NATIONAL PRIVACY COMMISSION

THIRD EDITION

NPC PRIVACY TOOLKIT

A GUIDE FOR MANAGEMENT & DATA PROTECTION OFFICERS

DICT DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

PrivacyPH privacy.gov.ph www.privacy.gov.ph

NATIONAL
PRIVACY
COMMISSION

THIRD EDITION
May 2018

TABLE OF CONTENTS

MESSAGE FROM THE PRESIDENT

MALACAÑAN PALACE
MANILA

MESSAGE

My warmest greetings to the **National Privacy Commission (NPC)** as it holds its **First Data Protection Officers Assembly** and publishes the **Data Privacy Act of 2012 Compliance Manual**.

Developing a culture protective of citizens' data privacy, while ensuring the free flow of information, forms part of our government's commitment to serve and defend the Filipino people. This compliance manual will definitely be a significant step towards the attainment of our goal. I congratulate and thank the NPC for completing this project that will set the standards for concerned public and private agencies as they perform their respective mandates with integrity and efficiency.

I hope that, through this assembly, all data protection officers will have a better understanding of the Data Privacy Act of 2012. May you work closely together in helping our citizens have full control of their personal information in this digital age.

To all participants, may you continue to be excellent professionals who are dedicated to fortify the foundation of our nation. Hand in hand, let us empower ourselves and our countrymen so that we can accelerate our momentum towards genuine and lasting progress.

Congratulations on this historic milestone.

RODRIGO ROA DUTERTE

MANILA
5 April 2017

THE PRESIDENT OF THE PHILIPPINES

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

MESSAGE

Congratulations to the National Privacy Commission (NPC) on the successful launch of the first-ever Philippine National Data Privacy Conference in the country, and on the publication of the 2018 NPC Privacy Toolkit, the official handbook of Philippine data privacy professionals in the government and the private sector.

After the Data Privacy Act (DPA) was signed into law on August 15, 2012, it became state policy to further ensure protection not just of the people, but also of their personal data – by safeguarding the people's privacy rights in an era when civil liberties of individuals are endangered and could be abused easily by perpetrators of cybercrimes and data processing malpractices.

In creating the NPC, the law gave it ample authority to match and respond to its arduous tasks. It was, thus, created to function as a regulatory agency and independent quasi-judicial body attached to the Department of Information and Communications Technology (DICT).

What the law cannot provide, however, is the drive and zeal of Team NPC. And for this I commend the inspired leadership that guides the Commission. After more than two years of fulfilling its mandate, the burgeoning agency has proven its capacity to deliver quality public service. More importantly, the NPC has shown that it has what it takes to turn the DPA from a fine piece of legislation into a visible instrument for the common good.

The DICT will continue to extend its support to the Commission. May the NPC build a lasting legacy of excellent public service on its early successes.

To the men and women of NPC, the DICT is proud that we are one family!

Eliseo M. Rio, Jr.
Officer-in-Charge/Undersecretary for Special Concerns
Department of Information and Communications Technology

DICT Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63(02) 920-0101 www.dict.gov.ph

FOREWORD

First I would like to congratulate you for getting hold of the latest NPC Toolkit. This is an important tool that will guide you on your journey towards compliance with the Data Privacy Act or DPA of 2012 . This toolkit has gone through several revisions to make it more helpful for users like you.

This toolkit is for everyone wanting to comply with the DPA. My guess is that you are either the head or part of your agency's management group or someone who had just been appointed as your organization's Data Protection Officer or DPO to take an interest in this toolkit. Either role, you are performing a very important job for your organization in these exciting but challenging times. This is if you would take the lead in bringing what you will learn in this toolkit to the boardroom and in applying its concepts to your day to day operations.

As a DPO, you will be doing a lot of firsts for your organization and these would be very crucial in ensuring your organization's success today and more importantly, in securing its viability in the future. You will be building a whole new mindset and promoting a new culture of privacy within your organization using this toolkit.

On a personal level, being a DPO opens a whole new set of opportunities for you, locally and even globally. In a recent article by Reuters, it cited the data Protection Officer as the "hottest tech ticket in town" owing to the expected rush of demand for DPO's worldwide. But for now, I will help you first focus on how to help your organization comply with the DPA. Believe me, being successful in implementing the concepts contained in this toolkit within your organization is sufficient reward enough.

Respecting one's right to privacy should not be complicated. It really is a simple concept. It's about respect towards individuals, personal space, identity and choices. This simple definition has been distilled throughout history. Of course, the genesis of privacy could be traced to what the former US Supreme Justice Louis Brandeis wrote in his treatise that appeared in the Harvard Law Review in 1890. He wrote about the right to privacy and equated it as the, "right to be let alone"; he further described it as - " the most comprehensive of rights and the right most valued by civilized men".

Brandeis penned this 61 years before the birth of the World Wide Web but its relevance has grown over time, in proportion to the growth of technology. Given the volume and the rate by which our personal data is now being processed, data privacy protection has become such a big deal. Along with the benefits of data usage, are the possible abuse and misuse of personal data which may result in real harms including discrimination, unfair decision making, identity theft and loss of reputation.

Improper processing of information such as race, color, ethnic origin and sex brings about unequal treatment & opportunities for certain groups of people. For instance in the human resource field, studies found that hiring algorithms which factored in a job applicant's home address were found to possibly lead to racial discrimination. Fears over unfair decision making have also been persistent. Some observed that false assumptions negatively affected the credit score of some individuals. Concerns were also recently raised on how genetic information from an open-source genetic database was used as to find feasible "suspects" behind 12 deaths and at least 50 rapes in the US.

Directly affecting personal finances of data subjects is identity theft. The story of the school teacher whose identity was stolen when he posted his Professional Regulatory Commission ID online resulting in salary loans he did not authorize, is just one of the many cases of identity theft in the country.

Even worse is an organization'smishandling of personal data, which may cause grave and irreversible reputational damages to individuals. Such is what happened with the hack of the Ashley Madison portal, a dating site that connected individuals looking for potential extramarital partners. As 30 million personal records were leaked, including those of politicians, priests, celebrities and other public figures, marital troubles, resignations and suicides followed.

In the face of these 21st century crimes, a 21st century law that upholds data privacy was clearly needed. Thus, is the rationale of the Data Privacy Act.

As I'm sure you've read, the complete title of the Data Privacy Act or the DPA is: "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." To understand the DPA, you need to know what it protects and regulates; whom it protects and regulates; and the relationships it governs.

First, the DPA protects and regulates personal information. Broadly speaking, this means any information that can either directly, or indirectly, when combined with other information, identify an individual.

Second, the DPA protects the Data Subject, or the individual who is identified by personal information and regulates the personal information controller (PIC) and personal information processor (PIP), or the individuals or organizations that hold and process personal information.

Finally, the DPA governs the rights of data subjects to their personal information and the obligations of PIC/Ps necessary to protect them.

Combining all these points, data privacy means acknowledging the spectrum of rights of data subjects in the protection of their personal information, and enforcing the obligations of PIC/Ps who process them.

My job as the Privacy Commissioner is to make it easy for everyone to fulfill their obligations and assume accountability in protecting data privacy. Thus, this Privacy Toolkit was developed.

This toolkit is packed with practical information on how to start complying with the DPA using the 5 Pillars of Data Privacy Accountability and Compliance approach. It includes guidance in the form of circulars, advisories, detailed privacy impact assessment guide, privacy management program guide, privacy manual guide, privacy notice guide, consent guide, data sharing guide, among others. Specific sections of the toolkit focus on the 10-Point Accountability and Compliance Framework that further details how PICs and PIPs can integrate privacy into their day to day operations.

While I will certainly not turn a blind eye to abusive conduct, I see the NPC primarily as the driver of inculcating privacy as an organizational value among private businesses and public agencies. I do not want to paint an image of an oppressive regulatory body hell bent on engaging in a witch-hunt for potential targets. The NPC is here to help at every step of the way especially now while information privacy in our country is undergoing its formative years. I hope this toolkit helps us achieve this goal.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

CHAPTER I

DATA PRIVACY THREATS:
THINGS TO WATCH OUT FOR AS A DPO

THINGS TO WATCH FOR AS A DPO

Our generation saw a tectonic shift in what creates value in societies and economies. Resulting to the emergence of the digital economy as a driver of global growth. Data has come to replace oil as the greatest currency, prompting economists to hail it as "the new oil". Braving this new frontier are innovative governments and businesses. They utilized personal data to improve existing services, products and policies. In so doing, they ended up generating better alternatives and new leads for future growth. For the first time in history, we are able to use personal data to build a society responsive to the needs of all. Unfortunately, along with the good came the bad. And so we see today how criminals can hijack personal data for malicious ends.

Threats to data privacy come from various actors. They include state-sponsored, hacktivists and commercial actors. State-sponsored actors usually target organizations with proprietary data such as those involved in technology, pharmaceuticals or finance. They aim to gain sustained access to an organization's IT infrastructure. On the other hand, hacktivists are generally viewed as those who use technology hacking to promote a political agenda and effect social change. Commercial or fraud-oriented actors are highly equipped and knowledgeable threat actors primarily interested in money they include identity thieves and personal data marketers.

Thus, the practice of information security becomes essential in ensuring personal data protection. By definition, information security is the process of protecting physical and electronic information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.

However, information security has become a tough job for organizations. Technological advancements that interconnect the world in an unprecedented degree, also brings with it countless types of threats. Threats that undermine privacy arise every day while organizations still address threats which have long been existing. As the online realm infinitely evolves, organizations' shields should always be up and constantly upgraded.

Thus, the NPC lists the following items that you, as a DPO, should currently be on the look out for to secure your organizations' information and avoid data breaches. This section underscores not only the common attacks but also the internal factors that makes organizations vulnerable as well as the emerging platforms used by perpetrators.

A. Internal weaknesses

Organizations can sometimes get too concerned with investing in the most updated and best information security software there is. What they fail to realize, however, is that any software becomes useless when vulnerabilities within the organization are not addressed.

A.1. Employee negligence

Employees serve as one of, if not the primary asset of any organization. But they may also be an organization's major security weakness. Compared to the previous year, the 2016 Ponemon Institute Study found that employee negligence accounts for 25% of data breaches, globally.

Without even resorting to sophisticated methods, perpetrators can use your unwitting employees as "portal" for their attacks. Considering organizations' use of advanced security software, social engineering still proves to be a very cost-effective tactic for perpetrators. All they need to do is identify and target the weakest link in the organization's security chain, who are none other than

your careless employees.

Some of the common mistakes employees make include having *weak password, email, social media and web browsing practices.* Cybercriminals exploit employees who do not use passwords, who use simple and short passwords, who use the same password across different services and accounts, and those who carelessly share passwords with others. Employees clicking on suspicious email links, social media content and website advertisements are also the easiest entry points to perpetuate malicious attacks discussed in the succeeding sections. Organizations also get exposed by employees' *poor security habits* outside work such as the use of unsecured personal device to access work-related data, and the connection to unsecured wi-fi networks.

Careless handling of data also results in self-inflicted data breaches. An example would be the Woolworths Data Breach, which forced management to cancel over $1 million in gift cards after someone within the Australian grocery chain accidentally email a spreadsheet containing customer information and redeemable codes for around 8,000 gift cards to over 1,000 customers.

Employees also put their organizations at risk when they *disregard well-crafted ICT standards* and even the organization's IT team. Critical errors under this category include doing unauthorized system changes, plugging unknown devices, downloading software and disabling security features—all without the IT team's knowledge.

A.2. Weak or lack of Information Security Policy

To avoid data breaches, it is desirable that an organization's information security policies be always at par with emerging technology trends. Due to fast-paced changes, it is highly possible that no standards exist yet for handling these nascent practices. One such trend is the so-called *"Bring Your Own Device"* or BYOD.

Organizations allow BYOD in a desire to reduce costs and increase productivity, given the new-found IT self-sufficiency among employees. The setup allows employees to work and access corporate data using their own device, be it a laptop, ultrabook, tablet or smartphone. This frees up organizations from so much hardware, software, and device maintenance expenses. Presumably, it also empowers and motivates employees, given the ease, mobility, and flexibility of access that it makes possible. Organizations expect the resulting convenience and employee satisfaction to drive productivity levels up.

However, without adequate standards and employee preparations in place, BYOD puts corporate data at risk. This, especially in the absence of clear policies on who can access which data, and on what to do in case a personal device gets lost, stolen or compromised,

The lack of standards on the use of *thumb drives or USB flash drives* also poses a risk. It is a favorite storage device of perpetrators as it is small and concealable. Perpetrators can easily steal corporate data through these devices or use them to install malicious programs in computers.

Unrestricted access to certain corporate data also jeopardizes an organization's security. For instance, access to sensitive employee information should be exclusive to the human resources department. This would make it harder for perpetrators to turn an employee into a portal of attack.

B. Malicious attacks

B.1. Phishing

This is a type of social engineering attack where cybercriminals pose as legitimate representatives of reputable organizations. The intent is to trick employees into divulging sensitive information that may result in data breach, identity theft and financial loss. Perpetrators carry this out through email, instant messages, phone calls, chat rooms, SMS, fake banner ads, message boards, fake job search sites and browser toolbars.

Phishing.org enumerates the common features of phishing emails as follows:

"Too Good To Be True" - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably is!

Sense of Urgency - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.

Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.

Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!"

