The Data Privacy Act and the National Privacy Commission's Five Pillars of Compliance

Ivy D. Patdu[*]
Jamael A. Jacob[**]

---

* '09 J.D. *with honors*, Ateneo de Manila University School of Law; '02 M.D., University of the Philippines College of Medicine. The Author is the Deputy Privacy Commissioner of the National Privacy Commission and a member of the National Health Data Privacy Experts Group of the National eHealth Program. The Author's previous works published in the *Journal* include *Medical Negligence*, 61 ATENEO L.J. 997 (2017); *Hospital Liability*, 55 ATENEO L.J. 219 (2010); & *Physician and Hospital Liability in Cases of Medical Negligence: A Comment on Professional Services, Inc. v. Agana*, 52 ATENEO L.J. 219 (2007). She was also a co-author of *Filiation and Legitimacy*, 52 ATENEO L.J. 356 (2007) with Atty. Estelito P. Mendoza and *The Legal Concept of Terrorism under International Law and Its Application to Philippine Municipal Law*, 51 ATENEO L.J. 4 (2007) with Dean Sedfrey M. Candelaria and Atty. Vera M. De Guzman-Ocfemia.

** '15 LL.M, *First Class Honors*, University of Auckland Law School; '07 LL.B, University of the Philippines College of Law. The Author is the Data Protection Officer of the Ateneo de Manila University. He served as OIC-Director IV of the Privacy Policy Office of the National Privacy Commission, and has been working in the field of data privacy since 2011.

Cite as 63 ATENEO L.J. 120 (2018).

I. DATA PRIVACY ACT

A. Right to Privacy

One of the popular definitions of the right to privacy is the "right to be let alone."[1] Speaking through his dissent in *Olmstead v. United States*,[2] Justice Louis Brandeis of the United States Supreme Court declared the right to privacy as the "most comprehensive of rights[ ] and the right most valued by civilized men."[3] While the rights to life, liberty, and property are rights almost universally encoded in the fundamental laws of most nations, a similar accord is not given to the right to privacy.[4]

Under the Philippine Constitution, the explicit mention of privacy in the Bill of Rights is found only in the context of privacy of communications.[5] Nonetheless, this should not detract from its value.[6] It has,

1. Olmstead v. United States, 277 U.S. 438, 478 (1928) (J. Brandeis, dissenting opinion).
2. *Id.*
3. *Id.*
4. For example, it was only in 2017 when the Supreme Court of India recognized the right to privacy as an intrinsic part of the right to life and liberty in its decision. *See* Justice K.S. Puttaswamy (Retd) v. Union of India and Ors. K.S. Puttaswamy v. Union of India, 10 SCC 1 (2017) (India).
5. PHIL. CONST. art III, § 3.
6. In the proposed Federal Constitution of the Philippines, the Bill of Rights specifically recognizes privacy as a right, and includes provisions on data protection. A copy of the proposed Federal Constitution is accessible at the website of the Philippine Daily Inquirer. *See* Julius N. Leonen, DOWNLOAD: The Complete Final Draft of the Federal Constitution, *available at* http://newsinfo.inquirer.net/1008581/download-the-complete-final-draft-of-the-federal-constitution (last accessed Aug. 31, 2018).

   Sections 3 and 4 of Article III provide —

   > SECTION 3. The right of persons to privacy shall be inviolable. Without lawful court order, all interference in personal and domestic relations, correspondence, and data are proscribed.
   >
   > SECTION 4. Data obtained about a person shall be used and processed only for purposes authorized by law.
   >
   > A person has the right to inquire from any government office or agency the information or data that has been obtained, stored, or processed about himself, and to demand[ ] that such data and information be corrected or deleted, or in case of a private entity or person, that their use be enjoined.

after all, long been recognized as a fundamental right in the domestic milieu. In *Morfe v. Mutuc*,[7] decided in 1968, the Supreme Court declared that "[t]he right to privacy as such[,] is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection."[8]

The right is insidious, pervading the core of liberty and individuality, and is situated "at the crucible of the Bill of Rights, supporting the right of persons to life, liberty and property, due process, the right of the people to be secure in their persons, houses, papers, and effects[,] and the right against self-incrimination."[9] As for freedom of speech and of the press, freedom of religion, freedom of movement, and freedom of association, their full enjoyment depends on freedom from unwarranted government intrusions, and a guarantee that individuals are entitled to a reasonable expectation of privacy in their personal lives.[10]

In 2012, the Data Privacy Act (DPA) of the Philippines was enacted into law.[11] It covers one important aspect of privacy, that of informational privacy. "Informational privacy" has been described as

> [t]he individual's ability to control the flow of information concerning or describing him [or her], which[,] however, must be overbalanced by legitimate public concerns. To deprive an individual of his [or her] power to control or determine whom to share information of his [or her] personal details would deny him [or her] of his [or her] right to his [or her] own personhood.[12]

The law applies to the "processing of all types of personal information and to any natural and juridical person involved in personal information processing,"[13] except for specific information outside its scope,[14] and the

---

Id. at 9.

7. Morfe v. Mutuc, 22 SCRA 424 (1968).

8. *Id.* at 444.

9. Ivy D. Patdu & Rasiele Rebekah DL. Rellosa, *Data Privacy Act*, 5 BEDAN REV. 1, 80 (2017).

10. *Id.*

11. An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating For this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

12. Kilusang Mayo Uno v. Director-General, National Economic Development Authority, 487 SCRA 623, 680 (2006).

13. Data Privacy Act of 2012, § 4.

limitations to its extraterritorial application.[15] With its enactment, protection of personal information effectively became a national policy and an enforceable obligation.

The DPA declares that "[i]t is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth."[16] This is an express recognition of the comparable significance of the right to privacy and the free movement of information to the country. The law assures that data protection shall not prevent people from obtaining the benefits of personal data use, while emphasizing the responsibility and obligations that arise from such use.

B. Personal Information

Personal information refers to any information about an identified or identifiable natural person.[17] Information that pertains to juridical persons is outside the ambit of protection provided by the DPA.[18] While a person's name constitutes personal information,[19] a name is not always necessary to identify a person. Where a medical abstract simply has the name of a patient redacted, the document remains to be personal information because of the presence of other identifiers that may include hospital number, address, specific dates of admission, hospital procedures, and discharge. At the same time, there are also instances when the name of an individual will be insufficient to ascertain his or her identity. For example, additional information may be required to determine the identity of a person with the name "Michael Santos." Consequently, what is necessary is that the information under consideration makes the identity of an individual apparent, which may require using other available information to directly and certainly identify an individual.[20]

14. *Id.*

15. *Id.* § 6.

