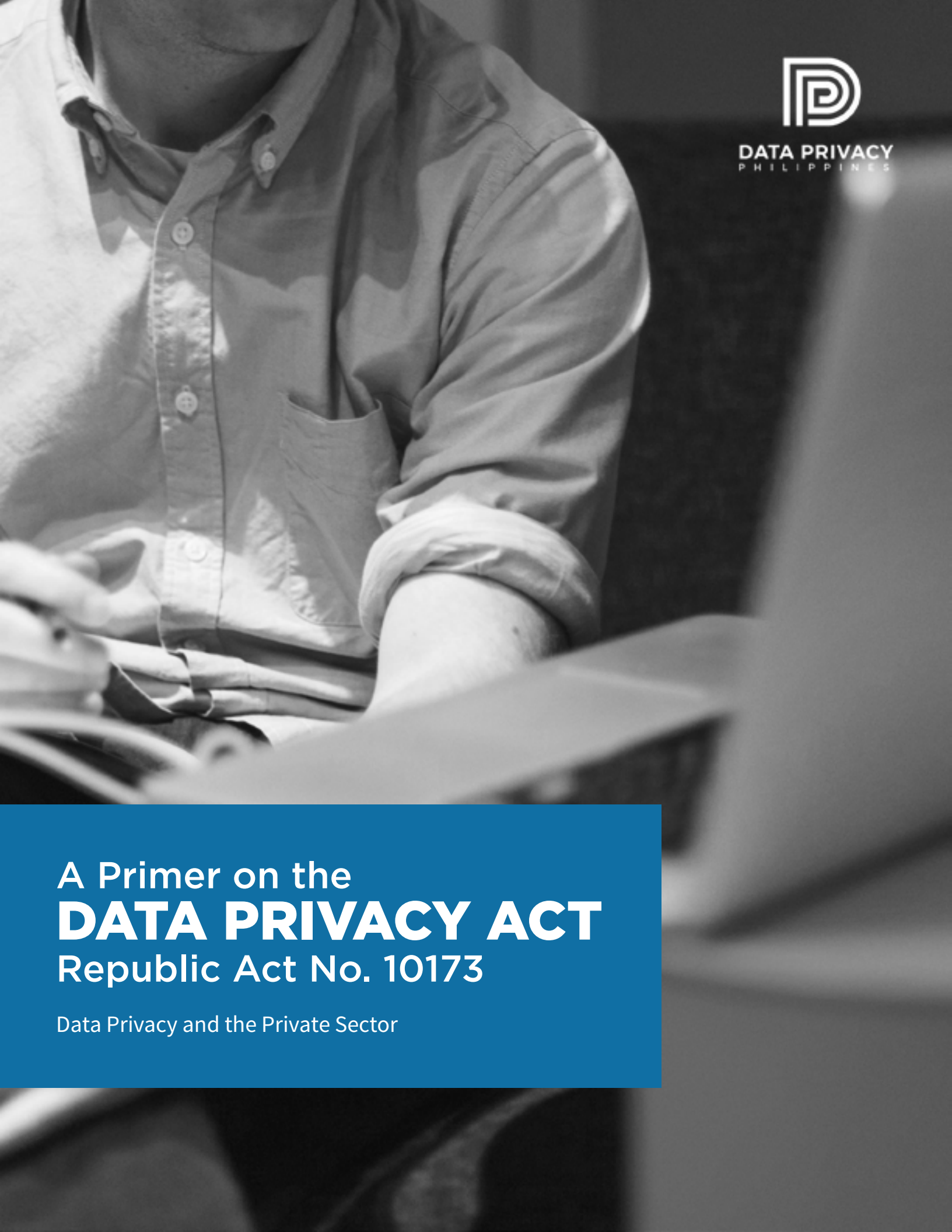


DATA PRIVACY
PHILIPPINES

A Primer on the
DATA PRIVACY ACT
Republic Act No. 10173

Data Privacy and the Private Sector

Introduction

Information is a cornerstone of modern life and lies at the heart of any business. The Data Privacy Act of 2012, set to be fully implemented by September 2017, will have far reaching impacts on how businesses handle information. In doing so, the law will change you relate to your employees, your customers, and any individual whose personal information you require.

This primer will help you understand what the Data Privacy Act is all about, and let you see what's up ahead for you or your business.