B.2. Malware

Malware is short for 'malicious software' which includes computer viruses, worms, Trojan horses, rootkit, ransomware, spyware, adware, scareware, among others. It is meant to infiltrate and infect computers to compromise device, disrupt service, steal data or monitor user activities. The common types of malware are described below:

Malware Type	Description
Virus	a type of malware that attaches itself to the program, executes itself and replicates itself by infecting other programs; may crash systems, acquire hard disk space or CPU time, spam email contacts, access private info, corrupt files or wipe data
Worm	similar to viruses but do not require a host program to spread and damage your computers
Trojan Horse	a malware that masquerades as a legitimate and harmless program; do not replicate themselves
Rootkit	an application or set of applications that enables administrator-level access to the victim's system while actively hiding its presence making it difficult to detect; allows perpetrator to execute files, access logs, monitor user activity and change computer's configuration
Ransomware	blocks victims' access to their files by locking the system's screen or encrypting victims' files; requires victims to pay a ransom to get back their files through a decrypt key
Spyware	a malware that collects information about victims' surfing habits, browsing history and other personal information, and passes this information to third parties through the internet
Adware	attached and downloaded with other software, designed to display unwanted advertisements in the form of pop-up windows; may collect marketing-type data about you to customize advertisements displayed
Scareware	a malware that deceives victims to download and purchase fake and potentially dangerous software using intimidating, unsettling and fear messages

B.3.Denial-of-Service

A denial-of-service or DoS attack seeks to disrupt a network's service and make it unavailable to its intended and legitimate users. This is done by flooding the network with useless traffic until it overwhelms the resources and crashes the system. Zeltser.com lists the following as common motives behind DoS attacks:

> "*Extortion via a threat of a DoS attack:* The attacker might aim to directly profit from his perceived ability to disrupt the vi ctim's services by demanding payment to avoid the disruption.
>
> *Turf wars and fights between online gangs:* Groups and individuals in engaged on Internet-based malicious activities might use DoS as weapons against each other's infrastructure and operations, catching legitimate businesses in the crossfire.

> *Anticompetitive business practices:* Cybercriminals sometimes offer DoS services to take out competitor's websites or otherwise disrupt their operations.
>
> *Punishment for undesired actions:* A DoS attack might aim to punish the victim for refusing an extortion demand or for causing disruption to the attacker's business model (e.g., spam-sending operations).
>
> *Expression of anger and criticism:* Attackers might use the DoS attack as a way of criticizing the company or government organization for exhibiting undesirable political or geopolitical, economic or monetary behaviors.
>
> *Training ground for other attacks:* Attackers sometimes might target the organization when fine-tuning DoS tools and capabilities for future attacks, which will be directed at other victims.
>
> *Distraction from other malicious actions:* Adversaries might perform a DoS attack just to draw your attention away from other intrusion activities that they perform elsewhere in your environment.
>
> *Self-induced:* Some downtime and service disruptions are the result of the non-malicious actions that the organization's employees took by mistake (e.g., a server configuration problem).
>
> *No apparent reason at all:* Unfortunately, many DoS victims never learn what motivated the attack."

In 2016, the largest DoS attacks were recorded. One hit the servers of Dyn that brought down Twitter, the Guardian, Netflix, Reddit, CNN, among other sites in Europe and US. This was carried out through a distributed DoS (DDoS) that utilized multiple devices infected with a special malware, called 'botnet'. A botnet is a group of inter-connected devices infected with malware to enable perpetrators to control the devices without the owners' knowledge. Around 100,000 malicious endpoints were estimated to have powered this 1.2Tbps-strong attack.

B.4. Man-in-the-Middle

This is an attack designed to intercept communication between two parties, say a consumer and a website, in an attempt to impersonate both parties and steal valuable personal information.

It takes advantage of the weaknesses in the authentication protocols used by the parties. MITM, usually used to commit financial fraud, may be done via Wi-Fi connection, browser, mobile, app, cloud or through any networked device.

C. Emerging attack platforms

C.1. Mobile

As a widely-used platform even in the workplace, mobile serves as a huge attack surface for perpetrators. The breadth of data found in mobile devices – contact information, photos, emails

and other sensitive data, also makes them a primary attack target. The relative security weakness of mobile compared to personal computers increases its vulnerability.

Symantec estimated that the overall volume of malicious Android apps grew by 105 percent in 2016 at 18.4 million. Meanwhile, the iOS operating system remains to be rarely attacked, but experienced one in 2016 through the Pegasus spyware. Clicking the malicious link sent via text message jailbreaks the phone and injects the malware into it. Pegasus accesses messages, calls and emails, and also gathers app information from services like Gmail, Facebook, Skype and WhatsApp.

C.2. Cloud

Similar to BYOD, cloud adoption in organizations has been on the rise. It is seen as a cost-efficient and effective measure to meet heightened computing needs. As cloud shifts organizations' data and applications over high-capacity networks hosted in the internet, it helps reduce infrastructure and maintenance cost and improve manageability. However, it also serves as a new and easily accessible threat surface for perpetrators.

The borderless nature of cloud computing allows threat actors to easily bypass organization-wide security policies. Cloud's dependence on third party applications also increases users' exposure to malware. In its 2016 report, the Cloud Security Alliance identified 12 critical cloud issues including: data breaches; weak identity, credential and access management; insecure application program interfaces; system and application vulnerabilities; account hijacking; malicious insiders; advanced persistent threats; data loss, insufficient due diligence; abuse and nefarious use of cloud services; DOS; and shared technology issues.

C.3. Internet of things

The internet of things or IoT is the concept of interconnectedness of physical devices ranging from cellphones, cars, ovens, washing machines, headphones, lamps, to wearable devices, via the internet. It espouses people-people, people-things and things-things relationships, intended to improve efficiency and promote a smart approach in doing things.

While the IoT opens the world to countless opportunities, it also presents serious challenges. One is the perceived weak security of most IoT devices, which are protected by factory default or hardcoded user names and passwords. The largest DDoS attacks in 2016 using Mirai, as discussed in the previous section, exploited IoT devices and converted them into bots. The seemingly harmless webcams produced by Chinese electronics firm Xiong Mai Technologies primarily powered the 1.2Tbps-strong attack on Dyn. Citizens become unaware

D. Combatting Data Privacy Threats

The National Privacy Commission has devised various means to address the above threats. These means are integrated into the "Five Pillars of Data Privacy Accountability and Compliance", as discussed in the succeeding sections. This framework is not only meant to combat data privacy threats, but to also help personal information controllers and processors comply with the Data Privacy Act of 2012. Encompassing organizational, physical and technical measures, the framework is aimed at helping develop an organizational culture protective of privacy.

CHAPTER II THE FIVE PILLARS OF DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE

NPC Advisory No. 2017-01

DATE : 14 MARCH 2017
SUBJECT : DESIGNATION OF DATA PROTECTION OFFICERS

Preamble

WHEREAS, Article II, Section 24 of the 1987 Constitution provides that the State recognizes the vital role of communication and information in nation-building. At the same time, Article II, Section 11 thereof stresses that the State values the dignity of every human person and guarantees full respect for human rights. Finally, Article XIII, Section 21 states that Congress shall give highest priority to the enactment of measures that protect and enhance the right of the people to human dignity;

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it 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. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, Section 21(b) of the DPA and Section 50(b) of its Implementing Rules and Regulations (IRR) provide that personal information controllers (PICs) shall designate an individual or individuals who are accountable for the organization's compliance with this Act. Section 14 of the DPA and Section 45 of the IRR also require personal information processors (PIPs) to comply with all the requirements of the Act and other applicable laws, including issuances by the NPC;

WHEREAS, pursuant to Section 26(a) of the IRR, any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer (DPO), compliance officer, or shall otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes ensuring compliance with the provisions of the DPA and with international standards for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, Section 4 of NPC Circular 2016-01 declares that a government agency engaged in the processing of personal data shall, through its head of agency, designate a DPO;

WHEREAS, in consideration of the foregoing premises, the NPC hereby issues this Advisory that prescribes the guidelines for the designation of a DPO:

Scope

These Guidelines shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject

to the applicable provisions of the DPA, its IRR, and issuances by the NPC.

Definition of Terms

Whenever used in this Advisory, the following terms shall have their respective meanings as hereinafter set forth:

a. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

b. "Commission" or "NPC" refers to the National Privacy Commission;

c. "Compliance Officer for Privacy" or "COP" refers to an individual or individuals who shall perform some of the functions of a DPO, as provided in this Advisory;

d. "Conflict of Interest" refers to a scenario wherein a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO. This includes, inter alia, holding a position within the PIC or PIP that leads him to determine the purposes and the means of the processing of personal data. The term shall be liberally construed relative to the provisions of this Advisory;

e. "Data Sharing Agreement" refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: Provided, that only personal information controllers shall be made parties to a data sharing agreement;

f. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

g. "Government Agency" refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

h. "Personal data" refers to all types of personal information, including privileged information;

i. "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, or when put together with other information would directly and certainly identify an individual;

j. "Personal information controller" or "PIC" 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; or
2. an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

k. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

l. "Privacy by Design" is an approach to the development and implementation of projects, programs, and processes that integrates into the latter's design or structure safeguards that are necessary to protect and promote privacy, such as appropriate organizational, technical, and policy measures;

m. "Privacy Impact Assessment" is a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure;

n. "Privileged Information" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication;

o. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

p. "Sensitive Personal Information" refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such 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.

General Principles

These Guidelines shall be governed by the following general principles:

a. The responsibility for complying with the Act, its IRR, issuances by the NPC, and all other applicable laws lies with the PIC or PIP.[1] When necessary, it must be capable of demonstrating its capacity to comply.

b. The DPO or COP shall act independently in the performance of his or her functions, and shall enjoy sufficient degree of autonomy. For this purpose, he or she must not receive instructions[2] from the PIC or PIP regarding the exercise of his or her tasks.

c. The DPO or COP is bound by secrecy or confidentiality concerning the performance of his or her tasks.

1 RA 10173, §21(a), and §14.
2 e.g., what results should be achieved, how to investigate a complaint, whether to consult the NPC, what view or interpretation of the law to take relative to a specific data protection issue, etc.

Mandatory Designation

A PIC or PIP shall designate an individual or individuals who shall function as DPO. The DPO shall be accountable for ensuring the compliance by the PIC or PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulations relating to privacy and data protection.
In certain cases, a PIC or PIP is allowed to designate a compliance officer for privacy (COP):

a. Local Government Units (LGUs). Each LGU shall designate a DPO. However, a component city, municipality, or barangay is allowed to designate a COP, provided that the latter shall be under the supervision of the DPO of the corresponding province, city, or municipality that that component city, municipality or barangay forms part of.

b. Government Agencies. Each government agency shall designate a DPO. Where a government agency has regional, provincial, district, city, municipal offices, or any other similar sub-units, it may designate or appoint a COP for each sub-unit. The COPs shall be under the supervision of the DPO.

c. 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.

d. Other Analogous Cases. PICs or PIPs that are under similar or analogous circumstances may also seek the approval of the NPC for the appointment or designation of a COP, in lieu of a DPO.

An individual PIC or PIP shall be a de facto DPO.

General Qualifications

The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security and/or data protection needs.

Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.

The minimum qualifications for a COP shall be proportionate to his or her functions, as provided in this Advisory.

Position of the DPO or COP

The DPO or COP should be a full-time or organic employee of the PIC or PIP.

In the government or public sector, the DPO or COP may be a career or appointive position.

In the private sector, the DPO or COP should ideally be a regular or permanent position.[3] Where the employment of the DPO or COP is based on a contract, the term or duration thereof should at least be two (2) years to ensure stability.
In the event the position of DPO or COP is left vacant,[4] the PIC or PIP should provide for the appointment, reappointment, or hiring of his or her replacement within a reasonable period of time. The PIC or PIP may also require the incumbent DPO or COP to occupy such position in an holdover capacity until the appointment or hiring of a new DPO or COP, in accordance with the PIC or PIP's internal policies or the provisions of the appropriate contract.

Independence, Autonomy And Conflict of Interest

A DPO or COP must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the PIC or PIP.

In his or her capacity as DPO or COP, an individual may perform (or be assigned to perform) other tasks or assume other functions[5] that do not give rise to any conflict of interest.

Duties and Responsibilities Of the DPO and COP

A DPO shall, inter alia:

a. monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:
   1. collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
   2. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
   3. inform, advise, and issue recommendations to the PIC or PIP;
   4. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
   5. advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

c. advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

d. ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

e. inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;

3 Consultants and project, seasonal, probationary, or casual employees should not be designated as DPOs
4 In the event of resignation, incapacity, or death of the DPO, or, where the term of the DPO is fixed or is coterminous with the appointing authority, in the case of government agencies, or based on a contract, in the case of private sector entities.
5 The designated DPO may also occupy some other position in the organization (e.g., legal counsel, risk management officer, etc.).

f. advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

g. serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;

h. cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

i. perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

Except for items (a) to (c), a COP shall perform all other functions of a DPO. Where appropriate, he or she shall also assist the supervising DPO in the performance of the latter's functions.

The DPO or COP must have due regard for the risks associated with the processing operations of the PIC or PIP, taking into account the nature, scope, context and purposes of processing. Accordingly, he or she must prioritize his or her activities and focus his or her efforts on issues that present higher data protection risks.