16. *Id.* § 2.

17. *Id.* § 3 (g).

18. *Id.*

19. Data Privacy Act of 2012, § 3 (g).

20. *Id.* § 2 (g).

In a recently decided case, *Patrick Breyer v. Germany*,[21] the Court of Justice of the European Union ruled that a dynamic internet protocol address (IP address) may be considered personal data.[22] It explained that

> a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data[,] which the internet service provider has about that person. [23]

This means that the holder of the information becomes part of the consideration. Information is deemed personal information to the extent that the holder of the information can directly or reasonably ascertain the identity of the individual.[24] The use of "reasonably" implies that the identification must be possible without need of extraordinary means, as evaluated based on the probability, difficulty, and potential of identification, including the required time, cost, and skill to ascertain identity.[25] According to the case of *Patrick Breyer*, the additional information may be from other sources, and not necessarily limited to that which the entity holds. [26]

The law distinguishes between personal information, in general, and personal information, which, by its nature, are considered sensitive personal information.

The categories of sensitive personal information include the following:

(a) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical[,] or political affiliations;

(b) 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(c) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or

21. Patrick Breyer v. Bundesrepublik Deutschland, Judgment, ECLI:EU:C:2016:779, ¶ 65 (1) (CJEU Oct. 19, 2016).

22. *Id.* ¶¶ 1-2 & 32.

23. *Id.* ¶ 49.

24. Data Privacy Act of 2012, § 3 (g).

25. Working Party, Opinion 4/2007 on the concept of personal data, WP 01245/07/EN, WP 136 (2007).

26. *Patrick Breyer*, ECLI:EU:C:2016:779, ¶ 44.

current health records, licenses or its denials, suspension or revocation, and tax returns; and

(d) Specifically established by an executive order or an act of Congress to be kept classified. [27]

The law also covers privileged information, which refers to "any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication."[28] The processing of sensitive personal information and privileged information is generally prohibited. [29] The standard of protection they need to be afforded with is more rigorous, there being a separate chapter in the DPA that prescribes the responsibilities of the government when securing sensitive personal information.[30]

Where a violation of the law involves sensitive personal information, the penalties are also higher.[31] The distinction is also important because when sensitive personal information is involved in a personal data breach, the incident may be subject to the mandatory notification requirements of the DPA.[32]

In the law's Implementing Rules and Regulations (IRR),[33] the term "personal data" is introduced to refer to all types of personal information.[34] The National Privacy Commission (NPC), as the agency primarily tasked with the implementation of the law, takes this to mean all three classes of information introduced in the DPA: personal information, sensitive personal information, and privileged information.[35]

C. Processing

27. Data Privacy Act of 2012, § 3 (l).

28. *Id.* § 3 (k).

29. Data Privacy Act of 2012, §§ 3 (k) & (l).

30. *Id.* ch. VII.

31. *See* Data Privacy Act of 2012, ch. VIII.

32. *Id.* § 20 (f).

33. National Privacy Commission, Rules and Regulations Implementing Data Privacy Act of 2012, Republic Act No. 10173, Known as the "Data Privacy Act of 2012" (2016).

34. *Id.* § 3 (j).

35. *See* National Privacy Commission, Various Queries Regarding the Implementing Rules And Regulations (IRR) of the Data Privacy Act (DPA) of 2012, Advisory Opinion No. 018, Series of 2017 (Apr. 21, 2017).

Processing is defined broadly under the DPA, and refers to almost any action performed on personal data, including collection, storage, retrieval, use, and destruction.[36] The law will apply whether the processing involves personal data in electronic systems or paper records.[37] It also governs personal data processing carried out by entities who, "although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch[,] or agency in the Philippines."[38] Specifically, it shall apply if:

> (a) The act, practice[,] or processing relates to personal information about a Philippine citizen or a resident;
>
> (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
>
> (a) A contract is entered in the Philippines;
>
> (b) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
>
> (c) An entity that has a branch, agency, office[,] or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
>
> (c) The entity has other links in the Philippines such as, but not limited to:
>
> (a) The entity carries on business in the Philippines; and
>
> (b) The personal information was collected or held by an entity in the Philippines.[39]

D. Personal Information Controllers and Personal Information Processors

Those involved in personal information processing are referred to in the DPA as either a Personal Information Controller (PIC) or a Personal Information Processor (PIP), or both, as determined by attendant circumstances.[40] Whether a natural or juridical person is a PIC or PIP depends on the personal information and the context by which such data is

36. Data Privacy Act of 2012, § 2 (j).

37. *Id.*

38. *Id.* § 4.

39. *Id.* § 6.

40. *Id.* § 3 (h) & (i).

processed.[41] Where the entity controls the purpose and means by which personal data is processed, on the one hand, the entity will be a PIC with respect to that particular dataset.[42] This includes instances where the PIC instructs another person to process the personal data on its behalf.[43] For instance, an employee of a PIC who processes personal data as part of his or her duties under his or her terms of employment is processing said personal data on behalf of the PIC, which, in this instance, pertains to the company, in its capacity as his or her employer. An individual who processes personal information in connection with his or her personal, family, or household affairs is, by provision of law, not considered a PIC.[44]

On the other hand, a PIP "refers to any natural or juridical person qualified to act as such under [the DPA] to whom a [PIC] may outsource the processing of personal data."[45] While it is unclear where the qualifications for a PIP is provided in the DPA, a PIP is generally one that processes personal data under contract with a PIC, and does not have actual control over the processing.[46] An example would be a business process outsourcing (BPO) company to whom a PIC may outsource particular aspects of its personal data processing activities. The BPO would be considered a PIP with regard to the personal data it processes for the PIC. In fact, its core activity makes the BPO a PIP. At the same time, however, it should be noted that as far as its ancillary activity of processing the personal data of its employees is concerned, the BPO is also a PIC.