What the Law Covers – Personal Information, Data Subjects and Processing

1. What is personal information?
"Personal information" refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information (e.g. a person's name, or any other unique identifier). This also includes information which, when put together with other information would directly and certainly identify an individual.[1]

2. Who is a data subject?
"Data Subject" refers to an individual whose personal information is processed.[2] For your business, this could include your employees and customers. You as an individual could also be a data subject – for other businesses, and for the government.

3. Is there a special category of personal information?
Under the DPA, **Sensitive Personal Information** and **Privileged Information** are given a treatment different from that of Personal Information

"Sensitive personal information" is enumerated under Section 3(l). It 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, 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;

(3) Issued by government agencies peculiar to an individual which includes, but 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.[3]

The law imposes more stringent requirements over the processing of sensitive personal information, and failure to meet these requirements will result in stiffer penalties.

On the other hand, "Privileged Information" refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.[4] In addition to the protection under the Rules of Court, privileged information is now also protected by the data privacy act.

1 Section 3(g)
2 Section 3(c)
3 Section 3(l)
4 Section 3(k)

4. What is the scope of the DPA? When does it apply?

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, including those personal information controllers and processors 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[5].

In the case of extraterritorial application, the DPA applies to an act done or practice engaged in and outside of the Philippines by an entity 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:

(1) A contract is entered in the Philippines;
(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
(3) 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:

(1) The entity carries on business in the Philippines; and
(2) The personal information was collected or held by an entity in the Philippines.[6]

5. What is processing?

"Processing" refers to any operation or any set of operations performed upon personal information. This includes, but is not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[7]

It is important to note that this list is not exhaustive. Hence, "any" kind of operation upon personal information is included in the word "processing." What the definition in the DPA provided is an example of operations performed upon personal information but the DPA did not limit the definition to the said list.

6. Does the DPA protect all personal information about private persons?

No. The DPA does not apply to the following:

(a) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

5 Section 4
6 Section 6
7 Section 3 (j)

(b) Information relating *to any discretionary benefit of a financial nature* such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(c) Personal information processed for *journalistic*, artistic, literary or research* purposes;

(d) Information *necessary in order to carry out the functions of public authority* which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in the law shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(e) Information *necessary for banks and other financial institutions* under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally *collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions*, including any applicable data privacy laws, which is being processed in the Philippines.[8] (emphasis supplied)

*Note: The provisions of the DPA cannot be construed to have amended or repealed the provisions of R.A. No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.[9]

7. When is there lawful processing of personal information?

To be considered as lawful processing, the personal information controller (and the personal information processor, as the case may be) must comply with two (2) sets of guidelines in the DPA: a) the General Data Privacy Principles under Section 11; and b) the Criteria for Legitimate Processing under Section 12 (for personal information), or Section 13 (for sensitive personal information and privileged information).

8 Section 6
9 Section 5

Who the Law Regulates – Controllers, Processors, and their Responsibilities

8. Who is a personal information controller?
"Personal information controller" refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

> (1) A person or organization who performs such functions as instructed by another person or organization; and
>
> (2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.[10]

9. Who is a personal information processor?
"Personal information processor" refers to any natural or juridical person qualified to act as such [under the DPA] to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.[11]

10. What are the General Privacy Principles[12]?
Personal information must be:

1. 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;

2. Processed *fairly and lawfully*;

3. *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;

4. *Adequate and not excessive in relation to the purposes* for which they are collected and processed;

5. *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

6. 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. However:

   A. Personal information collected for other purposes may be processed for *historical, statistical or scientific purposes*, and in cases laid down in *law may be stored for longer periods;* and
   B. Adequate safeguards are guaranteed by said laws authorizing their processing.

10 Section 3(h)
11 Section 3(i)
12 Section 11

11. If what is processed is merely personal information, what other conditions, apart from the general privacy principles, must be complied before there can be lawful processing?

The Criteria for Legitimate Processing is only permitted under the DPA if first, it is not prohibited by law and it complies with any of the following conditions:

> (a) The data subject has given his or her *consent*;
> (b) The processing of personal information is necessary and is *related to the fulfillment of a contract* with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
> (c) The processing is *necessary for compliance with a legal obligation* to which the personal information controller is subject;
> (d) The processing is *necessary to protect vitally important interests of the data subject*, including life and health;
> (e) The processing is necessary in order to respond to *national emergency*, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
> (f) The processing is *necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party* or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[13] (emphasis supplied)

12. What is consent?

"Consent of the data subject" refers to 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. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.[14]

13. If what is processed are sensitive personal information, what are the conditions for lawful processing other than compliance with the general privacy principles?