General Obligations of the PIC or PIP Relative to the DPO or COP

The PIC or PIP should:

a. effectively communicate to its personnel, the designation of the DPO or COP and his or her functions;

b. allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;

c. provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;

d. grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;

e. where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;

f. promptly consult the DPO or COP in the event of a personal data breach or security incident; and

g. ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.

Outsourcing or Subcontracting of Functions

A PIC or PIP may outsource or subcontract the functions of its DPO or COP. However, to the extent possible, the DPO or COP must oversee the performance of his or her functions by the third-party service provider or providers. The DPO or COP shall also remain the contact person of the PIC or PIP vis-à-vis the NPC.

Protections

To strengthen the autonomy of the DPO or COP and ensure the independent nature of his or her role in the organization, a PIC or PIP should not directly or indirectly penalize or dismiss the DPO or COP for performing his or her tasks. It is not necessary that the penalty is actually imposed or meted out. A mere threat is sufficient if it has the effect of impeding or preventing the DPO or COP from performing his or her tasks. However, nothing shall preclude the legitimate application of labor, administrative, civil or criminal laws against the DPO or COP, based on just or authorized grounds

Publication and Communication Of Contact Details

To ensure that its own personnel, the data subjects, the NPC, or any other concerned party, is able to easily, directly, and confidentially contact the DPO or COP, a PIC or PIP must publish the DPO's or COP's contact details in, at least, the following materials:

a. website;
b. privacy notice;
c. privacy policy; and
d. privacy manual or privacy guide

A PIC or PIP may introduce or offer additional means of communicating (e.g., telefax, social media platforms, etc.) with its DPO or COP.
For this purpose, the contact details of the DPO or COP should include the following information:

a. title or designation
b. postal address
c. a dedicated telephone number
d. a dedicated email address

The name or names of the DPO or COP need not be published. However, it should be made available upon request by a data subject or the NPC.

Weight of Opinion

The opinion of the DPO or COP must be given due weight. In case of disagreement, and should the PIC or PIP choose not to follow the advice of the DPO or COP, it is recommended, as good practice, to document the reasons therefor.

Accountability

While the responsibility of complying with the DPA, its IRR, issuances by the NPC, and other applicable laws remains with the PIC or PIP, malfeasance, misfeasance, or nonfeasance on the part of the DPO or COP relative to his designated functions may still be a ground for administrative, civil, or criminal liability, in accordance with all applicable laws.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Date: 14 March 2017

RECORDS OF PROCESSING ACTIVITIES

Name of Organization:			
Email:		**Contact Number:**	
Data Protection Officer:			
Contact Details:	**Email:**		
	Contact Number:		
Joint Controllership: (If aaplicable)			

NO.	NAME *(State the name of the data processing system)*	DATA SUBJECTS *(Check and specify the data subjetcs)*
		☐ Employees ☐ Clients ☐ Students ☐ Employees ☐ Clients ☐ Students
		Others: (Please State)

PURPOSE OF PROCESSING (State the information about the purpose of the processing of personal data, including any intended future processing or data sharing.)

TYPE OF SYSTEM			MANAGING AS			SUBCONTRACTED		
☐ Manual	☐ Electronic	☐ Both	☐ PIC	☐ PIP	☐ Both	☐ YES	☐ NO	

GENERAL INFORMATION (State the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data. List all personal data (e.g. Personal Full Name, address, gender, phone number, etc.,) and state which is/are the sensitive personal information (e.g. race, ethnicity, marital status, health, genetic, government issued numbers).)

DESCRIPTION OF SECURITY MEASURES (State a general description of the security measures in place.)

TO WHOM WILL THE PERSONAL DATA BE DISCLOSED THROUGHOUT THIS PROCESSING ACTIVITY? (State to whom will the personal data be disclosed.)

2. KNOW YOUR RISKS:

CONDUCT A PRIVACY IMPACT ASSESSMENT

NPC Advisory No. 2017-03

DATE : 31 July 2017
SUBJECT : GUIDELINES ON PRIVACY IMPACT ASSESSMENTS

Preamble

WHEREAS, Article II, Section 11 of the 1987 Constitution declares that the State values the dignity of every human person and guarantees full respect for human rights, and Article XIII, Section 21 states that Congress shall give highest priority to the enactment of measures that protect and enhance the right of the people to human dignity. At the same time, enshrined in jurisprudence is the recognition of the right to privacy as a right fully deserving of constitutional protection;

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it 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. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, Section 20(c) of the DPA and Section 29 of its Implementing Rules and Regulations (IRR) provide that the determination of the appropriate level of security for an agency or organization processing personal data shall take into account the nature of the personal information to be protected, the risks represented by the processing to the rights and freedoms of data subjects, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is mandated to administer and implement the provisions of the DPA, monitor and ensure compliance of the country with international standards set for data protection, and coordinate with government agencies and the private sector on efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country;

WHEREAS, Sections 4, 5, and 6 of NPC Circular 2016-01 requires government agencies to conduct a Privacy Impact Assessment (PIA) for each program, process, or measure within the agency that involves personal data. At the same time, Section 6 of NPC Circular 2016-03 recommends the conduct of a PIA as part of any organization's security incident management policy.

WHEREFORE, in consideration of the foregoing premises, the NPC hereby issues this Advisory that prescribes guidelines for the conduct of a Privacy Impact Assessment:

Scope

This Advisory shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and other relevant issuances of the NPC

Definition of Terms

For the purpose of this Advisory, the following terms are defined, as follows:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
B. "Commission" or "NPC" refers to the National Privacy Commission;

C. "Compliance Officer for Privacy" or "COP" refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01;

D. "Control Framework" refers to a comprehensive enumeration of measures a PIC or PIP has established for the protection of personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination;

E. "Data Protection Officer" or "DPO" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: Provided, that, except where allowed otherwise by law or the Commission, the individual must be an organic employee of the government agency or private entity: Provided further, that a government agency or private entity may have more than one DPO;

F. "IRR" refers to the Implementing Rules and Regulations of the DPA;

G. "Personal data" refers to all types of personal information, including privileged information;

H. "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, or when put together with other information would directly and certainly identify an individual;

I. "Personal information controller" or "PIC" 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; or
    2. an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs;
    3. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

J. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

K. "Privacy Impact Assessment" is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology

product of a PIC or PIP program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations;

L. "Privacy Management Program" refers to a process intended to embed privacy and data protection in the strategic framework and daily operations of a personal information controller or personal information processor, maintained through organizational commitment and oversight of coordinated projects and activities.

M. "Privileged Information" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication;

N. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

O. "Risk" refers to the potential of an incident to result in harm or danger to a data subject or organization;

P. "Risk Rating" refers to a function of the probability and impact of an event;

Q. "Sensitive Personal Information" refers to personal information:

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

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

R. "Threat" refers to a potential cause of an unwanted incident, which may result in harm or danger to a data subject, system, or organization;

S. "Vulnerability" refers to a weakness of a data processing system that makes it susceptible to threats and other attacks.

General Principles

A Privacy Impact Assessment (PIA) helps a PIC and PIP navigate the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

The identification of risks and the use of a control framework for risk management should consider existing laws, regulations, and issuances relevant to privacy and data protection, as well as the rights of data subjects. The most appropriate standard recognized by the sector or industry of the PIC or PIP, as well as that of the information and communications technology industry shall also be considered.

Key Considerations

In general, a PIA should be undertaken for every processing system of a PIC or PIP that involves personal data. It may also be carried out vis-à-vis the entire organization of the PIC or PIP with the involvement or participation of the different process owners and stakeholders.

A PIA should be conducted for both new and existing systems, programs, projects, procedures, measures, or technology products that involve or impact processing personal data. For new processing systems, it should be undertaken prior to their adoption, use, or implementation. Changes in the governing law or regulations, or those adopted within the organization or its industry may likewise require the conduct of a PIA, particularly if such changes affect personal data processing.

A PIC may require a PIP or a service or product provider to conduct a PIA. For this purpose, the report prepared by the PIP or the service or product provider may be considered by the PIC in determining whether the former is able to provide a comparable level of protection to the processing of personal data.

A PIC or PIP may choose to conduct a single PIA for multiple data processing systems that involve the same personal data and pose similar risks. A single PIA may also be conducted on a data processing system where two or more PICs or PIPs are involved.

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.

Objectives

The conduct of a PIA is intended to:

A. identify, assess, evaluate, and manage the risks represented by the processing of personal data;

B. assist the PIC or PIP in preparing the records of its processing activities, and in maintaining its privacy management program;

C. facilitate compliance by the PIC or PIP with the DPA, its IRR, and other applicable issuances of the NPC, by determining:

   a. its adherence to the principles of transparency, legitimate purpose and proportionality;
   b. its existing organizational, physical and technical security measures relative to its data processing systems;
   c. the extent by which it upholds the rights of data subjects; and

D. aid the PIC or PIP in addressing privacy risks by allowing it to establish a control framework;

In conducting a PIA, it is important that its results are properly documented in a report that includes information on stakeholder involvement, proposed measures for privacy risk management, and the process through which the results of the PIA will be communicated to internal and external stakeholders.

Responsibility

The PIC or PIP is primarily accountable for the conduct of a PIA. This responsibility remains even when it elects to outsource or subcontract the actual conduct of the activity. For this purpose, the PIC or PIP may lay down a policy, which establishes the circumstances under which a PIA shall be carried out, including the personnel involved, the resources available, and the review process that will be undertaken.

A recommendation for the conduct of a PIA may also come from the DPO of the PIC or PIP. Part of the functions of a DPO is to ensure the conduct of PIA relative to activities, measures, projects, programs, or systems of the PIC or PIP. In case of disagreement between the DPO and its principal on the conduct of a PIA, this should be properly documented, particularly the reason for the conflicting views.

The extent of the involvement of the DPO in the PIA is left to the discretion of the PIC or PIP. The PIC or PIP may allow the DPO to actively take part in the PIA, or it may simply consult and seek his or her recommendations based on the results of the PIA.

Where the PIC or PIP has a COP, the involvement of the latter in the PIA shall also be determined by the PIC or PIP.

Stakeholder Involvement

Stakeholder involvement is important in the conduct of a PIA. This may be accomplished through their direct participation in the process, through consultations in a public forum or focus group discussions, or through the use of surveys and feedback forms.

Stakeholders may be involved in the whole process, or may be consulted for specific stages, such as in preparatory stage, during risk analysis and evaluation, or after the process during review that leads up to the preparation of the report.

The results of a PIA should be communicated to the stakeholders via a written report.

Structure and Form

There is no prescribed standard or format for a PIA. As such, the PIC or PIP may determine the structure and form of the PIA that it will use. It is not precluded from utilizing any existing methodology,[6] provided the latter is acceptable based on the following criteria:[7]

6 Acceptable methodologies include ISO/IEC 29134, which provides standards for the conduct of the PIA.
7 This takes into consideration Art 29 Data Protection Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (4 April 2017) and the provisions of the DPA.

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

    1. purpose of the processing, including, where applicable, the legitimate interest pursued by the PIC or PIP;
    2. data inventory identifying the types of personal data held by the PIC or PIP;
    3. sources of personal data and procedures for collection;
    4. 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;
    5. transfers of personal data to another agency, company, or organization, including transfers outside the country, if any;
    6. storage and disposal method of personal data;
    7. accountable and responsible persons involved in the processing of personal data; and
    8. existing organizational, physical and technical security measures

2. 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.

3. 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.

    1. *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.
    2. *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.
    3. *Remedial measures.* Based on an assessment of risks, measures should be proposed on how to address and manage the said risks.

4. It is an inclusive process, in that it ensures the involvement of interested parties and secures inputs from the DPO and data subjects.

Planning a PIA

The following should be considered when planning the conduct of a PIA:

1. The PIC or PIP should signify its commitment to the conduct of a PIA. This means:

    a. deciding on the need for a PIA;
    b. assigning a person responsible for the whole process;
    c. providing resources to accomplish the objectives of the PIA; and
    d. issuing a clear directive for its conduct.

2. The program, project, process, measure, system or technology product on which a PIA will be conducted should be identified. The scope of the PIA must be clearly delineated.

3. The process owners, participants, and the persons in charge of conducting the PIA, including

the preparation of its report, should be identified. When the scope of the PIA is determined to be broad and/or comprehensive, a taskforce or secretariat may be necessary. The PIC or PIP may also outsource the conduct of the PIA, but great care should be taken in evaluating the adequacy and propriety of the methodology that will be utilized, and the expected outputs.

4. The PIC or PIP should determine how internal and external stakeholders will be involved.

5. Other matters that should be established:

    1. objectives, schedules, and available resources;
    2. means of communicating the results of the PIA to stakeholders; and
    3. procedure for integrating the recommendations of the PIA into the control framework of the organization.

Preparatory Activities

The following should be considered in the preparatory activities leading up to the conduct of a PIA:

1. There should be records of the processing activities of the PIC or PIP, and an inventory of the personal data involved in such activities. For this purpose, a personal data flow should be created, starting from the collection of personal data, all the way up to its deletion or disposal, including storage. The process owners may be assigned to provide these documents prior to conduct of the PIA.

2. A preliminary assessment should be undertaken to determine baseline information, including existing policies and security measures of the organization. It is critical that this be carried out in coordination with the different units or offices of the organization, such as those in charge of compliance, quality management, records and information management, information technology, administration and planning, customer relations, and legal concerns.