The distinction is important because the PIC is primarily accountable for the protection of the personal data it processes, whether by itself, through its employees, or through its agents, as in the case of a PIP under a proper outsourcing agreement.[47] In the case of the latter, the PIC must ensure that proper safeguards are in place for personal data protection even if it has transferred the personal data to a third party for processing.[48] The PIC also retains the obligation for mandatory breach notification even if a breach

41. Rules and Regulations Implementing Data Privacy Act of 2012, § 3 (m) & (n).

42. *Id.*

43. *Id.*

44. Data Privacy Act of 2012, § 3 (h) (2) & Rules and Regulations Implementing Data Privacy Act of 2012, § 3 (m) (2).

45. Data Privacy Act of 2012, § 3 (i).

46. *Id.*

47. *Id.* § 20.

48. Data Privacy Act of 2012, §§ 14 & 21 & Rules and Regulations Implementing Data Privacy Act of 2012, §§ 43 & 47.

occurs while the affected personal data is in the custody of a PIP.[49] It is for this reason that the DPA requires the PIC to use contractual or other reasonable means to ensure that its PIP maintains a comparable level of data protection.[50]

Nonetheless, it is worth remembering that the DPA does provide that PIPs should still comply with all its requirements and that of other applicable laws.[51] This means that, in cases of a violation of the DPA, both the PIC and its PIP can be liable, if so determined by the surrounding circumstances.

As a general rule, a natural or juridical person acting as PIC or PIP has obligations under the DPA for personal data protection.[52] These obligations include meeting the conditions for the processing of personal data, specifically, adherence to the general data privacy principles and the criteria for lawful processing.[53] The DPA likewise mandates the implementation of reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information.[54] The law also includes a declaration of the rights of data subjects,[55] which must be upheld, except for few specific instances.[56]

These obligations are sanctioned by law, such that a violation could constitute a criminal offense. The law further clarifies that if the offender is a corporation, partnership, or any juridical person, the penalty shall be imposed upon the responsible officers who participated in, or by their gross negligence, allowed the commission of the crime, whichever is applicable.[57] As for the entity itself, the DPA provides that the court may "suspend or

49. Data Privacy Act of 2012, § 20 (f) & Rules and Regulations Implementing Data Privacy Act of 2012, § 38.

50. Data Privacy Act of 2012, § 21 (a) & Rules and Regulations Implementing Data Privacy Act of 2012, rule XII.

51. Data Privacy Act of 2012, § 14 & Rules and Regulations Implementing Data Privacy Act of 2012, § 45.

52. *See* Data Privacy Act of 2012, § 3 (h) & (i) & Rules and Regulations Implementing Data Privacy Act of 2012, § 3 (m) & (n).

53. Data Privacy Act of 2012, §§ 11-13 & Rules and Regulations Implementing Data Privacy Act of 2012 §§ 21-23.

54. Data Privacy Act of 2012, §§ 20 & 22-24 & Rules and Regulations Implementing Data Privacy Act of 2012, §§ 25 & 30-33.

55. Data Privacy Act of 2012, §§ 16-18 & Rules and Regulations Implementing Data Privacy Act of 2012, §§ 6-7.

56. Data Privacy Act of 2012, § 19.

57. *Id.* § 34 & Rules and Regulations Implementing Data Privacy Act of 2012, § 61.

revoke any of its rights" under the law.[58] With these, the DPA forms part of the recent wave of laws that actually imposes a criminal penalty on juridical persons, although by express provision, the penalty will be imposed on the "responsible officer."[59]

E. National Privacy Commission

For purposes of administration and implementation of the DPA, as well as compliance of the country with international standards set for data protection, the law created the National Privacy Commission (NPC), an independent body with both rule-making and quasi-judicial powers.[60] The Commission was formally established in 2016 with the appointment of its three (3) original members.[61]

II. FIVE PILLARS OF COMPLIANCE

The NPC developed the so-called "Five Pillars of Compliance" as a means of introducing the basic obligations imposed by the DPA on those engaged in personal data processing.[62] While the requirements of the law and other issuances of the Commission can be operationalized using a more detailed "Accountability and Compliance Framework,"[63] the *Five Pillars* provide a simpler means of appreciating the law's cornerstone principles of compliance, namely: (1) Designation of a Data Protection Officer;[64] (2) Conduct of a Privacy Impact Assessment;[65] (3) Maintenance of a Privacy Management Program; [66] (4) Implementation of Data Privacy and Data Security

58. Data Privacy Act of 2012, § 34.

59. *Id.*

60. Data Privacy Act of 2012, § 7.

61. *See* Noelle Jenina Francesca E. Buan, *National Privacy Commission promulgates IRR of Data Privacy Act of 2012*, BUSINESSWORLD, Sep. 1, 2016, *available at* http://www.bworldonline.com/content.php?section=Opinion&title=national-privacy-commissi on-promulgates-irr-of-data-privacy-act-of-2012&id=132723 (last accessed Aug. 31, 2018).

62. National Privacy Commission, NPC Privacy Toolkit: A Guide for Management and Data Processing Officers at 20, *available at* https://privacy.gov.ph/wp-content/files/attachments/Privacy-Toolkit-compressedAug152017a.pdf (last accessed Aug. 31, 2018) [hereinafter NPC Privacy Toolkit].

63. *Id.* at 77.

64. *Id.* at 23-31.

65. *Id.* at 32-54.

66. *Id.* at 54-76.

Measures;[67] and (5) Management of Personal Data Breaches.[68] The Five Pillars, in effect, are all parts of the Privacy Management Program, and should be viewed as interrelated components and coordinated activities rather than separate and distinct obligations.

A. Designation of a Data Protection Officer

The designation of a Data Protection Officer (DPO) is based on the principle of accountability. Section 21 of the DPA states —

> Section 21. Principle of Accountability. — Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
>
> (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.
>
> (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.[69]

The NPC imposes a similar requirement to PIPs based on Section 14 of the law which categorically provides that "the personal information processor shall comply with all the requirements of this Act and other applicable laws."[70]

The accountability principle requires both PICs and PIPs to comply with the law, and be prepared to demonstrate or provide proof as regards its compliance efforts.[71] The designation of a DPO constitutes one such proof. It does not end there, however. A PIC or PIP should be able to further demonstrate that its DPO is actually able to fulfill his or her duties.[72] Accordingly, the DPO must have been accorded proper authority and resources necessary to perform such tasks as monitoring the compliance of

67. *Id.* at 77-105.

68. NPC Privacy Toolkit, *supra* note 65, at 106.

69. Data Privacy Act of 2012, § 21.

70. *Id.* § 14.

71. *Id.* § 21 & Rules and Regulations Implementing Data Privacy Act of 2012, § 50.