Under the DPA, sensitive personal information and privileged information shall be prohibited except in the following cases:

(a) The data subject has given his or her *consent, specific to the purpose prior to the processing*, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
(b) The processing of the same is *provided for by existing laws and regulations*: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
(c) The 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* prior to the processing;
(d) The processing is *necessary to achieve the lawful and noncommercial objectives of public organizations* and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal

13 Section 12
14 Section 3(b)

information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;

(e) The processing is *necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution*, **and** an *adequate level of protection* of personal information is ensured; or

(f) The processing concerns such *personal information as is necessary for the protection of lawful rights and interests* of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[15]

The Rights of Data Subjects

14. What are the rights of a data subject?

A data subject has two sets of rights. The first set of substantive rights involves specific entitlements = of the Data Subject under Chapter IV of the DPA which refers largely to the processing of personal information; and the second set of auxiliary rights involves rights that may be exercised by the Data Subject to be able to hold the Controllers and/or Processors Liable.

The following are the substantive rights of the Data Subject:

1. Right to be Informed
2. Right of Access
3. Right to Correction
4. Right to Suspend, Withdraw, or Order the Removal of Personal Information from the Controller's Filing System
5. Right to Indemnity
6. Right to Data Portability

The Data Subject has the following auxiliary rights:

7. Right to Lodge a Complaint before the Commission
8. Right to Know the Identity of Accountable Individuals

Substantive Rights of the Data Subject
Right to be Informed

15. What the data subject's right to be informed?

The following information must be provided before the entry of the personal information into the processing system, or at the next practical opportunity:

(1) Description of the personal information to be entered into the system;
(2) Purposes for which they are being or are to be processed;
(3) Scope and method of the personal information processing;
(4) The recipients or classes of recipients to whom they are or may be disclosed;
(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
(6) The identity and contact details of the personal information controller or its representative;

15 Section 13

(7) The period for which the information will be stored; and
(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.[16]

The data subject must also be informed whether personal information pertaining to him or her shall be, are being or have been processed.[17]

16. When does the Right to Information not apply?
The notification required before the entry of the personal information (See **Question 15** above) does not apply when any of the following conditions are present:

1) the personal information is needed pursuant to a *subpoena;*
2) when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service;
3) when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject; or
4) when the information is being collected and processed as a result of legal obligation[18]

Right of Access

17. What is the right of access of a data subject?
The data subject has reasonable access to, upon demand, the following:
(1) Contents of his or her personal information that were processed;
(2) Sources from which personal information were obtained;
(3) Names and addresses of recipients of the personal information;
(4) Manner by which such data were processed;
(5) Reasons for the disclosure of the personal information to recipients;
(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
(7) Date when his or her personal information concerning the data subject were last accessed and modified; and
(8) The designation, or name or identity and address of the personal information controller[19]

Also, in case when there are inaccuracies and error in the personal information and the same have been corrected by the personal information controller, the personal information controller shall, after correction, ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients.[20]

16 Section 16(b)
17 Section 16(a)
18 Section 16(b)
19 Section 16(c)
20 Section 16 (d)

Right to Correction

18. What is the right to correction[21]?
The right to correction involves the right of the data subject to dispute inaccuracies or error in the personal information and have the same corrected immediately.

19. Can the personal information controller refuse to correct personal information?
Yes, the personal information controller can refuse to correct the inaccuracy or error when the request is vexatious or otherwise unreasonable.[22]

Right to Suspend, Withdraw, or Order the Removal of Personal Information from the Controller's Filing System

20. What is the data subject' right to suspend, withdraw or order the removal of personal information from the controller's filing system?
The data subject has the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information.[23]

Right to Indemnity

21. When is the data subject entitled to indemnity[24]?
The data subject is entitled to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal information.[25]

Right to Data Portability

22. What is the data subject's right to data portability?
The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.[26]

21 Section 16 (d)
22 Section 16 (d)
23 Section 16 (e)
24 Section 16 (f)
25 Section 16 (f)
26 Section 18

Exception to Substantive Rights

23. When are the rights under Sections 16 and 18 not applicable?[27]
Under Section 19, the rights granted to the data subject under Chapter IV are not applicable if any of the following situations are present:

1. The processed personal information are used only for the needs of scientific and statistical research, subject to the following conditions:
    a. No activities are carried out and no decisions are taken regarding the data subject; and
    b. The personal information shall be held under strict confidentiality and used only for the declared purpose

2. The processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative, or tax liabilities of a data subject.

Auxiliary Rights of the Data Subject
Right to Lodge a Complaint before the Commission

24. What is the legal basis for this right?
This right can be inferred from the duty of the National Privacy Commission under Section 7 of the DPA to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report.[28]

Right to Know the Identity of Accountable Individuals

25. What is the data subject's right to know the identity of accountable individuals?
The data subject has a right to be informed of the identities of individual/s who are accountable for the organization's compliance with the DPA as designated by the personal information controller.[29]

26. What are the remedies of a data subject in case of breach?

1. *Administrative remedy*[30]
Lodge a complaint before the National Privacy Commission

2. *Judicial Remedy*
    A. Indemnity under Section 16(f) – See **Question 21** above
    B. Restitution under Section 37
    C. Criminal Action for Crimes defined under Chapter VIII

27 Section 19
28 Section 7(b)
29 Section 21
30 Section 7(b)

27. How is restitution determined for purposes of the DPA?
Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.[31]

28. What are the crimes under Chapter VIII?
See **Annex A** for the Table of Crimes

29. Is the DPA applicable to Cross-border flow of data[32]?
Yes, See Question 4 on Extraterritorial application

30. When is it not applicable?
Under Section 4(g), the DPA does not apply to personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

31. How is this regulated?
The National Privacy Commission is mandated to regulate the Cross-Border flow of data.

31 Section 37
32 Section 6

Personal Information Controller and/or Processor

32. Who is a personal information controller?
"Personal information controller" refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.[33]

Under this definition, both natural and juridical persons may be considered as a personal information controller. It is important to note that the term explicitly excludes two (2) categories of persons under its definition: a) person or organization instructed by the personal information controller; and b) individuals who collect for household affairs.

The first set of excluded of persons or organizations can fall within *personal information processor* (see **Question 33**).

33. Who is a personal information processor?
"Personal information processor" refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.[34]

34. When can there be lawful processing of personal information by the personal information controller and/or processor?
(See **Question 7**)

35. Can the private sector process personal information without complying with the conditions for lawful processing?
Yes, if the same is within the exceptions provided for under Section 4 of the DPA. (See **Question 6**)

36. What are the obligations of the personal information controller?
Aside from the complying with the conditions for lawful processing of personal information, the personal information controller has the following obligations relating to the rights of the data subject:

1. Obligation to Inform the Data Subject when his or her Personal Information is processed
2. Obligation to Notify the Data Subject before the entry of his or her Personal Information into the Processing System of the Personal Information Controller[35]
3. Obligation to Allow Access to Personal Information pertaining to the Data Subject, upon demand
4. Obligation to Correct any Inaccuracy or Error[36]
5. Obligation to Remove Personal Information from its Filing System, upon demand and proof[37]

33 Section 3(h)
34 Section 3(i)
35 Subject to an exception: See Question 16
36 Subject to an exception: See **Question 19**
37 Proof that personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.

6. Obligation to Indemnify Data Subject for Breach
7. Obligation to Furnish the Data Subject a Copy of Data undergoing processing in an Electronic or Structured Format
8. Obligation to Inform the Data Subject of the Identity of Accountable Individuals, upon request

37. As regards security of personal information, what measures must the personal information controller take?
In addition to the obligations provided in the preceding question, the personal information controller also has obligations relating to the security of the personal information. The Security of Personal Information are subject to the following guidelines:

(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. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
(2) A security policy with respect to the processing of personal information;
(3) 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
(4) 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.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission[38] and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only 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.

> (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.
> (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.
> (3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach."[39]

38. What are the fundamental responsibilities of a personal information controller in relation to the information it maintains? To what extent must it perform these responsibilities?
Section 21 provides for the accountability personal information controllers. It provides that the personal information controller is responsible for the personal information under its control and custody. This includes information transferred to a third party for processing (or personal information processor), whether the same was transferred domestically or internationally.

Under the said section, personal information controllers have the following responsibilities:

(a) Accountable for complying with the requirements of this Act;
(b) Use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party;
(c) Designate an individual or individuals who are accountable for the organization's compliance with this Act;
(d) Inform the data subject the identity of the individual(s) so designated upon request.

