Rose Marie M. King-Dominguez Partner
rmmking@syciplaw.com
SyCip Salazar Hernandez & Gatmaitan, Makati City

The challenges under the new Philippine data privacy regime

According to Rose Marie M. King-Dominguez, Partner at SyCip Salazar Hernandez & Gatmaitan, as a result of the average citizen in the Philippines reportedly spending about an hour and a half more on the internet than the average user on a global basis, its OOTD-sharing population has helped it earn the unofficial title of social media capital of the world. Personal data in the Philippines appears to be on a digital tap: free flowing and plentiful. Rose Marie examines the impact of the Philippines' new privacy framework in such a world and the challenges it poses for the jurisdiction and for those operating within it.

In a 2014 case[1], the Philippine Supreme Court rejected a Facebook user's claim that her right to privacy (over photos of herself in swimwear) had been violated, observing that the user had lost an expectation of privacy when she failed to properly deploy the platform's privacy tools. The Supreme Court reiterated this view in a more recent case[2] that upheld a lawyer's suspension from the practice of law for his 'Facebook posts maligning and insulting' the complainant, a famous beauty doctor who counted local movie stars as clients.

The Court did not accept the lawyer's argument that the statements were private since he had restricted access to the page to 'Friends Only,' further observing that 'even if the Court were to accept the [lawyer's] allegation that his posts were limited to or viewable by his 'Friends' only, there is no assurance that the same [...] will be safeguarded as within the confines of privacy.' It noted the social media platform's goal of allowing 'the world to be more open and connected [...] in every conceivable way,' the implied message being that a person who shares information on social media shouldn't be surprised or angry if that information actually does get shared.

So is privacy dead in the Philippines? Not quite, and under a new regulatory regime on data protection, perennially connected Filipinos may actually become much more conscious and vigilant about their privacy.

A new privacy regime

Partly in line with the Philippines' agreements under ASEAN Vision 2020 (a plan adopted by members of the Association of Southeast Asian Nations to create an EU-like economic community), partly at the urging of the local business process outsourcing industry, the Philippines passed Republic Act No. 10173 or the Data Privacy Act of 2012 ('DPA'). The DPA 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[3].' Its 'twin' bill (since it aims to promote cyber security), Republic Act No. 10175 or the Cybercrime Prevention Act, was also passed in 2012.

In a nutshell, the DPA:

- Regulates the collection and processing of data that enables identification of individuals;
- Requires that collection and processing of personal data must have a lawful basis or 'criteria for lawful processing,' e.g. consent;
- Requires that personal information controllers and processors adhere to the general privacy principles of transparency, legitimate purpose and proportionality;
- Identifies rights of data subjects that personal information controllers and processors must observe;
- Sets out certain measures and steps that personal information controllers and processors need to comply with; and,
- Sanctions violations of the law.

The DPA was modelled after the Data Protection Directive (95/46/EC) and adopts terminology and principles common to many current privacy regimes and policies.

For example, it makes a distinction between personal information and sensitive personal information, with the latter being data that involves matters such as age, marital status, ethnicity, religion and sexual orientation. The requirements and standards for collecting and processing sensitive personal information are more restrictive.

A distinction is also made between personal information controllers and personal information processors, processors being persons to whom controllers may outsource processing of personal data. But 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 DPA's key touchstones are the principles of transparency ('the data subject must be aware of the nature, purpose, and extent of processing')[4], legitimate purpose ('processing [...] shall be compatible with a declared and specified purpose') and proportionality ('retention of personal data shall only be for as long as necessary')[5] and the DPA reiterates them in specific expressions of principles for collection,

1. *Vivares v. St. Theresa's College*, GR No. 202666, dated 29 September 2014.
2. Belo-Henares v. Guevarra, AC No. 11394, dated 1 December 2016.
3. Section 2, DPA.
4. Section 18(a), IRRs.
5. Section 19(d), IRRs.

processing, retention and data sharing. Prior to the DPA, personal information found protection under general privacy principles set out in the Philippine Constitution, the Civil Code, and the Electronic Commerce Act (Republic Act No. 8792) 2000, as well as a number of rules and policies that tackled specific types of data such as bank accounts, data in electronic form, information about HIV patients, and recordings of conversations. Thus, the DPA is the Philippines' first privacy statute with a general application.