72. Rules and Regulations Implementing Data Privacy Act of 2012, § 50.

the organization with the law, providing recommendations on matters relevant to data protection, and engaging with both internal and external stakeholders.[73]

The guidelines for the designation and the corresponding duties of the DPO is provided under NPC Advisory No. 17-01 (2017), [74] which effectively aligns the DPA requirements with the General Data Protection Regulation (GDPR) of the European Union (EU).[75] The GDPR became effective on 25 May 2018.[76] In contrast to the GDPR, however, the DPA makes the designation of an individual or individuals accountable for an organization's compliance with the DPA mandatory for all PICs and PIPs.[77] As per its EU counterpart, a PIC or PIP is only required to designate a DPO where:

> (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
>
> (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.[78]

Moreover, while the GDPR provides that a group of undertakings may appoint a single DPO as long as the latter is easily accessible from each

73. *Id.* § 26.

74. National Privacy Commission, Designation of Data Protection Officers, Advisory No. 01, Series of 2017 (Mar. 14, 2017).

75. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 37 (1) (EU) [hereinafter GDPR].

76. EU General Data Protection Regulation, GDPR Portal: Site Overview, *available at* https://www.eugdpr.org (last accessed Aug. 31, 2018).

77. Rules and Regulations Implementing Data Privacy Act of 2012, § 26.

78. GDPR, *supra* note 78, art. 37 (1).

establishment,[79] a similar arrangement under the DPA may only be allowed upon the NPC's prior approval, to wit —

> Private Sector. Where a private entity has branches, sub-offices, or any other component units, it may also appoint or designate a COP for each component unit.
>
> Subject to the approval of the NPC, a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies. Where such common DPO is allowed by the NPC, the other members of the group must still have a COP, as defined in this Advisory.[80]

NPC Advisory No. 2017-01 further recommends that the DPO should be a regular employee of the entity as opposed to a consultant, probationary, or casual employee.[81] Where the employment of the DPO is based on contract, the term should at least be two years to ensure stability.[82] Notably, both the Advisory and the GDPR allow the DPO to perform concurrent tasks and duties, provided they do not result in conflict of interest scenarios.[83]

The designation of a Data Protection Officer should not be confused with the separate requirement of registration of Data Processing Systems.[84] A PIC or PIP shall still be required to designate a Data Protection Officer even if it is not covered by the registration requirements.[85]

The designation of the DPO is deemed part of maintaining a governance structure within a PIC or PIP that includes top management involvement in data protection, the establishment of an internal data privacy network, and allocation of resources for the DPO to perform his or her responsibilities.[86]

---

79. *Id.* art. 37 (2).

80. NPC, Advisory No. 01, s. 2017, at 5.

81. *Id.*

82. *Id.*

83. GDPR, *supra* note 78, art. 38 (6) & NPC, Advisory No. 01, s. 2017, at 5.

84. *See* National Privacy Commission, Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making, Circular No. 17-01 [NPC Circ. 17-01] (July 31, 2017).

85. *Id.*

86. Ivy Patdu & Jamael Jacob, Data Privacy 101: What's a Data Protection Officer?, *available at* https://www.rappler.com/technology/features/206315-data-protection-officer-functions (last accessed Aug. 31, 2018).

The position of the DPO within an organization, the scope of his or her responsibilities, and the reporting lines available to him or her all reflect the privacy strategy being implemented by that organization.[87] All these demonstrate organizational commitment, which is a key feature of a privacy management program.

B. Conduct of a Privacy Impact Assessment

The obligations of PICs and PIPs to carry out a Privacy Impact Assessment (PIA) is not explicitly provided by the DPA. The law does require them to determine the appropriate level of security that must be adopted relative to their respective data processing activities by taking into account a multitude of critical factors, such as: (1) nature of the personal information they need to protect; (2) risks represented by their processing system; (3) their size as an organization; (4) complexity of their operations; (5) current data privacy best practices; and (6) implementation cost of security measures.[88] Suffice to say, this task is best achieved through the conduct of a PIA.

More than anything else, a PIA allows an organization to gauge the impact of its data processing operations on the rights and freedoms of data subjects.[89] The output of this process enables management to make informed decisions when addressing gaps vis-à-vis its compliance efforts.

Embodying a risk-based approach to compliance, the conduct of a PIA is also consistent with the GDPR, which, for its part, uses the term, "Data Protection Impact Assessment."[90] The EU law explains —

> In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity[,] and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of

87. *Id.*

88. Data Privacy Act of 2012, § 20 (c).

89. *Id.*

90. GDPR, *supra* note 78, art. 35.

> available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.[91]

Notably, the GDPR instructs a PIC to consult the competent supervisory authority prior to processing in cases where the DPIA indicates that there are high risks in the processing operations that it cannot mitigate.[92] There is no similar requirement in the DPA. On the part of the NPC, the agency only requires that the PIA be made available by an organization if so requested by the Commission for compliance monitoring purposes.[93]

Under the GDPR, a DPIA is required in cases of:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Article 9 [ ] (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
>
> (c) a systematic monitoring of a publicly accessible area on a large scale.[94]

NPC Advisory No. 2017-03, on the other hand, allows a PIC or PIP to determine its own threshold for the conduct of a PIA, to wit —

> The PIC or PIP may forego the conduct of a PIA only if it determines that the processing involves minimal risks to the rights and freedoms of individuals, taking into account recommendations from the DPO. In making this determination, the PIC or PIP should consider the size and sensitivity of the personal data being processed, the duration and extent of processing, the likely impact of the processing to the life of data subject[,] and possible harm in case of a personal data breach.[95]

The NPC also does not prescribe any particular methodology. Instead, it has provided criteria that can be used to determine if a specific PIA model or technique is deemed appropriate or acceptable, namely:

> (a) It provides a systematic description of the personal data flow and processing activities of the PIC or PIP. This includes:

---

91. *Id*. whereas cl. 84.

92. *See* GDPR, *supra* note 78, art. 56.

93. National Privacy Commission, Guidelines on Privacy Impact Assessments, Advisory No. 03, Series of 2017 (July 31, 2017).