39. Does the private sector, as personal information controller, have special obligations vis-à-vis the sensitive personal information it maintains?
Generally, No. However, in the case of Government Contractors that entered into a contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, the DPA provides that the provisions on securing sensitive personal information and privileged information under Chapter VII of the DPA apply. This Chapter deals specifically with the security of *sensitive personal information* maintained by government, its agencies and instrumentalities.

(**Questions 40 and 41** are applicable only to Government Contractors that entered into a contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals)

38 National Privacy Commission
39 Section 20

40. What is the special rule for government contractors?
Under Section 24 of the DPA, when the government enters into a contract that may involve accessing or requiring sensitive personal information from 1,000 or more individuals, the contracting agency shall require the contractor and latter's employees:

1. To register their personal information system with the NPC
2. To comply with the other provisions of the DPA including the requirements relating to access by its personnel to sensitive personal information.

41. What are the requirements[40] relating to access to sensitive personal information by agency personnel?

For On-site and Online access[41], no employee shall have access to sensitive personal information on government property or through online facilities unless said employee has *security clearance* from the head of the *source* agency.

For Off-site Access[42], sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;
(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and
(3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

43. What are the prohibited acts under the DPA?
See **Annex A** for the Table of Crimes

44. Is there a qualifying circumstance that would increase the penalties prescribed in the specific crimes provided under Chapter VIII?

Yes. in case there is the offense is *large-scale*. Sec. 35 provides: [T]he maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions[43].

45. In case of breach of the obligations above, including the commission of the prohibited acts, what is the extent of liability of each participant?

40 Section 23
41 Except as may be allowed through guidelines to be issued by the National Privacy Commission
42 Unless otherwise provided in guidelines to be issued by the National Privacy Commission
43 This pertains to the penalized acts under Sections 25 to 33.

Aside from imprisonment and fine, additional penalties are given to offenders. Sec. 37 provides that the "[r]estitution for any aggrieved party shall be governed by the provisions of the New Civil Code." Also, under Sec. 34, additional penalties are given:

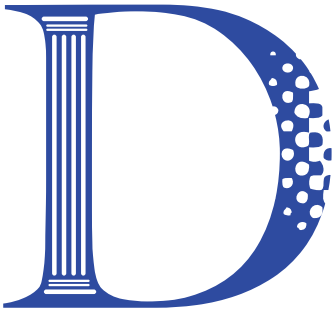
a) In the case of juridical person, "the court may suspend or revoke any of its rights under this Act."
b) In case the offender is an alien, "he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed."

Annex A

	Penalized Acts	Penalties	
		Prison Term	Fine*
Sec. 25	Unauthorized Processing of Personal Information	1-3 years	500,000 to 2 Million
	Unauthorized Processing of Sensitive Personal Information	3-6 years	500,000 to 4 Million
Sec. 26	Accessing Personal Information due to Negligence	1-3 years	500,000 to 2 Million
	Accessing Sensitive Personal Information due to Negligence	3-6 years	500,000 to 4 Million
Sec. 27	Improper Disposal of Personal Information	6 mos - 2 years	100,000 to 500,000
	Improper Disposal of Sensitive Personal Information	1-3 years	100,000 to 1 Million
Sec. 28	Processing of Personal Information for Unauthorized Purposes	1 yr and 6mos to 5 years	500,000 to 1 Million
	Processing of Personal Information for Unauthorized Purposes	2 - 7 years	500,000 to 2 Million
Sec. 29	Unauthorized Access or Intentional Breach	1-3 years	500,000 to 2 Million
Sec. 30	Concealment of Security Breaches involving Sensitive Personal Information	1 yr and 6mos to 5 years	500,000 to 1 Million
Sec. 31	Malicious Disclosure	1 yr and 6mos to 5 years	500,000 to 1 Million
Sec. 32	Unauthorized Disclosure of Personal Information	1-3 years	500,000 to 1 Million
	Unauthorized Disclosure of Sensitive Personal Information	3-5 years	500,000 to 2 Million
Sec. 33	Combination or Series of Acts	3-6 years	1 Million to 5 Million

*In pesos

DATA PRIVACY
PHILIPPINES



DISINI&DISINI
LAW OFFICE

Unit 320 Philippine Social Science Center,
Commonwealth Avenue, Diliman, Quezon City, 1101 PHILIPPINES

Phone: +632 454-5442 · +63 2 426-0486
Fax: +63 2 454-5442 ext. 102

Email: info@disini.ph