3. Stakeholders may be consulted during the preparatory stage to identify their concerns, expectations, and perception of the risks posed by the processing activities of the organization. Existing reports may be considered, such as customer satisfaction surveys, internal audits, and other assessment activities.

4. The objectives, scope, and methodology of the PIA should be established. A control framework should be selected. For agencies that process the personal data records of more than one thousand (1,000) individuals, including agency personnel, the Commission recommends the use of the ISO/IEC 27002 and ISO/IEC 29151 control set as the minimum standard to assess any gaps in the agency's control framework.

5. The detailed plan for the conduct of the PIA should be prepared, including:

    1. schedules and timelines for the completion of preparatory activities, conduct of the PIA, and reporting or publication of results;
    2. approval of resource and budget allocations;
    3. participants and methods for stakeholder involvement;
    4. documentation and review process;
    5. other supporting documents.

Conduct of the PIA

The following should be considered in the conduct of a PIA:

1. The records of processing activities, the personal data inventory, and the personal data flows should all be evaluated to determine whether additional information are necessary for the proper conduct of a PIA. Taken together, these constitute the baseline information, along with the following:

    1. purpose and legal basis of the processing activities, including data sharing and other forms of data transfers.;
    2. persons responsible for processing personal data, including a list of those individuals with access thereto;
    3. list of all information repositories and technology products used;
    4. sources and recipients of personal data; and
    5. existing policies, procedures and security measures relevant to personal data protection.

2. Once baseline information is complete, the processing activities should be evaluated against the legal obligations of the PIC or PIP, and the latter's chosen control framework.

3. The control framework should adhere to the data privacy principles. It should implement security measures and establish procedures for the proper exercise by data subjects of their rights. Privacy and data protection measures, whether planned and existing, should be considered.

4. The data processing systems of the PIC or PIP should be assessed to determine if there are gaps at any stage of the processing. There is a gap when:

    1. there is a violation of any data privacy principle;
    2. the organizational, physical, and technical security measures are inadequate to safeguard the confidentiality, availability, and/or integrity of personal data; or
    3. the exercise of data subjects of their rights is not possible or restricted without legal basis.

5. Gaps should be evaluated to determine the risks involved to personal data, possible threats, and existing vulnerabilities of the systems. Risks include the following:

    1. unauthorized or unlawful processing;
    2. confidentiality breach;
    3. integrity breach;
    4. availability breach; and
    5. violations of rights of data subjects

6. Risks, in turn, should be assessed to determine whether the breach or privacy violation it poses is likely to happen. The assessment should consider the processing operations of the PIC or PIP, vulnerabilities and threats, as well as existing safeguards, if any. A determination of how the risk will affect the rights and freedoms of data subjects should be done based on the amount and nature of personal data involved, and the impact of possible harm.

7. Measures to address the risks identified should be proposed. They may mitigate, accept, avoid, or transfer the risks posed by the processing, by taking into account the likelihood and impact of a breach or privacy violation, the available resources of the organization to address the risks, current data privacy best practices, and industry or sector standards. The proposed measures should include:

    1. risks and strategies for risk management;
    2. implementing activities, including definite plans and specific projects;
    3. controlling mechanisms to monitor, review, and support implementation;
    4. proposed time frame, expected completion, or schedules;
    5. responsible and accountable persons; and
    6. necessary and available resources.

8. Involvement of stakeholders should be documented.

9. The report featuring the results of the PIA should be reviewed before being finalized and approved. It should include the proposed measures that should serve as basis for implementing changes in the organization (e.g., new policies and procedures, security measures to strengthen data processing systems, etc.). The report should also include recommendations as to when the PIA will be updated and reviewed.

10. Results of the PIA should be reported to management and communicated to internal and external stakeholders. The PIC or PIP can limit the information provided to the public based on its legitimate interests, such as the legal, business operation, or security risks that disclosure may give rise to.

Documentation and Review

A PIA requires documentation and procedures for review. Its results should be contained in a corresponding report.

The PIC or PIP must maintain a record of all its PIA reports. When a report contains information that are privileged or confidential, the PIC or PIP may prepare a PIA Summary that can be made available to data subjects upon request. Other means of communicating the results of the PIA to internal and external stakeholders should be considered, such as publishing key findings or result summaries in the PIC or PIP website, through newsletters, annual reports, and other similar materials.
A PIA should be evaluated every year. This, however, does not preclude the conduct of a new PIA on the same data processing system, when so required by significant changes required by law or policy, and other similar circumstances.

Compliance and Accountability

The conduct of a PIA is one of the ways a PIC or PIP is able to demonstrate its compliance with the DPA, its IRR, and related issuances of the NPC. It also represents a proactive approach to the management of risks represented by personal data processing by ensuring that the rights of data subjects are protected.

In the event a personal data breach occurs, or a complaint is filed by a data subject against the PIC or PIP, the conduct of a PIA shall be considered in evaluating if the PIC or PIP exercised due diligence in the processing of personal data.

When the NPC determines that a processing system of a PIC or PIP poses a significant risk to the rights

and freedoms of data subjects, it may request for a copy of the PIA report regarding such system. When so requested, such copy shall also be made available to the Commission for compliance monitoring purposes.

Approved:

[SGD] RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Date: 31 July 2017

PRIVACY IMPACT ASSESSMENT

Overview

A Privacy Impact Assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes personal information and in consultation with stakeholders, for taking actions as necessary to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001.

A PIA is more than a tool: its process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed. Initiatives vary substantially in scale and impact.[1]

This document is intended to provide scalable guidance that can be applied to all initiatives. Since guidance specific to all circumstances cannot be prescriptive, the guidance in this document should be interpreted with respect to individual circumstance. A Personal Information Controller may have a responsibility to conduct a PIA and may request a Personal Information Processor to assist in doing this, acting on the Personal Information Controller's behalf. A Personal Information Processor or a third party may also wish to conduct their own PIA.

1 ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment

Privacy Impact Assessment GUIDE

I. Project/System Description

a.Description

Describe the program, project, process, measure, system or technology product and its context. Define and specify what it intends to achieve. Consider the pointers below to help you describe the project.

- Brief Description of the project/system
  - Describe the process of the projects
  - Describe the scope and extent
  - Any links with existing programs or other projects
- The system/project's overall aims (purpose of the project/system)
  - What is the project/system aims to achieve?
  - What are the benefits for the organizations and data subjects?
- Any related documents to support the projects/system
  - Project/System Requirements Specification
  - Project/System Design Specification
  - Or any related documents

b. Scope of the PIA

This section should explain, what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover.

- What will the PIA cover?
- What areas are outside scope?
- Is this just a "desk-top" information gathering exercise, do I have to get information from a wide variety of sources?
- Who needs to be involved and when will they be available?
- Where does the PIA need to fit in the overall project plan and timelines?
- Who will make decisions about the issues identified by the PIA? What information do they need and how long will it take to get sign-off from them?
- Do I need to consult with anyone (for instance the individuals whose personal information the project will involve)? When and how should this happen?
- Are there any third parties involved and how long do I need to allow for them to play their part?

II. Threshold Analysis

The following questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

a. Will the project or system involve the collection of new information about individuals?

O No O Yes

b. Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?

O No O Yes

c. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

O No O Yes

d. Will the initiative require you to contact individuals in ways which they may find intrusive?

O No O Yes

e. Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?

O No O Yes

f. Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)?

O No O Yes

g. Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

O No O Yes

h. Are the personal data collected prior to August 2016?

O No O Yes

III. Stakeholder(s) Engagement

State all project stakeholders, consulted in conducting PIA. Identify which part they were involved. (Describe how stakeholders were engaged in the PIA process)

Name	Role	Involvement	Inputs/ Recommendations
*			

** add additional rows if needed.*

IV. Personal Data Flows

Sample Data Flow

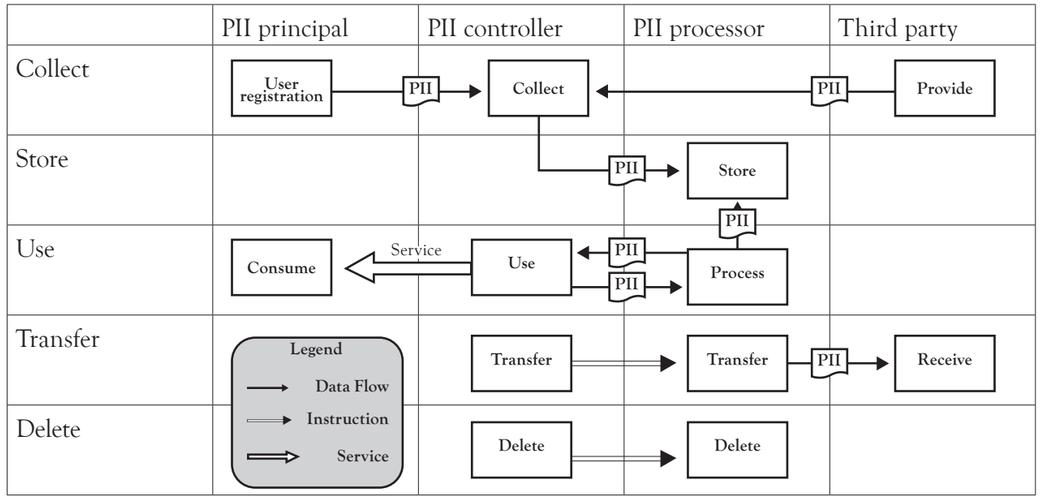


Figure 1. Information flow of personal information can be visualized in a work flow diagram on personal information processing.

- **Objective:** To identify information flows of personal information under assessment.
- **Input:** Description of the process and information system to be assessed.
- **Expected output:** Summary of findings on the information flow of personal information within the process.
- **Actions:** The person responsible for conducting a PIA should consult with others in the organization and perhaps external to the organization to describe the personal information flows and specifically:
  - how personal information is collected and the related source;
  - who is accountable and who is responsible within the organization for the personal information processing;
  - for what purpose personal information is processed;
  - how personal information will be processed;
  - personal information retention and disposal policy;
  - how personal information will be managed and modified;
  - how will personal information processors and application developers protect personal information;
  - identify any personal information transfer to jurisdictions where lower levels of personal information protection apply;
  - whether applicable, notify the relevant authorities of any new personal information processing and seek the necessary approvals.

Output of this process in terms of the information flow of personal information should be documented in the PIA report

- Implementation Guidance:

  Use of personal information (or transfer of personal information) may include approved data sharing flows of personal information to other parties.

  As an input to the PIA, the organization should describe the information flow in as detailed a manner as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, privacy related regulations, e.g. telecommunications acts. The whole personal information life cycle should be considered.

Identify the personal data involved and describe the data flow from collection to disposal by answering the following questions below:

What personal data are being or will be processed by this project/system?

List all personal data (e.g. Personal Full Name, address, gender, phone number, etc.,) and state which is/are the sensitive personal information (e.g. race, ethnicity, marital status, health, genetic, government issued numbers).

All the information stated above will be in accordance to the next section.

Collection

1. State who collected or will be collecting the personal information and/or sensitive information.

2. How the personal information/sensitive personal information is collected and from whom it was collected?
   - » *If personal information is collected from some source other than the individual?*

3. What is/are the purpose(s) of collecting the personal data?
   - » *Be clear about the purpose of collecting the information*
   - » *Are you collecting what you only need?*

4. How was or will the consent be obtained?
   - » *Do individuals have the opportunity and/or right to decline to provide data?*
   - » *What happen if they decline?*

Storage

1. Where is it currently being stored?
   - » *Is it being stored in a physical server or in the cloud?*

2. Is it being stored in other country?
   - » *If it is subject to a cross-border transfer, specify what country or countries.*

3. Is the storage of data being outsourced?
   - » *Specify if the storing process is being done in-house or is it handled by a service provider*

Usage

1. How will the data being used or what is the purpose of its processing?
   - » *Describe how the collected information is being used or will be used*
   - » *Specify the processing activities where the personal information is being used.*

Retention

1. How long are the data being retained? And Why?
   - » *State the length of period the data is being retained?*
   - » *What is the basis of retaining the data that long? Specify the reason(s)*

2. The data is being retained by the organization or is it being outsourced?
   - » *Specify if the data retention process is being done in-house or is it handled by a service* provider

Disclosure/Sharing

1. To whom it is being disclosed to?

2. Is it being disclosed outside the organization? Why is it being disclosed?
   - » Specify if the personal information is being shared outside the organization
   - » What are the reasons for disclosing the personal information

Disposal/Destruction

1. How will the data be disposed?
   - » Describe the process of disposing the personal information

2. Who will facilitate the destruction of the data?
   - » State if the process is being managed in-house or if it is a third party

V. Privacy Impact Analysis

Each program, project or means for collecting personal information should be tested for consistency with the following Data Privacy Principles (as identified in Rule IV, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"). Respond accordingly with the questions by checking either the "Yes" or "No" column and/or listing the what the questions may indicate.