94. GDPR, *supra* note 78, art. 35, ¶ 3.

95. NPC, Advisory No. 03, s. 2017, at 5.

(a) purpose of the processing, including, where applicable, the legitimate interest pursued by the PIC or PIP;

(b) data inventory identifying the types of personal data held by the PIC or PIP;

(c) sources of personal data and procedures for collection;

(d) functional description of personal data processing, including a list of all information repositories holding personal data and their location, and types of media used for storage;

(e) transfers of personal data to another agency, company, or organization, including transfers outside the country, if any;

(f) storage and disposal method of personal data;

(g) accountable and responsible persons involved in the processing of personal data; and

(h) existing organizational, physical[,] and technical security measures[.]

(b) It includes an assessment of the adherence by the PIC or PIP to the data privacy principles, the implementation of security measures, and the provision of mechanisms for the exercise by data subjects of their rights under the DPA.

(c) It identifies and evaluates the risks posed by a data processing system to the rights and freedoms of affected data subjects, and proposes measures that address them.

(a) *Risk identification*. Risks include natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration[,] and contamination.

(b) *Risks evaluation based on impact and likelihood*. The severity or extent of the impact of a breach or privacy violation on the rights and freedoms of data subjects must be determined. The probability of the risk happening and the sources of such risk should also be taken into consideration.

(c) *Remedial measures*. Based on an assessment of risks, measures should be proposed on how to address and manage the said risks.

(d) It is an inclusive process, in that it ensures the involvement of interested parties and secures inputs from the DPO and data subjects.[96]

96. *Id*. at 6-7.

A PIA should be viewed as an important management process. Where PICs or PIPs decide to forego the conduct of a PIA based on their risk threshold, they should nonetheless maintain records of their processing activities that include a data inventory and a description of data processing systems.[97] Risk assessment is a key component of the compliance framework which requires, as a minimum, that a PIC or PIP documents its processing systems and manages risks entailed by the processing activities.[98]

C. Maintenance of a Privacy Management Program

A Privacy Management Program (PMP) is a comprehensive strategy or framework that allows a PIC or PIP to establish a robust data protection infrastructure whereby privacy management activities are seamlessly embedded throughout an organization and its personal data processing operations.[99]

As in the case of the PIA, maintaining a PMP is not explicitly mentioned in the DPA. Nonetheless, this duty proceeds from the same principle that underpins these *Five Pillars* — accountability. The principle emphasizes the responsibility of an entity engaged in personal data processing over all personal data under its control or custody.[100]

Accordingly, an accountable organization in relation to data protection is one that has accepted its responsibility for data protection, and has thereby established appropriate policies and procedures that promote good data protection practices which, when taken together, make up a proper and effective PMP.

Such responsibility includes ensuring that proper safeguards are in place even when it transfers personal data to a third party.[101] Indeed, where personal data processing is outsourced or subcontracted, a PIC is instructed to use contractual or other reasonable means to afford the data with a comparable level of protection while being processed by the third party recipient.[102]

97. Rules and Regulations Implementing Data Privacy Act of 2012, § 26 (c).

98. *Id.*

99. NPC Privacy Toolkit, *supra* note 65, at 55.

100. Data Privacy Act of 2012, § 21 & Rules and Regulations Implementing Data Privacy Act of 2012, § 50.

101. Data Privacy Act of 2012, § 21.

102. *Id.* § 21 (a).

A PMP should, *inter alia*, minimize the risk of experiencing security incidents or at least reduce the damage arising therefrom, while maximizing the ability of an organization to address the underlying problems of its data processing activities. Insofar as an organization's relationship with its stakeholders is concerned, the PMP demonstrates its commitment to build and foster trust through open and transparent policies and practices.

To accomplish these, a proper PMP should, by default, be defined by three (3) essential features:

(1) *Organizational Commitment*. There has to be buy-in from top management. This is key to the successful development of a PMP in any organization and is a prerequisite before any culture of privacy can emerge among the stakeholders. The designation of a DPO has to be carried out in a manner that goes beyond paper compliance (i.e., superficial) on the part of the organization. This means the individual or the office must be accorded the proper authority to carry out its tasks, and is given adequate support in the form of manpower, finances, and other resources. Effective internal audit and reporting mechanisms must also be set up and enforced consistently.[103]

(2) *Program Controls*. In establishing a baseline that will guide all program control mechanisms, an organization has to build a comprehensive data inventory. Together with the results of the enterprise-wide risk assessment, the inventory will inform the policies a PIC or PIP is expected to develop and implement as part of its PMP. Such policies must ensure consistent and effective safeguard mechanisms for personal data all throughout its lifecycle. At the same time, there also needs to be proper management of third-party engagements, whether they consist of PIPs, other service providers, or entities with whom personal data are shared or disclosed by the organization. This is usually addressed through standard contract templates or standard contractual clauses. Whereas policies determine the standards PIC or PIP personnel ought to abide by to facilitate data protection, a capacity-building program and information

103. *See generally* NPC Privacy Toolkit, *supra* note 65, at 56-58. The latest version of the toolkit identifies the PMP components as: "Governance" corresponding to the Organizational Commitment; "Program Controls;" and "Continuity and Establishing a Privacy Ecosystem" corresponding to Continuing Assessment and Development. *Id*.

awareness campaigns develop the culture of privacy that is necessary to sustain an organization's PMP.[104]

(3) *Continuing Assessment and Development.* A privacy management program requires as a critical component a means to ensure continuity and improvement of the program. This requires an oversight and review plan which may include development of metrics to regularly evaluate the program and its key components. The review process is intended to improve implementation and accommodate changes in the privacy ecosystem and technological developments.[105]

Together, these three are referred to by the NPC as a Data Privacy Accountability and Compliance Framework.[106] In a practical sense, the PMP is the embodiment of the provisions of the Data Privacy Act as reflected in a program of coordinated projects and activities. The purpose of the program is for PICs and PIPs to comply with their obligations under the law and to achieve the greater purpose of protecting individuals through the protection of their personal data.[107]

Under the GDPR, the development and implementation of a PMP is best exemplified by the primary responsibility ascribed to a controller, namely

> [t]aking into account the nature, scope, context[,] and purposes of processing[,] as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.[108]

These measures include the implementation of appropriate data protection policies, and even adherence to codes of conduct[109] and/or certification mechanisms,[110] approved by a competent supervisory authority. They must be designed to implement data protection principles in an effective manner and must be integrated into the processing activities

104. *Id.* at 58-62.

105. *Id.* at 62-63.

106. *Id.* at 56-63.

107. *Id.*

108. GDPR, *supra* note 78, art. 24 (1).

109. *Id.* art. 24 (2).

