PHILIPPINES' PUTS KEY PRIVACY RULES IN PLACE BUT NPC FACES PRESSURE

GRAHAM GREENLEAF

(2016) 143 *Privacy Laws & Business International Report*, 19---21, October 2016

[2017] *UNSWLRS* 8

UNSW Law
UNSW Sydney NSW 2052 Australia

Philippines' puts key privacy rules in place but NPC faces pressure

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*
(2016) 143 *Privacy Laws & Business International Report*, 19-21, October 2016

Philippines' President Rodrigo Duterte, in office since June 30 2016, acquired a reputation as a provincial politician for supporting extra-judicial killing of alleged drug dealers, and promised during the Presidential election campaign that 'fish will grow fat' in Manila Bay from feasting on their corpses. During his first ten weeks in Presidential office, over 1,800 people were killed, apparently by either police or vigilantes.[1]

At the same time, the Philippines's new National Privacy Commission (NPC), only appointed in March 2016,[2] took swift steps to bring the Philippines *Data Privacy Act* (DP Act), dormant since enactment in 2012, into force. On 25 August 2016 it issued the finalized *Implementing Rules and Regulations* (IRRs) necessary for the Act to become effective. However, three days before the NPC issued the IRRs, Duterte purported to require the resignation of all its members.

This article provides a brief account of the effect of the IRRs on the *Data Privacy Act*, the NPC's issuing of data breach notification rules (its other most significant actions to date), and the implications of the attempted forced resignation of the Commission members.

Implementing Rules and Regulations finalized

The NPC issued the *Implementing Rules and Regulations* (IRRs)[3] on 24 August 2016, after consultations with interest groups, to take effect 15 days after publication (9 September 2016). Business and government agencies required to comply with the Act are given one year from this effective date to comply with the registration requirements under the IRRs. All other provisions of the IRRs are effective from 9 September 2016.

The Act does not specify what matters the IRRs must cover. The 49 pages of the IRRs repeat (in somewhat different wording) much of the content of the relatively short Act, making it difficult to disentangle precisely which aspects the IRRs merely paraphrase the Act, which clarify its meaning, which add more details to its implementation, and which (arguably) add substantive new obligations not found in the Act.

It is arguable that the IRRs do add some substantive new obligations (but fewer or less onerously than the draft IRRs), in such areas as requirements for data sharing agreements to

* Valuable comments and permission to cite observations have been received from data privacy legal practitioners in the Philippines. All content remains the responsibility of the author.

[1] Amanda Taub 'How countries like the Philippines fall into vigilante violence' *International New York Times*, 13 September 2016, p3.

[2] G Greenleaf 'Philippines appoints Privacy Commission in time for massive electoral data hack' (2016) 141 *Privacy Laws and Business International Report*, 22-23

[3] National Privacy Commission 'Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" ', 24 August 2016 <http://www.gov.ph/2016/08/25/implementing-rules-and-regulations-of-republic-act-no-10173/>

be approved by the NPC, and a right for data subjects to object or withhold consent to processing, particularly in relation to direct marketing, automated processing or profiling.[4]

The IRRs also add many other essential details as to how the Act will operate. For example, personal data processing systems operating in the Philippines that involve the processing of personal information concerning at least 1,000 individuals must be registered with the NPC, with a deadline of 9 September 2017 (unless an extension is granted). Controllers or processors that employ less than 250 persons are generally exempt from the registration requirement, subject to certain conditions.[5] Such registration requirements are now very unusual in Europe or in other countries with data privacy laws (Malaysia is an exception).

It is beyond the scope of this brief article to compare the entirety of the Act[6] and the IRRs, in order to establish exactly what matters of substance, or of procedural detail, are added by the IRRs, but those who have to comply with the Act must undertake such a comparison.

Data breach notification Rules issued

Prior to issuing the IRRs, the NPC also issued a draft *Rules of Procedure for Data Breach Notification and Other Responsibilities*.[7] Breaches only require notification, consistent with s.20(f) of the Act, if three conditions are satisfied:

> "1. The compromised data involves sensitive personal information or other information that may be used to enable identity fraud;
> 2. There is reason to believe that the information may have been acquired by an unauthorized person; and
> 3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject."

The Rules set out in detail the following matters:

- That data controllers are responsible for notification, even if outsourced processors suffer the breach, and for ensuring that they are informed.
- That the NPC should be informed within 72 hours of knowledge or reasonable belief, and the conditions for any permitted delays.
- That data subjects should be notified within 72 hours is 'likely to result in a high risk' to them, and the conditions on which the NPC may grant exemptions on public interest grounds.
- The content of the notifications to both the NPC and to data subjects, and the means by which it must be done.
- That, after investigating a breach, the NPC 'may award indemnity, issue cease and desist orders, issue a temporary or permanent ban on the processing of personal data, recommend criminal prosecution, impose fines and penalties in accordance with applicable law or rules, or issue orders directing any further action'.