Transparency	**Yes**	**No**	**Not applicable**
1. Are data subjects aware of the nature, purpose, and extent of the processing of his or her personal data?			
2. Are data subjects aware of the risks and safeguards involved in the processing of his or her personal data?			
3. Are data subjects aware of his or her rights as a data subject and how these can be exercised? Below are the rights of the data subjects: ✓ Right to be informed ✓ Right to object ✓ Right to access ✓ Right to correct ✓ Right for erasure or blocking ✓ Right to file a complaint ✓ Right to damages ✓ Right to data portability			
4. Is there a document available for public review that sets out the policies for the management of personal data? *Please identify document(s) and provide link where available:* _____ _____			
5. Are there steps in place to allow an individual to know what personal data it holds about them and its purpose of collection, usage and disclosure?			
6. Are the data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data?			
7. Are the data subjects provided information about how to contact the organization's Data Protection Officer (DPO)?			
Legitimate Purpose	**Yes**	**No**	**Not applicable**
1. Is the processing of personal data compatible with a declared and specified purpose which are not contrary to law, morals, or public policy?			
2. Is the processing of personal data authorized by a specific law or regulation, or by the individual through express consent?			
Proportionality	**Yes**	**No**	**Not applicable**
1. Is the processing of personal data adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose?			
2. Is the processing of personal data necessary to fulfill the purpose of the processing and no other means are available?			

Collection	Yes	No	Not applicable
1. Is the collection of personal data for a declared, specified and legitimate purpose?			
2. Is individual consent secured prior to the collection and processing of personal data? If no, specify the reason _____ _____			
3. Is consent time-bound in relation to the declared, specified and legitimate purpose?			
4. Can consent be withdrawn?			
5. Are all the personal data collected necessary for the program?			
6. Are the personal data anonymized or de-identified?			
7. Is the collection of personal data directly from the individual?			
8. Is there authority for collecting personal data about the individual from other sources?			
9. Is it necessary to assign or collect a unique identifier to individuals to enable your organization to carry out the program?			
10. Is it necessary to collect a unique identifier of another agency? *e.g. SSS number, PhilHealth, TIN, Pag-IBIG, etc.,*			
Use and Disclosure	**Yes**	**No**	**Not applicable**
1. Will Personal data only be used or disclosed for the primary purpose?			
2. Are the uses and disclosures of personal data for a secondary purpose authorized by law or the individual?			

Data Quality	Yes	No	Not applicable
1. Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.1 *Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.2 *The system is regularly tested for accuracy			
1.3 *Periodic reviews of the information			
1.4 *A disposal schedule in place that deletes information that is over the retention period			
1.5 *Staff are trained in the use of the tools and receive periodic updates			
1.6 *Reviews of audit trails are undertaken regularly			
1.7 *Independent oversight			
1.8 *Incidents are reviewed for lessons learnt and systems/ processes updated appropriately			
1.9 *Others, please specify _____ _____			
Data Security	**Yes**	**No**	**Not applicable**
1. Do you have appropriate and reasonable organizational, physical and technical security measures in place? *organizational measures - refer to the system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing (i.e. access control policy, employee training, surveillance, etc.,)* *physical measures – refers to policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media (i.e. locks, backup protection, workstation protection, etc.,)* *technical measures - involves the technological aspect of security in protecting personal information (i.e. encryption, data center policies, data transfer policies, etc.,)*			

Organizational Security	Yes	No	Not applicable
*Have you appointed a data protection officer or compliance officer?			
*Are there any data protection and security measure policies in place?			
*Do you have an inventory of processing systems? Will you include this project/system?			
*Are the users/staffs that will process personal data through this project/system under strict confidentiality if the personal data are not intended for public disclosure?			
*If the processing is delegated to a Personal Information Processor, have you reviewed the contract with the personal information processor?			
Physical Security	**Yes**	**No**	**Not applicable**
*Are there policies and procedures to monitor and limit the access to this project/system?			
*Are the duties, responsibilities and schedule of the individuals that will handle the personal data processing clearly defined?			
*Do you have an inventory of processing systems? Will you include this project/system?			
Technical Security	**Yes**	**No**	**Not applicable**
*Is there a security policy with respect to the processing of personal data?			
*Do you have policies and procedures to restore the availability and access to personal data when an incident happens?			
*Do/Will you regularly test, assess and evaluate the effectiveness of the security measures of this project/system?			
*Are the personal data processed by this project/system encrypted while in transit or at rest?			

2. The program has taken reasonable steps to protect the personal data it holds from misuse and loss and from unauthorized access, modification or disclosure?			
3. If yes, which of the following has the program undertaken to protect personal data across the information lifecycle:			
3.1 * Identifying and understanding information types			
3.2 * Assessing and determining the value of the information			
3.3 * Identifying the security risks to the information			
3.4 * Applying security measures to protect the information			
3.5 * Managing the information risks.			
Disposal	**Yes**	**No**	**Not applicable**
1. The program will take reasonable steps to destroy or de-identify personal data if it is no longer needed for any purpose. *If YES, please list the steps* _____ _____			
Cross-border Data Flows (optional)	**Yes**	**No**	**Not applicable**
1. The program will transfer personal data to an organization or person outside of the Philippines *If YES, please describe* _____ _____			
2. Personal data will only be transferred to someone outside of the Philippines if any of the following apply: a. The individual consents to the transfer b. The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012 c. The transfer is necessary for the performance of a contract between the individual and the organization d. The transfer is necessary as part of a contract in the interest of the individual between the organization and a third party e. The transfer is for the benefit of the individual;			

3. The organization has taken reasonable steps so that the information transferred will be stored, used, disclosed and otherwise processed consistently with the DPA of 2012 *If YES, please describe* _____ _____			

VI. Privacy Risk Management

For the purpose of this section, a risk refers to the potential of an incident to result in harm or danger to a data subject or organization. Risks are those that could lead to the unauthorized collection, use, disclosure or access to personal data. It includes risks that the confidentiality, integrity and availability of personal data will not be maintained, or the risk that processing will violate rights of data subjects or privacy principles (transparency, legitimacy and proportionality).

The first step in managing risks is to identify them, including threats and vulnerabilities, and by evaluating its impact and probability.

The following definitions are used in this section,

Risk - "the potential for loss, damage or destruction as a result of a threat exploiting a vulnerability";
Threat - "a potential cause of an unwanted incident, which may result in harm to a system or organization";
Vulnerability - "a weakness of an asset or group of assets that can be exploited by one or more threats";
Impact - severity of the injuries that might arise if the event does occur (can be ranked from trivial injuries to major injuries); and
Probability - chance or probability of something happening;

Impact		
Rating	Types	Description
1	Negligible	The data subjects will either not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2	Limited	The data subject may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3	Significant	The data subjects may encounter significant inconveniences, which they should be able to overcome but with serious difficulties.
4	Maximum	The data subjects may encounter significant inconveniences, or even irreversible, consequences, which they may not overcome.

Probability		
1	Unlikely	Not expected, but there is a slight possibility it may occur at some time.
2	Possible	Casual occurrence. It might happen at some time.
3	Likely	Frequent occurrence. There is a strong possibility that it might occur.
4	Almost Certain	Very likely. It is expected to occur in most circumstances.

Select the appropriate level or criteria of impact and probability to better assess the risk. Kindly refer to the table below for the criteria.

Note: Try to itemize your risks by designating a reference number. This will be used as a basis on the next sections (VII. Recommended Privacy Solutions and VIII. Sign off and Action Plan). Also, base the risks on the violation of privacy principles, rights of data subjects and confidentiality, integrity and availability of personal data.

Ref#	Threats/ Vulnerabilities	Impact				Probability				Risk Rating	
		1	2	3	4	1	2	3	4		
		1	2	3	4	1	2	3	4		
		1	2	3	4	1	2	3	4		
		1	2	3	4	1	2	3	4		

**add additional rows if needed*

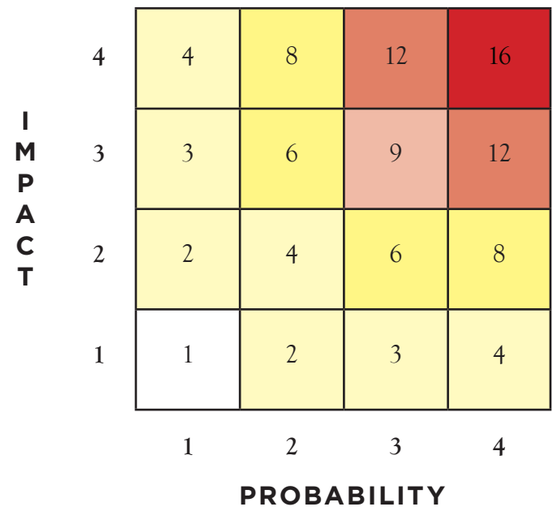
Kindly follow the formula below for getting the Risk Rating:

Risk Rating = Impact x Probability

Kindly refer to the table below for the criteria.

Rating	Types
1	Negligible
2 to 4	Low Risk
6 to 9	Medium Risk
10-16	High Risk

PRIVACY RISK MAP



VII. Recommended Privacy Solutions

From the risks stated in the previous section, identify the recommended solution or mitigation measures. You can cite your existing controls to treat the risks in the same column.

Recommended Solutions (Please provide justification)

**add additional rows if needed*

3. BE ACCOUNTABLE:

DEVELOP A PRIVACY MANAGEMENT PROGRAM AND PRIVACY MANUAL

Privacy Management Program Guide

The digital age undeniably made the world interconnected. At the same time, it entailed extensive use of our personal data in corporate, professional and personal transactions. It may have resulted in efficient and optimized processes, but it exposed us to various security risks.

Over a billion records of personal identifiable information have been stolen in recent years worldwide. In the latest study of IBM and Ponemon Institute, organizations decreased an average cost of $3.64 million from the $4 million of data breaches last year, the Philippines included in this number. While in our country alone, a security breach at the Commission on Elections exposed the personal information of about 55 million voters in 2016.

The losses and dangers from data breach prompted global waves of data protection policies. In 2012, the Philippines legislated Republic Act No. 10173, also known as the Data Privacy Act (DPA). It created the National Privacy Commission (NPC) to safeguard our fundamental right to privacy while supporting the free flow of information as the backbone of the new digital economy. The NPC was established in 2016 and is now set to implement the DPA.

With this, the government and the private sectors covered by the DPA—the personal information controllers (PICs) and personal information processors (PIPs), probably have several questions in mind. How do we comply with the provisions of the law? How do we not commit any data privacy violation? Where do we start? The simplest answer is to have a Privacy Management Program (PMP) in place.

The NPC came up with a Guide to help you in this undertaking. It is meant to see PICs and PIPs through the whole exercise of developing and maintaining a Privacy Management Program. Given the fast-changing landscape of data protection, this Guide will be updated whenever necessary.

Why create a Privacy Management Program?

It puts everyone on the same page. A PMP provides an easier way to explain to the management and staff: why are we doing this, what are the results we expect, what are the benefits of those results, and what do we need to do to get there. With this, you will smoothly get everyone on board.

Compliance with the Act becomes more manageable. As a PMP outlines everything that stakeholders need to know about the what(s) and how(s) of data privacy, there is a reduced likelihood you will violate the DPA and incur penalties.

It gives PICs and PIPs competitive advantage. Implementing a PMP shows your organization's commitment to protect the personal information of your customers. This, in turn, leads to increased trust and higher patronage.

It saves PICs and PIPs from avoidable expenses. 'Clean up' costs during personal data breaches may be prevented through a strong PMP. Further, it helps safeguard the reputation of organizations and individuals as well.

Privacy Management program Guide

Overview

A Privacy Management Program (PMP) is a holistic approach to privacy and data protection, important for all agencies, companies or other organization involved in the processing of personal data. It is a process intended to embed privacy and data protection in the strategic framework and daily operations of a personal information controller or personal information processor. The Privacy Management Program is maintained through organizational commitment and oversight of coordinated projects and activities implemented throughout the agency, company or organization, that allows efficient use of available resources, implements control measures to assure privacy and data protection, and puts in place a system for review to allow for improvements responsive to data privacy best practices and technological developments.

A PMP is an acknowledgement by the PIC or PIP[1] of their accountability for complying with the requirements of the Act and their responsibility for personal data under their control or custody. The Act mandates that PICs and PIPs ensure implementation of data privacy principles,[2] security measures,[3] and procedures for data subjects to exercise their rights.[4] The objective of a PMP is to pave the way for changes within the organization that will: address the threats, vulnerabilities, risks and gaps identified during the privacy impact assessment (PIA);[5] strengthen data processing systems to minimize the costs of personal data breaches; allow meaningful use of information for the benefit of both the organization and the data subjects; and manage the challenges of the digital age to safeguard the right to information privacy.

This guide is intended to help organizations develop their Privacy Management Program. The development of it within the organization should always consider careful planning and consideration across law regulation, disciplines and job functions. In this guide, components of the privacy management program are divided into three (3) stages. Each stage has specific tasks for the organization to follow in fully completing their privacy management program. This also outlines the Commission's privacy advocacies as good approaches for developing an encompassing privacy management program. The Commission expects that through this guide, organizations will be able to further strengthen their good practices, demonstrate due diligence, and potentially elevate their privacy awareness as well as their personal data protection.

[1]Data Privacy Act Sec.14 (The personal information processor shall comply with all the requirements of this Act and other applicable laws.).
[2] Data Privacy Act Sec. 11 (The personal information controller must ensure implementation of personal information processing principles set out herein.)
[3] Data Privacy Act Sec. 20 (The personal information controller must implement reasonable and appropriate organizational, physical and technical measures.)
[4] Data Privacy Act Secs. 16-19 (Rights of Data Subjects).
[5] NPC Advisory 17-03 (Privacy Impact Assessment is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product)

Key Components of a Privacy Management Program

To establish a strong and effective Privacy Management Program, it must have a firm organizational commitment, steady program controls and continuous evaluation and review. Cultivating a strong and resilient privacy culture within the organization must have these components.