110. *Id.* art. 24 (3).

themselves.[111] Similarly, they must ensure, by default, that only personal data necessary for the purpose of the processing activity involved are in fact processed.[112] These last two obligations represent what is referred to under the GDPR as "data protection by design and by default."[113]

The foregoing responsibility finds its counterpart in the main components of Section 20 of the DPA, to wit —

> SEC. 20. Security of Personal Information. — (a) The personal information controller must implement reasonable and appropriate organizational, physical[,] and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration[,] and disclosure, as well as against any other unlawful processing.
>
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration[,] and contamination.
>
> (c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices[,] and the cost of security implementation.[114]

These provisions have been expounded further in the IRR of the DPA,[115] adopting the language of the GDPR on "data protection by design and by default."[116] Under the IRR of the DPA —

> b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures ... .
>
> (a) The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.

---

111. *Id.* art. 25 (1).

112. *Id.* art. 25 (2).

113. *Id.* art. 25.

114. Data Privacy Act of 2012, § 20.

115. Rules and Regulations Implementing Data Privacy Act of 2012, § 26 (b).

116. GDPR, *supra* note 78, art. 25.

(b) The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.

(c) The policies shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.[117]

The conduct of a PIA is most effective in facilitating the development of a PMP, while a Privacy Manual is the most common tool used to feature the various components of an organization's PMP.

D. Implementation of Data Privacy and Data Security Measures

The fourth pillar of compliance goes into how policies are operationalized through procedures and actual practice.[118] The strategy and roadmap for the overall management and review of the PMP are established through organizational commitment, but the extent by which the goals of the program are accomplished would depend on how program controls are embedded in day-to-day operations.[119]

The implementation of data privacy and data security measures should necessarily consider the rights and obligations outlined in Chapter III of the Data Privacy Act which pertains to data privacy principles and the criteria for lawful processing;[120] Chapter IV affirms the rights of a data subject;[121] Chapters V and VII refer to implementation of security measures and mandatory breach notification;[122] and Chapter VI provides for the principle of accountability.[123]

The Data Privacy Act provides that 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

117. Rules and Regulations Implementing Data Privacy Act of 2012, § 26 (b).

118. *See* NPC Privacy Toolkit, *supra* note 65, at 77-96.

119. *Id.*

120. Data Privacy Act of 2012, ch III.

121. *Id.* ch. IV.

122. *Id.* ch. V & VII.

123. *Id.* ch. VI.

proportionality." [124] These general data privacy principles are further crystallized through the requirement that personal information be:

> (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only [(purpose limitation)];
>
> (b) Processed fairly and lawfully [(lawfulness, fairness)];
>
> (c) Accurate, relevant[,] and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed[,] or their further processing restricted [(accuracy)];
>
> (d) Adequate and not excessive in relation to the purposes for which they are collected and processed [(data minimization)];
>
> (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
>
> (f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided*, [t]hat personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided*, *further*, [t]hat adequate safeguards are guaranteed by said laws authorizing their processing [(storage limitation)].[125]

These principles are substantially similar with the principles relating to processing of personal data under Article 5 of the GDPR.[126] The GDPR

---

124. *Id.* § 11.

125. *Id.* The parenthetical notes in the quoted passage are supplied by the Author.

126. GDPR, *supra* note 78, art. 5. This provision, entitled "Principles Relating to Processing of Personal Data," provides that personal data shall be:

> (1) processed lawfully, fairly[,] and in a transparent manner in relation to the data subject ('lawfulness, fairness[,] and transparency');
> (2) collected for specified, explicit[,] and legitimate purposes[,] and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes[,] or statistical purposes shall, in accordance with Article 89 [ ] (1), not be considered to be incompatible with the initial purposes ('purpose limitation');

principles are enclosed in parentheses and indicated in the preceding paragraphs.

The general data privacy principles of transparency, legitimate purpose, and proportionality are relevant to establishing trust between those who process personal data and the data subjects.[127] The principle of transparency generally requires fairness and openness in personal information processing, which corresponds to the right of data subjects to information that relates to the processing of their personal information.[128] There is transparency if data subjects will not be unfairly surprised with the nature and extent by which their personal information is processed.[129] Thus, the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised.[130]

---

(3) adequate, relevant[,] and limited to what is necessary in relation to the purposes for which they are processed ('data minimi[z]ation');
(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes[,] or statistical purposes in accordance with Article 89 [ ] (1) subject to implementation of the appropriate technical and organi[z]ational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthori[z]ed or unlawful processing and against accidental loss, destruction[,] or damage, using appropriate technical or organi[z]ational measures ('integrity and confidentiality.')

Id.

127. Rules and Regulations Implementing Data Privacy Act of 2012, § 18.

128. *See* Rules and Regulations Implementing Data Privacy Act of 2012, § 18 (a).

129. *Id.*

130. *Id.*

In addition to the right to be informed, data subjects are entitled to the following rights:

(1) Right to be informed and be furnished with information relevant to the processing of their personal data;[131]

(2) Right to reasonable access, upon demand, [to the] contents of his or her personal information processed and details of the processing; [132]

(3) Right to correct and dispute inaccuracies or errors in their personal information;[133]

(4) Right to object to processing and order erasure of their personal information when no longer necessary for the purpose for which they were collected and other circumstances;[134]

(5) Right to data portability or the right to obtain a copy of data undergoing processing in an electronic or structured format in a form which allows further use by the data subject;[135]

(6) Right to complain and right to damages for privacy violations.[136]

The law guarantees these rights in order for the data subjects to have greater control over the processing of their personal data.[137] Thus, the procedures for the exercise of these rights should be established.

Any information and communication relating to the processing of personal data or exercise of data subject rights should be easy to access and understand using clear and plain language.[138] One of the means by which the principle of transparency can be incorporated in daily operations is through effective privacy notices.

131. *See* Data Privacy Act of 2012, § 16 (a) & (b).

132. *Id.* § 16 (c).

133. *Id.* § 16 (d).

134. *Id.* § 16 (e).

135. *Id.* § 18.

136. *Id.* § 16 (f).

137. *See generally* Data Privacy Act of 2012, ch. IV.