A new regulator

The DPA also creates the National Privacy Commission ('NPC'), the agency tasked with administering and implementing the provisions of the DPA. The NPC is headed by a Privacy Commissioner, assisted by two Deputy Commissioners. It is attached to the Department of Information and Communications Technology ('DICT'), which itself was only created in 2016 or about four years after the enactment of the DPA; this created a kind of legal anachronism since the DPA had provided that the NPC would be attached to the then non-existent DICT.

As for the NPC, it was only formally organised in 2016, and has had to work double-time to put the DPA into effect. The NPC issued implementing rules and regulations ('IRRs') for the DPA on 24 August 2016, as well as four circulars in the last quarter of 2016, including one on personal data breach management, and another on rules of procedure for complaints for violations of the DPA.

DPA to-do list

Those covered by the DPA will also have to work double-time to understand the DPA and how it impacts them.

Apart from needing to adopt and observe the basic regulatory framework of the DPA so that, for instance, persons that regularly collect and use personal data from employees, customers, suppliers, site browsers, etc. must now be mindful that this is done with consent, these persons may also have to:

- appoint a Data Protection Officer who will be accountable for ensuring compliance with the DPA;
- adopt data protection policies that provide for organisation, physical, and technical security measures (including a policy for security incident management);
- create a data breach response team to ensure timely action in the event of a security incident or personal data breach;
- document outsourcing and data sharing arrangements to comply with DPA requirements; and
- register data processing systems ('DPS') operating in the Philippines with the NPC.

In respect of the registration requirement, not all controllers or processors with a DPS operating in the Philippines need to comply. A person with fewer than 250 employees need not register their DPS unless (a) the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, (b) the processing is not occasional, or (c) the processing includes sensitive personal information of at least 1,000 individuals. The IRRs provides a period of one year from the rules' effectivity (or until 9 September 2017) to comply with the registration requirement.

NPC Circular No. 16-03, dated 15 December 2016, provides the details for a data breach notification requirement. Notification of the NPC and the data subject is generally required when the data breach involves sensitive personal information or any other information that may be used to enable identity fraud, this information 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 should be done within 72 hours upon knowledge of the breach or reasonable belief that it has occurred.

Compliance challenges

With the IRRs and the DPA's principal implementing agency not even a year old, the regulated and the regulator face more than a few challenges. With no real precedents to provide guidance, and circulars still being issued to manage gaps in the DPA and the IRRs, many controllers and processors are struggling to understand how to comply with the new regime.

For instance, persons with less than 250 employees and who do not process the sensitive personal information of 1,000 individuals will need to figure out what is meant by 'processing that is likely to pose a risk to rights and freedoms of data subjects' and 'processing that is not occasional.' This will surely create many grey areas.

Meanwhile, non-resident entities with Philippine dealings may be surprised to find out that they are covered by the DPA and its requirements. The DPA provides that it applies to processing even outside the Philippines if the processor has a 'link' to the country, such as the processing of personal data of Philippine citizens or residents.

But beyond the challenges of practical comprehension and compliance is that of creating a 'privacy mindset.' At present, discussions even with top executives and senior officers of local companies about the DPA can include dealing with denial/amazement at what the statute requires, and even doubts about whether the DPA is actually already in force (the NPC confirms that it is).

Even the Philippine Commission on Elections ('COMELEC'), a body created by the Constitution to manage elections and voter registration, expressed dismay that the NPC was focusing its regulatory ire on the COMELEC in relation to a 2016 leak of personal data of millions of registered voters. Its Chairman, who may face criminal liability under the DPA, has argued that the focus should be on the hackers and not the victim of the hacking.

A Filipino word for privacy

Some of the larger corporates, and those affiliated with global companies that operate in jurisdictions with mature privacy regimes, should have less problems with DPA compliance. The NPC in the meantime has sought to assure businesses and organisations that its priority at this time will be to educate, guide and encourage compliance; in one forum, a Commissioner said that the NPC's focus is not to "jail people." But companies that are anxious about the NPC's monitoring function and punitive powers may need to be more concerned about a possible rise in privacy violation complaints. With the NPC having issued rules of procedure for such claims and a growing awareness of privacy rights under the DPA and the IRRs, it may only be a matter of time before Philippine data subjects take those rules of procedure out for a spin. Early this year, at least two bills were filed seeking to regulate social media. With these developments, it is not clear if, for instance, courts will continue to put the onus of privacy protection on the data subject as seems to have been the case in recent Supreme Court decisions. While, as noted by the NPC's website, there is no Filipino word for privacy, this could very well change as the Philippines' new privacy regime begins to mature.