GOVERNANCE
1. Management Buy-In
2. Data Protection Officer
3. Reporting Mechanisms
PROGRAM CONTROLS
1. Records of Processing Activities
2. Risk Assessment
3. Registration
4. Policies and Procedures
5. Data Security
6. Capacity Building
7. Breach Management
8. Notification
9. Third-Party Management
10. Communication
CONTINUITY and ESTABLISHING a PRIVACY ECOSYSTEM OVERSIGHT and REVIEW PLAN
1. Oversight and Review Plan
ASSESS and REVISE PROGRAM CONTROLS
1. Updates and Revision

Instructions:

This is essentially a rating tool that will allow the organizations to envision the development of each component's element of the privacy management program. When complete, it will serve as a summary of results. You will assess each element of its status towards completion and implementation. The components have specific elements per stages, some components are only up to Stage 1, while some goes all the way up to Stage 3.

1. This tool begins by assessing the first two (2) elements of the components: Organizational Commitment and Program Controls. For example, under organizational commitment there are three (3) elements (e.g. Management Buy-In, Accountable and Responsible Persons, Reporting Mechanisms). All of which needs a specific requirement. State your evaluation of each requirement by describing its status in your organization and you can add your organization's equivalent document when applicable in the "Remarks" section. The goal here is to have an accurate view of your organization's current status. Please consider the results of your Privacy Impact Assessment.

2. For each requirement, score your organization's compliance on a scale of 1 to 4. You are not bounded by these scale of number as you can give partial points. Kindly round off to one decimal place.

3. Average the score of all the requirements (all stages) in each element to come up with an overall score that you will record in the overall rating row.

4. Record the overall score.

5. Once all stages are complete, review the summary sheet at the last page and develop a plan to move all your ratings to 4.

RATING	DESCRIPTION
1.0 – 1.9	No documented evidence or in practice
2.0 – 2.9	No documented evidence but there is evidence of practice (initiative)
3.0 – 3.9	Documented evidence is present, but inconsistent in practice
4.0	Evidence is documented and in practice

SAMPLE DATA

HEADER	STAGE 1	Rating	STAGE 2	Rating	STAGE 3	Rating
1. Management Buy-In The PIC or PIP, through head of agency or board, resolves to acknowledge the need to comply with the Data Privacy Act and related issuances of the NPC, and to acknowledge its accountability for the protection of personal data under its control or custody.	a. Appoint or designate a Data Protection Officer(DPO) or Office and register with the NPC (Phase I).	2.9	a. Management should regularly monitor the progress of the program controls.	2.0		
	b. Management endorses the organization's compliance with the Data Privacy Act of 2012 by releasing a communication / memorandum order on its target compliance within the organization.	3.0				
	c. Evidence of supportive top management by providing all the necessary resources for privacy management.	4.0				
Average Rating:	Average Rating is 3. Following the formula (2.9 + 3.0 + 4.0 + 2.0) / 4 (Round-off to one decimal place)					
Average the rating of all elements included in each stage. Formula: AR = (E1+E2+E3+En...) / number of elements of all the stages.						
Remarks:						

PRIVACY MANAGEMENT PROGRAM (PMP)

In order to have a complete Privacy Management Program, all stages of development must be completed.

HEADER	STAGE 1	Rating	STAGE 2	Rating	STAGE 3	Rating
GOVERNANCE						
1. **Management Buy-In** The PIC or PIP, through head of agency or board, resolves to acknowledge the need to comply with the Data Privacy Act and related issuances of the NPC, and to acknowledge its accountability for the protection of personal data under its control or custody. The PIC or PIP maintains a Privacy Management Program to implement control measures for privacy and data protection and put in place a review system for assessment and continuous improvement of the program. There are policies, procedures, projects and activities intended to embed privacy and data protection in the organization's daily operations.	a. Appoint or designate a Data Protection Officer(DPO) or Office and register with the NPC (Phase I).		a. Management should regularly monitor the progress of the program controls.			
	b. Management endorses the organization's compliance with the Data Privacy Act of 2012 by releasing a communication/ memorandum order on its target compliance within the organization.					
	c. Evidence of supportive top management by providing all the necessary resources for privacy management.					
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

2. Data Protection Officer The PIC or PIP, through head of agency or Board, designates or appoints a DPO or team. The PIC or PIP, through head of agency or Board, provides resources for the DPO to effectively perform its functions. For the full list of functions, see NPC Advisory 17-01. The responsibility for complying with the Data Privacy Act has been assigned to DPO, process owners, and the organization's personnel.	a. The DPO or office appointed/designated is responsible in jump starting the following programs:					
	a.1. Ensure the compliance of the organization to the Data Privacy Act of 2012					
	a.2. Ensure that the organization, especially the accountable persons, are informed of their responsibility to protect personal information.					
	a.3. Create a facility for data subjects to exercise all their rights.					
	a.4. Involve personnel from the ff. departments: human resources, risk management, policy, internal audit, information communications technology (ICT) and other relevant departments.					

	a.5. Take part in creating privacy policies or integrating them into the organization's regulations.					
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						
PROGRAM CONTROLS						
1. Records of Processing Activities There is an inventory of personal data and data processing systems, including its purpose, data flow, and measures taken	a. An inventory of personal information is produced which includes the data processing system that act on the personal data, its data flow, purpose of processing and its security measures.					
2. Risk Assessment Privacy impact assessment conducted in accordance with a PIA plan. Process in place for regularly testing, assessing, and evaluating the effectiveness of security measures	a. Preliminary preparations for privacy impact assessments					

	b. Conduct of privacy impact assessments on the process and systems listed in the inventory including new or upcoming projects.					
	c. Develop proposals for mitigation and solutions based on the risks, threats and vulnerabilities that were identified from the privacy impact assessments.					
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						
3. Registration Data Processing Systems have been registered	a. Data Processing Systems are registered with the National Privacy Commission.		a. Registration of data processing systems is renewed annually.		a. Review of the organization's data processing systems. b. Update the registered data processing systems when applicable.	

Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						
4. Policies and Procedures There is a privacy manual containing key components of the Privacy Management Program There are policies and procedures to govern the processing of personal data from collection to storage or disposal. These include the ff.: • On Adhering to Data Privacy Principles • On Implementing security measures • For the data subjects to exercise their rights • For the documentation, review and updating of the Privacy Management Program	a. Creation of policies and procedures that adhere to the data privacy principles[1] and their integration to day-to-day operations:		a. Policies to address the risks and gaps identified during the conduct of the privacy impact assessments.			

	a.1. Policies and procedures on how to contact the Data Protection Officer.		b. Implementation and dissemination of the approved privacy and data protection policies, procedures and activities within the organization.			
	a.1. Policies and procedures regarding transparency with the data subjects.					
	a.2. Policies and procedures that value the legitimacy of purpose and authority of the organization to process personal data.					
	a.3. Policies and procedures ensuring that all personal data are always accurate and proportional to the purpose of processing.					
	a.4. Make sure that data privacy policies and procedures are well-integrated into the day-to-day operations.					

[1] Transparency, Legitimate Purpose and Proportionality

	b. Policies and procedures for the data subjects to exercise their rights.					
	c. Creation and planning of activities, events and trainings regarding privacy and data protection.					
	d. Formulation of the organization's Privacy Manual		c. Dissemination of the privacy manual within the organization.			
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

5. Data Security The organization implements organizational, physical and technical security measures to maintain the confidentiality, integrity and availability of personal data.	a. Consider the risks and gaps identified from the Risk Assessments section to craft or update organizational, physical and technical measures		a. Implementation of organizational, physical, and technical security measures to ensure that all personal data are properly protected.			
	b. Identify all departments that hold or process personal information and create a security clearance policy when sharing personal information within and outside.		b. Implement security clearance policy.			
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

6. Capacity Building • There are capacity building, orientation or training programs for employees, agents or representatives, regarding privacy or security policies. • Time, resources, equipment, and training provided are to be updated with developments in data privacy and security. • Knowledge building on privacy and data protection is supported through privacy awareness projects or by having resource materials available	a. Privacy training is made mandatory for all employees.		a. Regular trainings regarding privacy and security policies are instituted for the employees to build a culture of privacy.			
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

7. Breach Management A Breach Management Program is in place, including personal data breach notifications and annual report on breaches and security incidents. For the full list of the reportorial requirements, see NPC Circular 16-03.	a. Create a Breach Management Program		a. Establishment of security breach drills within the organization.		a. Continuous security breach drills.	
	a.1. Creation of the Data Breach Response Team				b. Documentation of all the activities regarding data breach management.	
	a.2. Implementation of the organizational, physical and technical security measures and personal data privacy policies					
	a.3. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications systems including reportorial and notification requirements		b. Document all successful and unsuccessful security incidents.			
	a.4. Compliance to NPC's Reportorial Requirements					

	a.5 Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach					
			c. Ensure that all NPC requirements are submitted.			
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						
8. Notification The organization complies with Reporting and notification requirements	a. The organization complies with the reportorial and notification requirements of the National Privacy Commission.		a. Annual report is submitted.			
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

9. Third-Party Management • Transfers of personal data shall be covered by data sharing agreements when applicable. • Contracts and other means are used to assure protection for personal data being processed by a third party. • Outsourcing contracts and agreements with PIPs are reviewed (For contract considerations, refer to Rule X of the IRR.)	a. **Provide a list of PICs and PIPs that the organization is in business with.**		a. Contracts and other means are used to assure protection for personal data being processed by a third party.		a. **Outsourcing contracts and agreements with PIPs are reviewed.**	
			b. Transfers of personal data shall be covered by data sharing agreements when applicable (if dealing with another PICs).			
			c. Obligations of the PIP are clearly defined by the PIC.			
			d. Sensitivity of personal information is addressed through arrangements such as data sharing agreements or contracts.			

			e. Compliance requirements which bind the service provider to the policies and practices of the PIC and require breach notification.			
	b. Identify all cross-border transactions of personal data and ensure their legal compliance.					
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

10. Communication • Any information and communication related to the processing of personal data should be easy to access and understand, using clear and plain language. • Privacy notices and consent forms are maintained. • Policies and procedures are in place to address complaints and to allow for the exercise of data subject rights.	a. Privacy notices are always served prior to the collection of personal data.		a. **Privacy notices and consent forms are reviewed.**		a. **Privacy notices and consent forms are kept up to date.**	
	b. Any information and communication that relates to the processing of personal data should be easy to access and understand, using clear and plain language.					
	c. Policies and procedures for informing individuals of their privacy rights and program controls of the organization are in place.					
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

Continuity and Establishing a Privacy Ecosystem **Oversight and Review Plan**						
1. Develop Oversight and Review Plan The DPO should monitor data processing systems and ensure the conduct of PIAs when necessary. The organization must provide policies for documentation, regular review, evaluation and updating of the privacy and security practices in the organization.					a. Develop a policy plan that will ensure the documentation, regular review, evaluation, and updating of the privacy and security policies and practices in the organization	
					b. The plan will revisit and update the personal information inventory as well as the data processing system inventory.	
					c. The plan will establish performance measures.	
					d. The plan will also include a schedule of the review of all privacy policies and programs.	
Average Rating:						
Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages						
Remarks:						

Continuity and Establishing a Privacy Ecosystem **Assess and Revise Program Controls**						
1. Update and Revision The organization conducts and updates PIAs regularly – when there are new programs, projects and products, a change in law or regulation, or other changes within the organization. The PMP must be regularly assessed and revised, considering PIAs, effectiveness of implementation, and data privacy best practices. The organization must monitor emerging technologies, new threats and risks to data processing systems, international data protection standards, and the legal and ICT environment.					a. Periodically monitor the effectiveness of the program controls.	
					b. Privacy Management Program is regularly assessed and revised, considering the PIAs, effectiveness of the implementation, and data privacy best practices	
					c. The organization monitors emerging technologies, new threats and risks to data processing systems, international data protection standards, and the legal and ICT environment.	

d. Revision of policies and procedures when needed.			
	Average Rating:	**Get the average rating (AR) of all elements included in each component. Formula: AR = (E1+E2+E3+...) / number of elements of all the stages**	**Remarks:**

Record the overall score in this page

Summary of Results	
PMP Component Requirements	Overall rating
Governance	
1. Management Buy-In	
2. Data Protection Officer	
3. Reporting Mechanisms	
Program Controls	
1. Records of Processing Activities	
2. Risk Assessment	
3. Registration	
4. Policies and Procedures	
5. Data Security	
6. Capacity Building	
7. Breach Management	
8. Notification	
9. Third-Party Management	
10. Communication	
CONTINUITY and ESTABLISHING a PRIVACY ECOSYSTEM Oversight and Review Plan	
1. Develop Oversight and Review Plan	
Assess and Revise Program Controls	
1. Updates and Revision	
TOTAL RATING	

DISCLAIMER:

The information provided in this guide is for general reference only. This document is not a "one-size-fits-all" solution. Each organization will need to decide how to structure its own privacy management program, taking into consideration a number of factors, like the size of the organization, internal resources and the amount and sensitivity of the personal information it handles. Such program will help foster a culture of privacy throughout an organization.