138. Rules and Regulations Implementing Data Privacy Act of 2012, § 18 (a).

The second principle is that of legitimate purpose, which refers to the principles of lawfulness of processing and purpose limitation.[139] Under the Civil Code, parties to a contract may establish therein "stipulations, clauses, terms, and conditions as they may deem convenient, provided that these are not contrary to law, morals, good customs, public order, or public policy."[140] The IRR of the DPA incorporates this condition in defining legitimate purpose.[141] Legitimate purpose requires a documented basis of processing, which may either be the data subject's express consent, or established on the basis of law or regulation.[142]

The DPA defines consent of the data subject as "any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her."[143] The legislative intent is to require express consent, further emphasized by requiring that consent "be evidenced by written, electronic[,] or recorded means."[144]

The DPA also provides the criteria for lawful processing, where consent is just one of these conditions.[145] There are circumstances wherein consent may not be required, depending on the nature of the personal data to be processed.[146] The criteria for lawful processing are provided for in the DPA under Section 12 for personal information and Section 13 for sensitive personal and privileged information.[147]

These include conditions, wherein consent may be implied by the relationship between data subject and PIC, thus the required express consent is dispensed with.[148] Where non-sensitive personal information is being processed, consent is not required where the processing is necessary and is related to the fulfillment of a contract with the data subject, or where processing is for the purposes of the legitimate interest pursued by the PIC

139. *Id.* § 18 (b).

140. An Act to Ordain and Institute the Civil Code of the Philippines [CIVIL CODE], Republic Act No. 386, art. 1306 (1950).

141. Rules and Regulations Implementing Data Privacy Act of 2012, § 18.

142. *Id.*

143. Data Privacy Act of 2012, § 3 (b).

144. *Id.*

145. *Id.* §§ 12 & 13.

146. *Id.*

147. *Id.*

148. *Id.*

or by a third party, or parties to whom the personal information is disclosed.[149] Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact.[150] In case of sensitive personal information, consent is not required where processing is necessary for purpose of medical treatment, carried out by a medical practitioner or medical treatment institution. [151]

The other conditions may have been included because of the nature of the processing activities and how they relate to a necessary purpose or public interest. For instance, the DPA provides that processing of non-sensitive personal information may proceed without consent where processing is necessary to comply with a legal obligation,[152] to protect vitally important interests of the data subject,[153] or to respond to national emergency and the requirements of public order and safety. [154] For sensitive personal information, processing may be allowed if the same is provided for by existing laws and regulations,[155] where "processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent." [156] Consent is also not required where the processing is necessary to protect lawful rights and interests, or establish or defend legal claims. [157] In all these cases, even where consent is not required, the personal information should be protected.

The principle of proportionality[158] is consistent with the principles of data minimization and storage limitation. In the DPA's IRR, proportionality also incorporates the requirement of necessity, mandating that personal data shall be processed only if the purpose of the processing could not reasonably

149. Data Privacy Act of 2012, §§ 12 (b) & (f).

150. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR) at 80, *available at* https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (last accessed Aug. 31, 2018).

151. Data Privacy Act of 2012, § 13 (e).

152. *Id.* § 12 (c).

153. *Id.* § 12 (d).

154. *Id.* § 12 (e).

155. *Id.* § 13 (b).

156. *Id.* § 13 (c).

157. Data Privacy Act of 2012, § 13 (f).

158. Rules and Regulations Implementing Data Privacy Act of 2012, § 18 (c).

be fulfilled by other means.[159] This principle means collecting only relevant information and storing them only for as long as necessary for the fulfillment of the purposes for which the data were collected.[160]

In order to operationalize these principles, the PIC or PIP should maintain records of processing activities, data inventory, and data flows.[161] This is one of the means by which the bases of processing, relationships with third parties, and proportionality in data collection, further processing, and retention can be documented, referred to, and reviewed. Where the basis of processing is consent of data subjects, the consent forms and processes for obtaining consent should be evaluated to ensure that they meet the required voluntariness and transparency under the DPA. Moreover, this fact should likewise be included in the documentation. Operationalizing these principles also means being cognizant of specific industry standards, where the nature of operations, business requirements and legal obligations would determine periods for record retention, allowable disclosures, and appropriate contractual clauses whenever personal data is shared or transferred to a third party.

Likewise, policies and procedures should be in place to guide the processing activities at every stage of the data life cycle, from personal data collection to disposal or destruction of records containing personal data. These policies and procedures should cover those for obtaining consent, acceptable use, access, disclosure, and data quality. They should cover particular activities like research, marketing and employee management, and data processing systems like those involving biometric data and close circuit television systems, among others.

Furthermore, the procedures and guidelines should be complemented by the appropriate security measures. The DPA provides as a minimum requirement the need to implement organizational, physical, and technical security measures, including:

(a) Safeguards to protect its computer network against accidental, unlawful, or unauthorized usage, or interference with or hindering of their functioning or availability;

(b) A security policy with respect to the processing of personal information;

159. *Id.*

160. *Id.*

161. *See* Rules and Regulations Implementing Data Privacy Act of 2012, § 26 (c).

(c) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective[,] and mitigating action against security incidents that can lead to a security breach; and

(d) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach. [162]

In determining the appropriate level of security, the conduct of a PIA will be instrumental in implementing a risk-based approach, to maximize available resources in managing privacy risks.[163] The goal of these security measures is to protect personal information "against any accidental or unlawful destruction, alteration[,] and disclosure, as well as against any other unlawful processing."[164] These include protection against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination. [165] The required security measures are envisaged to maintain the confidentiality, integrity, and availability of personal information.[166] This is consistent with the principle of integrity and confidentiality under the Article 5 (f) of the GDPR providing that the processing of personal information should be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthori[z]ed or unlawful processing and against accidental loss, destruction[,] or damage, using appropriate technical or organi[z]ational measures."[167]

In addition, the DPA provides security measures specific for sensitive personal information in government. [168] The DPA mandates the head of a government agency or instrumentality to "be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order

162. Data Privacy Act of 2012, § 20 (c).

163. *Id.* § 20 (a).

164. *Id.*

165. *Id.* § 20 (b).

166. *Id.*

167. GDPR, *supra* note 78, art. 5 (1) (f).

168. Data Privacy Act of 2012, ch. VII.

to satisfy the minimum standards."[169] NPC has provided additional standards for data protection in government through NPC Circular No. 16-01.[170]

E. Management of Personal Data Breaches

Personal data breach management represents a reminder for PICs and PIPs to constantly remain prepared for a personal data breach, as well as other security incidents.

