only in 2012 that a general privacy statute on personal data was enacted. The Data Privacy Act of 2012 ('DPA') was modelled after the EU Data Protection Directive (95/46/EC) (the 'EU Directive'), and a quick glance at the law will show that it adopts terminology and principles common to privacy regimes and policies in other countries.

THE DPA

Republic Act No. 10173 (also known as the Data Privacy Act of 2012) is founded on "the policy of the State to protect the fundamental human right to privacy of communication while ensuring free flow of information to promote innovation and growth...[and] the [State's] inherent obligation to ensure that personal information in information and communications systems in government and in the private sector are secured and protected."

National Privacy Commission

The DPA creates the National Privacy Commission ('NPC'), the agency tasked with administering and implementing the provisions of the act. It is headed by a Privacy Commissioner, assisted by two Deputy Commissioners. It is attached to the Department of Information and Communications Technology, which itself was only created in 2016.

The NPC has the following powers:

- Monitor and ensure compliance with the DPA, as well as the rules and regulations implementing its provisions;
- Receive and resolve complaints and institute investigations;
- Issue cease and desist orders and impose a temporary or permanent ban on personal information processing;
- General authority to compel any entity, public or private, to abide by its orders or to take action in a matter affecting data privacy;
- Recommend the prosecution and imposition of penalties specified in the DPA to the Department of Justice;

Key points

- DPA was modelled after the EU Directive.
- The DPA regulates the collection and processing of personal information.
- Certain types of personal information are considered "sensitive personal information" ('SPI').
- Certain controllers and processors must have their data processing systems registered with the NPC by September 9, 2017.
- Consent is a lawful basis for the collection and processing of both personal information and SPI.
- In light of the growing emphasis on (and extra-territorial effect of) cyber security and data privacy laws across Asia and the EU, multinational corporations (including those operating in, and from, the Philippines) should be vigilant in handling personal data and be aware of the exposure to international regulatory and enforcement risks.

- Provide guidance on the protection of data privacy; and
- Facilitate cross-border enforcement of data privacy laws.

Laws and issuances

Apart from the DPA, which became effective on November 3, 2012, the following NPC issuances should be taken note of:

- Implementing Rules and Regulations (IRR) of the DPA dated August 24, 2016.
- NPC Circular No. 16-01 dated October 10, 2016, which deals with the security of personal data in government agencies.
- NPC Circular No. 16-02 dated October 10, 2016, on data sharing agreements with the government.
- NPC Circular No. 16-03 dated December 15, 2016, on personal data breach management which sets out the requirements for data security breach notification.
- NPC Circular No. 16-04 dated December 15, 2016, which is the NPC's rules of procedure.
- NPC Advisory No. 2017-01 dated March 14, 2017, which provides guidance on the appointment of data protection officers.

It is expected that the NPC will continue to issue a number of new circulars, in efforts to further implement the DPA.

"It is expected that the NPC will continue to issue a number of new circulars, in efforts to further implement the DPA."

Cyber security

Those looking into local cyber security law issues may also wish to take note of a statute enacted the same year as the DPA, Republic Act No. 10175 (also known as the Cybercrime Prevention Act). This aims to promote and protect the security of cyber systems. This law characterises certain acts as offences against the confidentiality, integrity and availability of computer data and systems (e.g. illegal access to the whole or part of any computer system, intentional or reckless alteration or damaging of computer data), computer-related offences (e.g., forgery and identity theft) or content-related offences such as libel committed through a computer system.

DPA in a nutshell

The DPA regulates the collection and processing of personal information, that is, "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can reasonably and directly be ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."

Sensitive personal information

Certain types of personal information are considered "sensitive personal information". SPI refers to information involving matters such as race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations, health, education, genetic or sexual life of a person, or to any proceedings for any offence committed or alleged to have been committed by such person. It also includes personal information issued by government agencies that is peculiar to an individual, such as his or her social security number or licences. In general, the requirements and standards for collecting and processing sensitive personal information are more restrictive and sanctions for breaches involving SPI are graver.

In general, regulation is in the form of:

1. *A requirement that collection and processing of personal data must be pursuant to at least one "criteria for lawful processing".*

The DPA lists these criteria, which among others, include consent of the data subject, fulfilment of contractual or legal obligations, compliance with the requirements of public order and public safety and the protection of the life and health of the data subject. The criteria for the processing of personal information is not the same as those for the processing of SPI, although both types of personal data can be collected and processed where the data subject has given consent.

One other criterion for the processing of personal information is when this 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." This condition is not an available basis for the processing of SPI.

