Quisumbing Torres.
Member Firm of Baker & McKenzie International

Client alert

Intellectual Property & Information Technology
Manila | March 2017

CLIENT ALERT:

A Call for Action: Data Processing Systems Registration Due in 6 Months

Data controllers and processors operating personal data processing systems in the Philippines should by now, at the very least, have commenced steps to comply with the registration requirement under the Implementing Rules and Regulations ("DPA Implementing Rules") of the Data Privacy Act of 2012, due on **9 September 2017**. Full compliance with the DPA Implementing Rules may not be achieved easily in a day. Failure to comply with the DPA Implementing Rules may mean not only mandatory business closure for the controller and processor, but also payment of damages and of steep fines. For responsible officers and employees, non-compliance by their organizations may even result in imprisonment.

Registration Requirement

Data processing systems operating in the Philippines and processing the sensitive personal information[1] of at least 1,000 individuals, whether it be of employees, clients, customers, or contractors, are required to register with the National Privacy Commission ("NPC").[2] The NPC's rules on said registration, expected to be issued within this March, shall require the following at a minimum:

- Proof of appointment of a Data Protection Officer (DPO);
- Privacy Impact Assessment (PIA) for each covered process;
- Privacy and data protection policies;
- Proof of data privacy training awareness within the applicant's organization;
- Description of each data processing system and of the manner of processing; and
- Data handling practices within the applicant's organization.

Substantive Compliance Matters

While covered controllers and processors are given a grace period of until 9 September 2017 within which to register their systems with the NPC, compliance with the substantive provisions of the Data Privacy Act of 2012 of all personal data controllers and processors is not given the same leniency. In fact, the NPC has recently ruled that the general obligation to comply with the principles of transparency, legitimacy of purpose, and proportionality enshrined by the Data Privacy Act of 2012, including the appointment of a Data Privacy Officer and the implementation of organizational, physical, and technical security measures in the processing of personal information, should have been complied with no later than 8 September 2013. As stated in *In Re: Investigation of the Data Breach Involving COMELEC Website and/or Data Processing System* (NPC Case No. 16-001, 28 December 2016):

> This Commission has the legal duty, therefore, to rule, as it rules in this matter, on the proper grace period for compliance with the Data Privacy Act of 2012; the grace period expired in 2013, or one year following the passage of the Data Privacy Act of 2012. This section has to be strictly construed being an exception to the general rule under Section 45 of the Data Privacy Act providing for the effectivity of the law. The use of the *term requirements* under Section 42 should be taken to mean formal requirements that could not be complied with unless specific details are supplied. This has to be distinguished from the general obligations under the Data Privacy Act, as provided in Section 11 —
>
> > SEC. 11. *General Data Privacy Principles*. - The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Formal Issuances by the National Privacy Commission

To date, the NPC has released four (4) memorandum circulars, all geared towards implementing and enforcing the Data Privacy Act of 2012. The first two (2) memorandum circulars apply to the processing of personal data in the public sector.[3] The two other circulars are as follows:

NPC Circular 16-03 on Personal Data Breach Management lays down the compliance obligations as regards data breach notification and requires, among others, the constitution by data controllers and processors of a data breach response team.[4]

The rules of procedure in instituting complaints with, or requesting advisory opinions from the NPC, were promulgated through NPC Circular 16-04 on the Rules of Procedure of the National Privacy Commission. Under said rules, the NPC may, on its own initiative, institute an investigation against any data controller or processor, including the on-site examination of systems and procedures.[5] The rules on procedure also grants the NPC to order a controller or processor temporarily and/or permanently cease from processing personal information.[6]

Actions to Consider

Considering the looming deadline for the registration of data processing systems with the NPC and more importantly, of the currently effective obligation imposed on all personal information controllers and processors to comply with the provisions of the Data Privacy Act of 2012, clients are advised to immediately act as regards their processing of personal information and take the following specific measures:

- Appoint a Data Protection Officer;
- Conduct an organization-wide Privacy Impact Assessment;
- Implement a Privacy Management Program;
- Develop and employ organization, physical, and security measures; and
- Install and implement a breach reporting system.

Quisumbing Torres' IP/IT lawyers are ready to assist and advice on your data privacy compliance matters.

[1]DPA Implementing Rules I, Section 3(t). Sensitive personal information refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

4. Specifically established by an executive order or an act of Congress to be kept classified.

[2]Rule XI, **Section 46. *Enforcement of the Data Privacy Act***. Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the following:

a. Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;

xxx xxx xxx

[3]NPC Circular 16-01 (Security of Personal Data in Government Agencies) and NPC Circular 16-02 (Data Sharing Agreements Involving Government Agencies).

[4]NPC Circular 16-03, Rule II, Section 5.

[5]NPC Circular 16-04, Rule IV, Section 23.

[6]NPC Circular 16-04, Rule III, Sections 19 and 20.

Contact us

Bienvenido A. Marquez III
Partner
Intellectual Property
Practice Group
Bienvenido.Marquez
@quisumbingtorres.com

Divina V. Ilas-Panganiban
Partner
Intellectual Property
Practice Group
Divina.Ilas-Panganiban
@quisumbingtorres.com

Neonette E. Pascual
Associate
Intellectual Property
Practice Group
Neonette.Pascual
@quisumbingtorres.com