---

[4] Hunton and Williams 'Final Rules for the Data Privacy Act Published in the Philippines', 13 September 2016 < https://www.huntonprivacyblog.com/2016/09/13/final-rules-data-privacy-act-published-philippines/>

[5] B Marquez III, D Ilas-Panganiban and N Pascual 'Final Rules and Regulations Implementing the Data Privacy Act Released, Taking Effect on 9 September 2016', Quisumbing Torres / Baker & McKenzie, September 2016 <http://www.bakermckenzie.com/-/media/files/insight/publications/2016/09/final-rules-and-regulations/al_ph_finalrulesregulations_sep16.pdf?la=en>

[6] For analysis of the Act prior to the IRRs, see 'The Philippines and Thailand—ASEAN's incomplete comprehensive laws', Chapter 12 of G. Greenleaf *Asian Data Privacy Laws: Human Rights and Trade Perspectives*, OUP, 2014.

[7] Rules of Procedure for Data Breach Notification and Other Responsibilities, NPC Circular 16-001, 10 June, 2016

These Rules establish that notification of data breaches is now a serious responsibility, of international standard, for all businesses coming within the scope of the Act. The later-issued IRRs in Rule IX also deal with data breach notifications, but only in a form which is consistent with but more brief than these Rules. These Rules therefore must continue to be considered, although the NPC has yet to clarify on when these Rules are to become effective, assuming that they have not been superseded by the IRRs.

Duterte's attempted forced resignation of the Privacy Commissioners

On 22 August President Duterte issued a Memorandum Circular entitled (with some irony) 'Courtesy Resignation of Presidential Appointees'.[8] 'In view of the President's desire to rid the bureaucracy of corruption, and to give him a free hand in achieving this objective, all presidential appointees are hereby directed to tender their unqualified courtesy resignations within seven (7) calendar days from date hereof…' it stated, and then listed six categories of exceptions.

However, it then stated that, although resignations were to be tendered to an officer's superior, only the President may act on them. Until that happens, such officials 'shall continue to report for work and perform their normal duties and responsibilities.' The Circular threatens that 'Any presidential appointee covered by the Memorandum Circular who fails or refuses without a valid reason to tender his or her courtesy resignation within the period stated above may be held administratively liable and meted the appropriate penalty.' This could be described (with appropriately bloody metaphors) as a 'Sword of Damocles' requirement, whereby officials are required to empower the President to cut off their heads at any time, at his discretion, rather then being required to fall on their swords immediately.

Some data privacy practitioners from the Philippines[9] are of the view that none of the six exemptions in the Circular benefit any of the three incumbent NPC Commissioners, because they are, under civil service law, classified as non-career officials. It is not known whether any of the Commissioners have tendered their resignations. However, it is their opinion of some Philippine legal practitioners that presidential appointees affected by this directive, including the Privacy Commissioners, may have valid grounds to challenge the constitutionality of the Circular because the Philippine Constitution provides that "No officer or employee of the civil service shall be removed or suspended except for cause provided by law" (Section 2(3) Article IX-B). This guarantee of security of tenure, they say, extends to all government employees, regardless of classification, such that removal from service may only be for just cause and upon observance of due process (see *Jocom vs. Regalado*, Philippine Supreme Court, G.R. No. 77373, August 22, 1991). The NPC commissioners are therefore protected from removal from office during their 3-year term fixed under Section 9 of the Data Privacy Act, unless due to their commission of any of the offenses enumerated by the Administrative Code of the Philippines. The president's issuance of a directive for mass dismissal is not one of the authorized grounds.

There are few if any parallels to this situation in the nearly fifty years of world-wide experience of data protection authorities, particularly since various guarantees of independence of DPAs became common – some of which guarantees appear in the Philippines' *Data Privacy Act*. Hungary's purported replacement of its DPA, which was found invalid by the European Court of Justice, is a rare instance.[10] Whether the International

[8] Memorandum Circular No. 4, s. 2016 <http://www.gov.ph/2016/08/22/memorandum-circular-no-4-s-2016/>

[9] Quotations following from these practitioners are not identified in this article due to the complex current situation in the Philippines.

[10] *Commission v Hungary* ECLI:EU:C:2014:237 (08/04/2014) <http://curia.europa.eu/juris/documents.jsf?num=C-288/12>. For summaries, see <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140053en.pdf> and <http://europa.eu/rapid/press-release_MEMO-14-267_en.htm>.

Conference of Data Protection and Privacy Commissioners (ICDPPC), the Asia-Pacific Privacy Authorities (APPA), or the various associations of privacy enforcement agencies (PEAs) will admit the NPC to membership under such circumstances is not known. Such factors are likely to have no effect on Duterte, but might send a significant signal to businesses considering outsourcing to the Philippines.

Conclusions

In the context of Duterte's contempt for both human life and the rule of law, it may seem something of a side-show to be considering a lesser-order human right such as data privacy. However, businesses across the world are using the Philippines for outsourced data processing, and many may do so on the assumption that the Philippines has effective (or at least operative) data privacy laws, plus at least some adherence to the rule of law. All businesses using or considering data processing in the Philippines need to understand fully the contexts in which their work is being carried out, and consider the implications.

On the one hand, the actions of the NPC in carrying out their statutory duties promptly and thoroughly under such uncertainty must be commended and supported, but at the same time their enforcement of the Act will need to be kept under close scrutiny until it becomes clear that the Philippines does in fact have a functioning Data Privacy Act.