PRIVACY MANUAL GUIDE

Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each personal information controller or personal information processor is expected to produce a Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

I. INTRODUCTION

This section lays down the basis of the Manual. Hence, it should provide an overview of the DPA, its IRR and other policies that relate to data protection and which are relevant issuances to the industry or sector of the organization, as well as the transactions it regularly carries out.

In brief, it should discuss how the organization complies with the data privacy principles, and upholds the rights of the data subjects, both of which are laid out in the DPA.

It is important that this portion impresses upon the user or reader why it is necessary for the organization to have a Privacy Manual.

> *Example:*
> This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values your data privacy rights, and makes sure that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.
>
> This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

II. DEFINITION OF TERMS

Terms used in the Manual must be defined for consistency and uniformity in usage. This portion will make sure of that, and allow users of the Manual to understand the words, statements, and concepts used in the document.

> *Examples:*
> "Data Subject" – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of this organization.
>
> "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, or when put together with other information would directly and certainly identify an individual.
>
> "Processing" – refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

III. SCOPE AND LIMITATIONS

This section defines the coverage of the Manual. Given that the document is essentially an internal issuance and is meant for the use and application of the organization's staff or personnel, that fact should be emphasized here.

Note that it would be useful to develop a separate Privacy Manual meant for external use or for persons who deal with the organization. Certain information may be omitted from that version, particularly those that relate to internal policies or processes that are relevant only to personnel of the organization.

> *Example:*
> All personnel of this organization, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual.

IV. PROCESSING OF PERSONAL DATA

This section lays out the various parts of the data life cycles (or processing systems) in existence within the organization—from the collection of personal data, to their actual use, storage or retention, and destruction.

A. **Collection** (e.g. type of data collected, mode of collection, person collecting information, etc.)

> *Example:*
> This company collects the basic contact information of clients and customers, including their full name, address, email address, contact number, together with the products that they would like to purchase. The sales representative attending to customers will collect such information through accomplished order forms.

B. **Use**

> *Example:*
> Personal data collected shall be used by the company for documentation purposes, for warranty tracking vis-à-vis purchased items, and for the inventory of products.

C. Storage, Retention and Destruction (e.g. means of storage, security measures, form of information stored, retention period, disposal procedure, etc.)

Example:
This company will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The company will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for a period longer than one (1) year. After one (1) year, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

D. Access (e.g. personnel authorized to access personal data, purpose of access, mode of access, request for amendment of personal data, etc.)

Example:
Due to the sensitive and confidential nature of the personal data under the custody of the company, only the client and the authorized representative of the company shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

E. Disclosure and Sharing (e.g. individuals to whom personal data is shared, disclosure of policy and processes, outsourcing and subcontracting, etc.).

Example:
All employees and personnel of the company shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

V. SECURITY MEASURES

As a personal information controller or personal information processor, an organization must implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data. Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination. This section gives you a general description of those measures.

A. Organizational Measures

Every personal information controller and personal information processor must also consider the human aspect of data protection. The provisions under this section shall include the following:

1. Conduct of Privacy Impact Assessment (PIA)

   Example:
   The organization shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party.

2. Data Protection Officer (DPO), or Compliance Officer for Privacy (COP)

   Example:
   The designated Data Protection Officer is Mr. Juan Dela Cruz, who is concurrently serving as the Executive Director of the organization.

3. Functions of the DPO, COP and/or any other responsible personnel with similar functions

   Example:
   The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

4. Duty of Confidentiality

   Example:
   All employees will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

5. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security

   Example:
   The organization shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

6. Review of Privacy Manual

   Example:
   This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

7. Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.

   Example:
   There shall be a detailed and accurate documentation of all activities, projects and processing systems of the company, to be carried out by the Risk Management Officer, in coordination with the Data Protection Officer.

B. Physical Measures

This portion shall feature the procedures intended to monitor and limit access to the facility containing the personal data, including the activities therein. It shall provide for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of

transfer, and the schedule and means of retention and disposal of data, among others. To ensure that mechanical destruction, tampering and alteration of personal data under the custody of the organization are protected from man-made disasters, power disturbances, external access, and other similar threats, provisions like the following must be included in the Manual:

1. Format of data to be collected

   Example:
   Personal data in the custody of the organization may be in digital/electronic format and paper-based/physical format.

2. Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/ separate room or part of an existing room);

   Example:
   All personal data being processed by the organization shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the company.

3. Access procedure of agency personnel

   Example:
   Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitation of access to room or facility

   Example:
   All personnel authorized to enter and access the data room or facility must fill out and register with the online registration platform of the organization, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration, and purpose of each access.

5. Design of office space/work station

   Example:
   The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6. Persons involved in processing, and their duties and responsibilities

   Example:
   Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.

7. Modes of transfer of personal data within the organization, or to third parties

   Example:
   Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

8. Retention and disposal procedure

   Example:
   The organization shall retain the personal data of a client for one (1) year from the data of purchase. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. Technical Measures

Each personal information controller and personal information processor must implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

1. Monitoring for security breaches

   Example:
   The organization shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used

   Example:
   The organization shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

   Example:
   The organization shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.

4. Encryption, authentication process, and other technical security measures that control and limit access to personal data

   Example:
   Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

VI. BREACH AND SECURITY INCIDENTS

Every personal information controller or personal information processor must develop and implement policies and procedures for the management of a personal data breach, including security incidents. This section must adequately describe or outline such policies and procedures, including the following:

1. Creation of a Data Breach Response Team

Example:
A Data Breach Response Team comprising of five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to prevent and minimize occurrence of breach and security incidents

Example:
The organization shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

3. Procedure for recovery and restoration of personal data

Example:
The organization shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

4. Notification protocol

Example:
The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

5. Documentation and reporting procedure of security incidents or a personal data breach

Example:
The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

VII. INQUIRIES AND COMPLAINTS

Every data subject has the right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor. Other available rights include: (1) right to dispute the inaccuracy or error in the personal data; (2) right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. This section shall feature such procedure.

Example:
Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization at inquiry@company.com and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to complaints@company.com. The concerned department or unit shall confirm with the complainant its receipt of the complaint.

VIII. EFFECTIVITY

This section indicates the period of effectivity of the Manual, as well as any other document that the organization may issue, and which has the effect of amending the provisions of the Manual.

Example:
The provisions of this Manual are effective this __ day of _____, 2017, until revoked or amended by this company, through a Board Resolution.

IX. ANNEXES

It is considered best practice that an organization provides copies of its policies, sample forms or templates that are useful or related to the implementation or enforcement of the provisions of the DPA.

Examples:

1. PRIVACY NOTICE

PRIVACY NOTICE GUIDE

(Note: Please consider the results of your Privacy Impact Assessment.)

The <NAME OF ENTITY – i.e. NATIONAL PRIVACY COMMISSION> is committed to protect and respect your personal data privacy. We are at the forefront of not only implementing but also complying with the Data Privacy Act of 2012.

1. SERVICE DESCRIPTION

What services does your organization provide?

List all the services that your organization provides. For data subjects to give meaningful consent, a short phrase for each service should be included, with a corresponding overview of the service, which can be accessed through a hyperlink.

2. PERSONAL INFORMATION THAT ARE COLLECTED

What are the actual personal information you collect?

Specify all pieces of personal information that will be collected in order to deliver each service, and as much as possible, present the data subject's actual personal information to be collected so he/she can properly determine whether or not to provide your organization, that exact personal information.

3. COLLECTION METHOD

How do you collect personal information controller from people?

Provide a clear explanation for the manner of collection to be applied on a particular piece of personal information.

4. TIMING OF COLLECTION

When do you collect personal information?

Give exact information on the date or period for which the personal information shall be collected, including where such personal information is intended to be collected even after notification to the data subject.

5. PURPOSES OF COLLECTED PERSONAL INFORMATION

Why do you collect this personal information? Is all information collected, necessary?

Present a clear and easily understandable justification for the collection of each piece of personal information, considering the order of presentation, wherein the purpose/use with the highest impact to the data subject should come first.

6. STORAGE AND TRANSMISSION OF PERSONAL INFORMATION

How do you store and transmit personal information?
How do you protect stored personal data?
How do you protect personal data in transit?

Demonstrate how you store and transmit personal information and include the security measures that are applied.

7. METHOD OF USE

Will the personal information be used as it is?
Will you use the personal information collected other than your listed services above? If yes, kindly provide relevant information.

Provide relevant information on the actions to be performed to the whole personal information lifecycle especially if the personal information will be subjected to additional processing before it is used for the stated purposes.

8. LOCATION OF PERSONAL INFORMATION

Where do you store the personal information that you have collected and processed?

Specify the location/s where the personal information will be stored and processed in a distinguished and detailed manner.

9. THIRD PARTY TRANSFER

Do you transfer personal information to third parties for further processing? If yes, kindly specify their identities and the reason for the data transfer.

Notify the data subject whether or not his/her personal information will be transferred to a third party, and include the reason/s for the transfer as well as the identity of the third-party recipients.

10. RETENTION PERIOD

How long do you keep collected personal information?
How do you dispose them?

Supply sufficient information about the retention period and/or disposal and de-identification schedule of all personal information that your organization is collecting.

11.PARTICIPATION OF DATA SUBJECT

What can the data subjects do in order to exercise their rights?

Inform the data subject about his/her rights under the Data Privacy Act of 2012 and how these may be properly exercised.

12. INQUIRY

How can data subjects reach out to you?

Provide your organization's contact details for all inquiries concerning the processing of personal information and where possible, indicate the Data Protection Officer's official contact information as well.

2. CONSENT GUIDE

ELEMENTS OF A GOOD CONSENT

- **Initial Consent and Choice**

Consent is not always required. Sometimes notice about personal information collection serves the purpose. This happens the data processing is based, for example, on complying with a legal requirement or in execution of the terms of a contract.

- **Informed and free consent**

The organization shall provide sufficient details concerning their processing of personal information that the personal information data subject can give their consent to that processing freely, specifically and on a knowledgeable basis. Consent is only considered to be informed consent if there is evidence that the personal information data subject has fully understood the notice. Consent needs to be freely given without the personal information data subject perceiving any form of coercion or compulsion.

- **Editable or withdrawable consent**

a) The organization shall provide facilities such that a personal information data subject can access their consent details and if appropriate, modify or withdraw that consent. The modification and withdrawal of the consent should be as easy as it was to give.

b) Where consent cannot be modified or withdrawn, then the reasons for this situation shall be explained to the data subject.

- **Identity of the data subject**

A data subject may have more than one online identity/persona. The organization shall clearly indicate which identities/persona they are asking to grant consent in order to avoid potential confusion on the part of the personal information data subject.

- **Independence from other consent**

The organization shall not obtain consent for matters related to privacy as part of the same notice as consent for other matters not related to data privacy.

- **Frequency**

The organization shall seek to confirm existing consent or gain new consents of a personal information data subject at an appropriate interval. However, if the organization asks for consent of the personal information data subject too often, he/she may overlook what the consent is about and start accepting it without really understanding the implication of it. This is sometimes referred to as click training. The organization shall not seek consent excessively to prevent this from happening.

- **Timeliness**

The organization shall obtain consent of the personal information data subject in a timely manner. However, seeking the consent of the personal information data subject too early may have practical issues in the choice given to the consent. The organization should not seek consent of the personal information data subject too early.

CONSENT GUIDE

(Note: Please consider the results of your Privacy Impact Assessment.)

We at the _____ are committed to provide you
(Name of the Personal Information Controller)
with the services pursuant to
_____

(As may be applicable: Government – indicate mandate under specific law/regulation; Private Entities – indicate contract/agreement/application)

while implementing safeguards to protect your privacy and keep your personal data safe and secure.

Processing of Personal Data

(Description of the personal data, the processing thereof, i.e. collection, access, use, disclosure or other processing, and the legitimate purpose, function, or activity of the personal information controller)

(Indicate primary and secondary purpose for the processing of personal data.)

(Indicate any data sharing agreement, disclosures or transfers of personal data to any third party)

(Indicate if company or agency engages services of any third party for processing of personal data)

Data Protection

(Description of the security measures to be implemented for the protection of personal data)

Example:
We shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collected.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing

(May include additional details on specific organizational, physical, and technical security measures to be implemented.)

Confidentiality

Our employees shall operate and hold personal data under strict confidentiality. They are required to sign non-disclosure agreements and are have received training on the company's privacy and security policies to ensure confidentiality and security of personal data.

Rights of the Data Subjects

You are entitled to the following rights:

A. Be informed on whether your personal information shall be, are being or have been processed;
B. Be furnished with the information indicated below before the entry of your personal information into the processing system of the personal information controller, 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;
   (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.

Any information supplied or declaration made to you on these matters shall not be amended without prior notification: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or 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 or when necessary or desirable in the context of an employer-employee relationship, or when the information is being collected and processed as a result of legal obligation;

C. Reasonable access to, upon demand, the following:
   (1) Contents of your 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 you;
   (7) Date when your personal information was last accessed and modified; and
   (8) The designation, or name or identity and address of the personal information controller.

D. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal

information shall be informed of its inaccuracy and its rectification upon your request;

E. Suspend, withdraw or order the blocking, removal or destruction of your 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; and

F. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

G. Right to data portability - where personal information is processed by electronic means and in a structured and commonly used format, you have the right 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.