2. *A requirement that personal information controllers and processors adhere to the general privacy principles of transparency, legitimate purpose, and proportionality. The various rules and specific requirements of the DPA could be viewed as arising from one or more of these principles.*

Transparency

- The principle of transparency refers to the duty of personal information controllers and processors to inform data subjects of the nature, purpose, and extent of the processing of their personal data. The principle is reflected in, among others, the rule requiring data subjects to be informed of certain specific information relating to the collection and processing of their personal data, such as, the identity and contact details of the personal information controller or its representative, scope and method of processing, the recipient or classes of recipients of their personal data and the basis of processing of their personal data when they have not provided consent.

Legitimate Purpose

- The principle of legitimate purpose requires that the processing of personal data be "compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy." A rule that reflects this policy is the need for collection and processing of personal data to be pursuant to a criterion for lawful processing.

Proportionality

- The principle of proportionality requires the scope and method of processing personal data to be "relevant, suitable, necessary and not excessive in relation to a declared and specified purpose." An example of a rule that implements this principle is the rule limiting the processing of personal data to only to what is necessary and compatible with the declared and specified purpose, as well as the rule limiting the retention period of personal data to only for as long as necessary.

3. *An obligation to observe the rights of data subjects. These rights are:*

  - Right to be informed whether personal information is being or has been processed, and the content of such personal information;

- Right to reasonable access to personal information;
- Right to dispute and rectify an inaccuracy or error in the personal information;
- Right to object to the processing of personal data;
- Right to suspend, withdraw or order the blocking, removal or destruction of personal data from the personal information controller's filing system;
- Right to damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of personal data;
- Transmissibility of rights of the data subject to his or her lawful heirs or assigns in certain defined cases; and
- Right to data portability.

4. *An obligation to put into place adequate security measures.*

These measures include organisational, physical and technical measures. In terms of organisational measures, personal information controllers and processors are required to appoint a data protection officer, formulate data protection policies and establish a data security breach management team. Physical security measures would include ensuring the privacy of workstations and the implementation of procedures for the transfer, removal, and disposal of data and technical security measures would include the encryption of stored data and regular monitoring for security breaches.

5. *Sanctions for breaches of the DPA, IRR and other issuances of the NPC that may be in the form of a fine or imprisonment or both.*

6. *A requirement to register the controller's or processor's data processing system with the NPC if:*

- The controller or processor has at least 250 employees; or
- The controller or processor has less than 250 employees but:
  - Processing is likely to pose a risk to the rights of a data subject;
  - Processing is not occasional; or
  - Processing includes the SPI of at least 1,000 individuals.

The deadline for existing controllers and processors to comply with this registration requirement is September 9, 2017.

CERTAIN KEY TERMS

Personal information controllers vs. personal information processors

- The DPA makes a distinction between personal information controllers and personal information processors, where the former refers to those who decide on the scope of the information collected, including the purpose or extent of its processing, while the latter refers to those to whom the processing of personal data is outsourced. While processing can be subcontracted, the controller remains responsible for ensuring the confidentiality of data, and can be made liable for damages to a data subject, even if the processor was at fault.

"The deadline for existing controllers and processors to comply with this registration requirement is September 9, 2017."

Consent of a data subject

- Consent is a lawful basis for the collection and processing of both personal information and SPI. Consent is defined as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection or processing of his or her personal data. This may be evidenced by written, electronic or recorded means. Consent may also be given on behalf of data subjects by other persons specifically authorised by them.

Outsourcing vs. data sharing

- The DPA allows the disclosure or transfer of personal data by a personal information controller to a personal information processor for the purposes of outsourcing the processing of personal data (subject to restrictions under other laws). The personal information controller must ensure, through contractual or other reasonable means, that proper safeguards necessary for maintaining the confidentiality, integrity, and availability of personal data are in place.
- Data sharing, on the other hand, refers to an arrangement involving the disclosure of personal data by the controller to a third party, but according to the IRR, and does not cover outsourcing agreements.
- Data sharing is allowed as long as the data subject consents and has been provided with specific information regarding the purpose and extent of data sharing, including the intended recipients or categories of recipients of his or her personal data. Consent is required even when the data is to be shared with an affiliate or mother company, or with others of similar relationships. Data sharing for a commercial purpose, including direct marketing, must be covered by a data sharing agreement, which should establish adequate safeguards for data privacy and security.

Data security breach notification

The NPC and the data subject must be notified when sensitive personal information or any other information (such as, but not limited to, a data subject's biometric data, copies of identification documents, and unique identifiers like the social security number and the taxpayer's identification number) that may be used to enable identity fraud has been acquired by an unauthorised person, and the acquisition is likely to give rise to a real risk of serious harm to the affected data subject. Notification of the data breach should be made within 72 hours upon knowledge of the breach or reasonable belief that it has occurred. Businesses should therefore review and develop their incident response plans to enable them to be agile in responding to data breaches.