In the context of data protection, a data breach specifically refers to a personal data breach. It is a breach of security that leads to the "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed[.]"[171] A data breach forms part of the broader concept of "security incident" which, in turn, refers to an "event or occurrence that affects or tends to affect data protection," in the sense that it may "compromise the availability, integrity[,] and confidentiality of personal data."[172] It includes cases that would otherwise result in a personal data breach, if not for available safeguards.

Under the DPA, the most explicit directive addressed to PICs regarding data breach management consists of the responsibility to promptly notify the NPC and affected data subjects of a personal data breach when it is attended by three specific circumstances, namely: (1) when it involves "sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud[;]" (2) when the information "are reasonably believed to have been acquired by an unauthorized person"; and (3) when the PIC or the Commission believes that the "unauthorized acquisition is likely to give rise to a real risk of serious harm to any of the affected data subject[s]."[173]

Such duty is largely consistent with the GDPR, albeit narrower in scope. The general rule under EU law is that a data controller must notify the competent supervisory authority about *any* personal data breach without undue delay.[174] If possible, such notification should be not later than 72

169. *Id.* § 22.

170. National Privacy Commission, Security of Personal Data in Government Agencies, Circular No. 16-01 (Oct. 10, 2016).

171. Rules and Regulations Implementing Data Privacy Act of 2012, § 3 (k).

172. *Id.* § 3 (s).

173. Data Privacy Act of 2012, § 20 (f).

174. GDPR, *supra* note 78, art. 33 (1).

hours after the controller becomes aware of the incident.[175] Otherwise, a late notification must be accompanied by an explanation for the delay.[176] Delayed notification may also be recognized by the NPC in the domestic context, but only when attended by specific conditions, such as that it should only be to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system, where it may stand in the way of a criminal investigation related to the breach.[177]

Dispensing with notification is generally frowned upon. In the EU, notification may be excused if it is "unlikely to result in a risk to the rights and freedoms of natural persons."[178] For the NPC, it may consider a number of factors when determining if notification is unwarranted, but only in relation to affected data subjects.[179] They include:

(1) implementation of security measures that would prevent use of the personal data by unauthorized persons;[180]

(2) good faith in the PIC's acquisition of personal data;[181] and

(3) if notification goes against public interest or that of affected data subjects.[182]

Still and all, the mandatory nature of the notification requirement under the DPA is highlighted best by the law's treatment of the act of concealment of a security breach, which it defines as a specific type of crime. Indeed, Section 30 of the DPA states —

> SEC. 30. Concealment of Security Breaches Involving Sensitive Personal Information. — The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos ([₱]500,000.00) but not more than One million pesos ([₱]1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission

175. *Id.*

176. *Id.*

177. National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 03, s. 2016], § 17 (B) (Dec. 15, 2016).

178. GDPR, *supra* note 78, art. 33 (1).

179. NPC Circ. No. 03, s. 2016, § 19.

180. *Id.* § 19 (A).

181. *Id.* § 19.

182. *Id.* § 18 (B).

> pursuant to Section 20 [ ] (f), intentionally or by omission conceal[ ] the fact of such security breach.[183]

Where the breach occurs while the personal data is under the custody of a data processor, the latter must notify the controller without undue delay after learning of the incident.[184]

To facilitate the effective management of security incidents, including personal data breaches, policies and protocols need to be developed by every PIC and PIP. Such an effort will form part of its organizational security measures relating to the processing of personal data, as prescribed by the Implementing Rules and Regulations of the DPA.[185] Various technical security measures ought to be put in place as well.

The NPC has laid out a concrete blueprint in terms of what it expects from PICs and PIPs and their respective personal data breach management practices with its issuance of Circular No. 16-03.[186] Among the elements of a personal data breach management program that are worth noting in the issuance are:

(1) Creation of a data breach response team;[187]

(2) Development of preventive or mitigating measures;[188]

(3) Establishment of an incident response policy and procedure, including that for personal data breach notification;[189]

(4) Documentation of all personal data breaches and security incidents.[190]

Under the GDPR, a similar obligation to document every personal data breach is imposed.[191] As a minimum, details should include the surrounding

183. Data Privacy Act of 2012, § 30.

184. GDPR, *supra* note 78, art. 33 (2).

185. Rules and Regulations Implementing Data Privacy Act of 2012, § 27 (e).

186. NPC Circ. No. 03, s. 2016.

187. *Id.* § 5.

188. NPC Circ. No. 03, s. 2016, § 6.

189. *Id.* rules IV & V.

190. *Id.* § 9.

191. GDPR, *supra* note 78, art. 33 (5).

facts, the effects of the breach, as well as the remedial measures taken by the controller.[192]

III. ACCOUNTABILITY

The DPA, which was enacted to law in 2012, is legislation intended to uphold "informational privacy," and ensure protection of personal data.[193] This right gives individuals the ability to control information about themselves and the ability to determine what information about them is collected or disclosed, how their personal data is to be used, and for what purpose.[194]

The five pillars of compliance form the cornerstones of accountability, intended to make compliance with Data Privacy Act grounded. For instance, the designation of a data protection officer signifies that the PIC or PIP is committed to comply with the law. In empowering the DPO to perform its functions, the PIC or PIP is ready to go beyond compliance, towards accountability. Through a PIA and a PMP, a PIC or PIP can implement a risk-based compliance roadmap, to put in place policies and procedures for data protection and breach management, and to embed these in day-to-day operations.

Accountability goes beyond checklists and meeting legal requirements. It requires PICs and PIPs to demonstrate how they have integrated data protection in their systems, from policies to actual practice.[195] It must be shown that data protection, as a core component of organizational culture, is practiced and embraced by all those involved in personal data processing, from top management to the rank and file employee. The challenge is to reap the benefits from the availability of information while protecting personal data from unlawful or unauthorized processing or threats to its confidentiality, integrity, and availability.

While the five pillars serve as a starting point and foundation, protecting personal information and cultivating trust constitute a continuous process that is built over time, one which is constantly being developed and improved. It aims not just to meet the requirements of the law, but also strives towards best practices to improve and strengthen systems for purposes

192. *Id.*

193. Data Privacy Act of 2012, § 2.

194. *Id.*

195. *See* Rules and Regulations Implementing Data Privacy Act, § 50.

of protecting individuals. Ultimately, accountability, at its core, is simply about doing what has to be done because it is the right thing to do.