A data breach may also trigger notification requirements under other data privacy laws. For example, if the processing arrangement is also caught under the incoming European Union (EU) General Data Protection Regulation (GDPR), data controllers will be required to report all security breaches affecting personal data to their data protection authority without undue delay and, where feasible, within 72 hours of becoming aware of the security breach. Under the GDPR, data processors must inform their controller when they become aware of security breaches affecting personal data.

A rapid response to each data security breach will therefore be required and an international outlook when mapping data breaches will be important.

"Businesses should therefore review and develop their incident response plans to enable them to be agile in responding to data breaches."

Extraterritorial application

In general, the DPA and the IRR apply to the processing of personal data when the entity involved in the processing is found or is established in the Philippines or the processing is done or engaged in the Philippines. The law also applies to the processing of personal data, even if the processing is engaged in or occurs outside of the Philippines, if the personal data involved relates to a Philippine citizen or resident or when the act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines. This might include among others use of equipment located in the Philippines, entering into a contract in the Philippines, or maintaining a branch office or subsidiary in the Philippines while providing access to personal data to the parent or affiliate entity.

To-do List

In various fora, the NPC has identified the compliance steps that controllers and processors should prioritise:

- Appointment of the DPO;
- Conduct of a privacy impact assessment;
- Creation of a data privacy manual (essentially the controllers or processor's procedures, policies and protocols for data protection);
- Implementation of security measures; and
- Readiness in the case of a data security breach.

Application of the law

The DPA and the privacy law regime it creates are relatively new. Many local companies, including affiliates of foreign entities, have questions regarding the obligations and requirements under the law. Until additional guidelines or precedents are created, controllers and processors may need to continue to look to the NPC for direction, or even to "best practices" in other jurisdictions, for guidance in respect of certain compliance issues.

GROWING GLOBAL EMPHASIS ON DATA PRIVACY LAWS

The upcoming developments and recent circulars issued in the Philippines are in line with the growing emphasis on data privacy laws globally.

The GDPR passed in 2016, which will come into effect in less than a year's time, on May 25 2018, represents the biggest change in EU data privacy law in a generation and is likely to form a model for new data privacy rules in other jurisdictions.

The GDPR will significantly extend the extraterritorial effect of the existing EU data protection regime, catching overseas controllers and processors who currently have no expectation that they will be caught by EU law. The GDPR extends the current EU regime so that it also applies to a controller or processor who carries out processing outside of the European Economic Area (EEA) if that processing is carried out in order to offer goods or services to, or monitor the behaviour of individuals within the EEA.

Businesses outside of the EEA (including those in the Philippines) should consider whether the GDPR will apply to them and global organisations should consider whether to apply standards based on the GDPR worldwide.

"Businesses outside of the EEA (including those in the Philippines) should consider whether the GDPR will apply to them."

In other parts of Asia, the new Cyber-Security Law of the People's Republic of China took effect on June 1 2017, and the Singapore Personal Data Protection Commission has taken enforcement action against various organisations for breach of the Singapore Personal Data Protection Act since its data protection provisions came into effect in July 2014.

Multinational corporations operating in the Philippines should therefore be vigilant in handling personal data and be aware of the exposure to regulatory and enforcement risks, in light of the growing emphasis on cyber security and data privacy laws across Asia and the EU.

For further information on this topic please contact the authors below.

Read our other publications

If you would like to receive copies of our other publications on the Philippines or this topic, please email: eddie.hobden@cliffordchance.com

- New EU General Data Protection Regulation (2017)
- GDPR Compliance Checklist (2017)
- New PRC Cyber-Security Law comes into Force (2017)
- Country M&A Handbook – The Philippines (2017)

CONTACTS

Rose Marie M. King-Dominguez
Senior Partner,
SyCipLaw

T +632 982 3500
E rmmking
@syciplaw.com

Paul Landless
Partner
Clifford Chance

T +65 6410 2235
E paul.landless
@cliffordchance.com

Janice Goh
Counsel
Clifford Chance Asia*

T +65 6661 2021
E janice.goh
@cliffordchance.com

Richard Jones
Director of Data Privacy
Clifford Chance

T +44 207006 8238
E richard.jones
@cliffordchance.com

Herbert Swaniker
Associate
Clifford Chance

T +44 207006 6215
E herbert.swaniker
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Sindhorn Building Tower 3, 21st Floor, 130-132 Wireless Road, Pathumwan, Bangkok 10330, Thailand