Contact Information

If you have further questions or concerns, you may contact our Data Protection Officer through the following details:

Contact Number : _____

Email Address : _____

I have read this form, understood its contents and consent to the processing of my personal data. I understand that my consent does not preclude the existence of other criteria for lawful processing of personal data, and does not waive any of my rights under the Data Privacy Act of 2012 and other applicable laws.

_____ _____

Signature Over Printed Name Date

Witness:

_____ _____

Signature Over Printed Name Date

3. INQUIRY SUMMARY FORM
4. ACCESS REQUEST FORM
5. REQUEST FOR CORRECTION OR ERASURE

4. DEMONSTRATE YOUR COMPLIANCE:

IMPLEMENT PRIVACY & DATA PROTECTION MEASURES

Data Privacy Accountability and Compliance Framework

a. Choose a DPO

b. Register
c. Records of processing activities
d. Conduct Risk Assessment

e. Privacy Management Program
f. Privacy Manual

g. Privacy Notice
h-o. Data Subject Rights
p. Data Life Cycle

q. Organization
r. Physical
s. Technical
- » Data Center
- » Encryption
- » Access Control Policy
- » Vulnerability Assessment and Penetration Testing

t. Data Breach Management
- » Security Policy
- » Data Breach Response Team
- » Incident Response Procedure
- » Document
- » Breach Notification

u. Third Parties:
- » Legal Basis for Disclosure
- » Data Sharing Agreements
- » Cross Border Transfer Agreement

v. Training and Certifications
w. Security Clearance

x. Continuing Assessment and Development
- » Regular Risk Assessment
- » Review Contracts
- » Internal Assessments
- » Review PMP
- » Accreditations

y. New Technologies and Standards
z. New Legal Requirements

I. Governance

a. Choose a DPO

Compliance to the DPA starts by choosing or designating a data protection officer for your organization. This person or other body shall be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. The NPC issued an advisory on designating a DPO.

(please refer to page 25)

II. Risk Assessment

b. Register

The Registration system is one of the means by which the NPC can ensure compliance of personal information controllers and personal information processors with the act. This will also assist both the NPC and those involved in processing of personal data in upholding the rights of a data subject.

(please refer to page 143)

c. Records of Processing Activities

In the Section 1 of the Implementing Rules and Regulations (IRR) of the Data Privacy Act (DPA), the term "processing" refers to any operation or any set or operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. In general terms, it is changing information in any manner detectable by any witness or observer. It may be performed through automated means, or manual processing, if the personal data are contained or intended to be contained in a filing system.

The processing activities have its data life cycle where it starts from collection of the personal data and will and must end at the disposal. Every personal information controller and personal information processor must maintain or keep track of their processing activities. They must firmly identify the duties and responsibilities of the individuals who currently have access and will have access to personal and sensitive personal information. This should apply to any internal and external processing activities that collect, use, store and dispose (or any equivalent processing activity) personal information. This can help every organization keep track of the purpose of each activity and its alignment to the organization's objectives.

The record should contain the purpose of the processing of personal data, description of categories of data subjects, personal data and recipients of information that will be involved with the processing, information of the data flow, security measures that are in place, and name and contact details of any individual or individuals accountable for ensuring data protection of the systems. To know more about this, you may refer to Section 26.c of the IRR of DPA of 2012.

d. Conduct Risk or Impact Assessment

This section describes the privacy risks you've identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

(please refer to page 35)

III. Organization

e. Privacy Management Program

A Privacy Management Program is a holistic approach to privacy and data protection, important for all agencies, companies or other organization involved in the processing of personal data. It is a process intended to embed privacy and data protection in the strategic framework and daily operations of a personal information controller or personal information processor.

(please refer to page 59)

f. Privacy Manual

The Privacy Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

(please refer to page 82)

IV. Day to Day

g. Privacy Notice

It is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement, or privacy policy.

As a privacy notice aims to empower the public and tell individuals what, how and why personal data is being collected from them, it should be highly readable to be effective. However, recent researches reveal that only a few actually read privacy notices.

With the average privacy notice taking ten minutes to read (at most 42 minutes), it is of no surprise that only 16% of internet users take the time to read them, based on the Internet Society's Global Internet User Survey. The figure may even be lower in the Philippines where the concept of data privacy is just emerging.

This prompted the NPC to compile the following tips on how to effectively craft your privacy

notice.

Easy-to-read

Privacy notices should be concise and written in plain language as you write for a diverse audience. A segment of your audience may not be familiar with data privacy. Thus, it is important to communicate the content clearly. If legal and/or technical terms are to be used, hyperlink these to a definition.

The notice should be concise, direct, and affirmative. Use short sentences in active voice for easier understanding. If you are enumerating several items, use bullet points. Each section of the notice should have an informative heading to accurately describe what follows.

Transparent

To reduce legal risks, privacy commitments in your notices should be aligned with your actual privacy practices. Various resources reveal that while notices should try to avoid using bold statements, they should not also be too generic. Notices should cover both current and prospective privacy practices, which necessitates strategic planning involving everyone in the organization.

The key is to conduct factual and legal due diligence. According to the International Association of Privacy Professional, factual due diligence allows you to determine what information your organization uses. The legal due diligence allows you to determine what laws govern the use of that information.
The conduct of a privacy impact assessment may already encompass both factual and legal due diligence.

The conduct of a privacy impact assessment may already encompass both factual and legal due diligence.

Frequently Asked Questions regarding Privacy Notice

1. What is the difference between a Privacy Notice and a Privacy Policy?

Privacy Policy: An internal statement that governs an organization or entity's handling practices of personal information. It is directed at the users of the personal information. A privacy policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.

Privacy Notice: A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.

2. Why do websites need a Privacy Notice?

Websites need Privacy Notice because the DPA says that the data subject is entitled to be

informed whether personal information pertaining to him or her, shall be, are being or have been processed.

3. What if my website doesn't have a Privacy Notice?

If the National Privacy Commission (NPC) issues an enforcement notice requesting that you either place a Privacy Notice on your site, or cease processing data, failure to comply could result in prosecution with a possible penalty of P4,000,000.

Generally, Section 65 of the DPA says that Violations of the Act, these Rules, other issuances and orders of the NPC, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with a schedule to be published by the NPC.

4. How do I know if my website requires a Privacy Notice?

If your site does any of the following, a Privacy Notice is required:

- Collects personal data (visitors filling in web forms, feedback forms, etc).
- Uses cookies or web beacons.
- Covertly collects personal data (IP addresses, e- mail addresses.)

5. What information should be contained within a Privacy Notice?

Please refer to page 95 for the Privacy Notice Guide.

6. Where should I place the Privacy Notice?

A Privacy Notice should be placed in a reasonably obvious position on the homepage. Typically, privacy statements can be found in the sub navigation menu which is normally situated in a bottom center position on the homepage alongside other menu items such as Security Statement, Disclaimer, Terms & Conditions etc.

Placing a statement only on a Home Page may not be sufficient, as links from other web sites or through search engines may bring a visitor into the site via a page other than the Home Page. The ideal solution to this problem is to place a link to the Privacy Statement on each page. Alternatively, a link could be placed on any page on which data are collected, though if the website uses cookies, effectively this could mean all pages.

7. Can I place the Privacy Notice within a "terms & conditions" document?

A Privacy Notice is a legal requirement and is distinct from terms and conditions, copyright or disclaimer notices. It should stand alone and be clearly identifiable. In order for a Privacy Notice to be of value, it must be readily accessible to the user, quickly read and easily understood.

8. How often should I review the Privacy Statement?

It should only be necessary to conduct a review if there is some change to on-line processes. However, some mechanism should be in place to notify the appropriate staff member to

initiate a review if:

- There is a change to data processing on the website
- There is a planned/actual redevelopment of the website
- There is a new web hosting arrangement
- There are suggestions / comments received from site users.

In any case, the Privacy Notice should be reviewed in the context of an internal audit procedure, which also should review the organizational Privacy Policy, at least on an regular basis. For more information, kindly refer to Continuity.

9. I am not an IT person, what are cookies?

A cookie is a block of data that a web server places on a user's PC. Typically, it is used to ease navigation through the site. However, it is also a useful means of the website identifying the user, tracking the user's path through the site, and identifying repeat visits to the site by the same user (or same user's machine). This can then lead to a website owner being able to profile an individual user's browsing habits - and all potentially done without the knowledge, or consent, of the user.

10. How do I know if my web site uses cookies?

This should be a question you address to the person who has developed your website, or to whomever maintains it for you. Most browsers can be set to prevent cookies being downloaded onto a PC. If you set your browser to block cookies, then visit your own site, you may get an error message displayed if your site is attempting to download a cookie. Alternatively, you can look into the "cookie" or "Temporary Internet" folder of your PC and see if you can identify a cookie placed by your site. Cookies often, but not always, contain site names.

11. Do I need to submit my Privacy Notice to the National Privacy Commission for approval?

Not required.

References:

- *https://iapp.org/resources/glossary/*
- *https://iapp.org/news/a/2012-09-13-best-practices-in-drafting-plain-language-and-layered-privacy/*
- *https://iapp.org/news/a/need-to-write-a-solid-privacy-notice-a-few-tips/*
- *https://www.ftc.gov/tips-advice/business-center/guidance/getting-noticed-writing-effective-financial-privacy-notices*
- *https://www.dataprotection.ie/docs/PrivStatements/290.htm*
- *ISO/IEC WD 29184 Information technology – Security techniques – User friendly online privacy notices and consent, December 4, 2016*

h. The right to be informed

As a data subject, you have the right to be informed that your personal data shall be, are being or have been processed.

The right to be informed is a basic right as it empowers you as a data subject to consider other

actions to protect your data privacy and assert your other privacy rights.

This right also requires personal information controllers (PICs) to notify you if within a specific period of time if your data has been compromised, i.e. in the case of a personal data breach.

i. The right to access

Concomitant to your right to be informed, you also have a right to gain reasonable access to your personal data.

You may request access to the following:

- Contents of your personal data that were processed;
- Sources from which they were obtained;
- Names and addresses of the recipients of your data;
- Manner by which such data were processed;
- Reasons for disclosure to recipients, if there were any;
- Information on automated processes where the data will or likely to be made as the sole basis for any decision which would significantly affect you;
- Date when your data was last accessed and modified; and
- Name and address of the personal information controller.

j. The right to object

You have a right to object to the processing of your personal data, including processing for direct marketing, automated processing or profiling.
You likewise have the right to be notified and given an opportunity to withhold consent to the processing in case of changes to the information given to you regarding the processing of your information.

k. The right to erasure or blocking

Under the law, you have the right to suspend, withdraw or order the blocking, removal or destruction of your personal data. You can exercise this right upon discovery and substantial proof of the any of the following:

1. Your personal data is incomplete, outdated, false, or unlawfully obtained;
2. It is being used for purposes you did not authorize;
3. The data is no longer necessary for the purposes for which they were collected;
4. You decided to withdraw consent, or you object to its processing, and there is no overriding legal ground for its processing;
5. The data concerns personal information prejudicial to the data subject – unless justified by freedom of speech, of expression, or of the press; or otherwise authorized;
6. The processing is unlawful; or
7. The personal information controller, or the personal information processor, violated your rights as a data subject.

l. The right to damages

You may claim compensation if you suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, considering any violation of your rights and freedoms as data subject.

m. The right to file a complaint

If you are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the DPA, may file complaints with the NPC.

n. The right to rectification

You have the right to dispute any inaccuracy or error in your personal data and have the personal information controller correct it immediately, unless the request is vexatious or unreasonable. Once corrected, the PIC should ensure that your access to both new and retracted information, and simultaneous receipt of the new and the retracted information by the intended recipients thereof.

o. The right to data portability

Where your personal information is processed by electronic means, you have a right to obtain from the personal information controller a copy of your personal data a copy of such data in an electronic or structured format that is commonly used and allows for further use.

The purpose of this right is to empower you and give you more control over your personal data. This right, which applies subject to certain conditions, supports user choice, user control and consumer empowerment.

It enables the free flow of your personal information across organizations according to your preference. This is important especially now that several organizations and services can reuse the same data.

Data portability allows you to manage your personal data, and to transmit your data from one personal information controller to another. As such, it promotes competition that fosters better services for the public.

p. Data Life Cycle

In Section 11 of the DPA, the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Data Life Cycle is composed of creation and collection, storage and transmission, use and distribution, retention, and disposal and destruction.

Creation and Collection

In Section 11.a of the DPA, personal information must be 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.

In Section 19.a of the Implementing Rules and Regulations of the DPA, Personal Information Controllers (PICs) or Personal Information Processors (PIPs) must keep in mind the following general principles for collecting personal data:

1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.

3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.

4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

Most common way to make sure that there is transparency is through privacy notice.

(please refer to Data Privacy Act IRR Rule IV)

Use

In Section 11 of the DPA, b. personal information must be processed fairly and lawfully; c. personal information must be 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; and d. Adequate and not excessive in relation to the purposes for which they are collected and processed.

(please refer to Data Privacy Act IRR Rule IV)

PICs or PIPs should uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing. The use of personal data must be in a manner compatible with declared, specified, and legitimate purpose.

(please refer to Data Privacy Act IRR Rule IV)

Storage

Data Storage is a general term for how information is kept in a digital format. To ensure protection of personal data against unauthorized or unlawful processing, PICs or PIPs should implement reasonable and appropriate security measures for the protection of personal data. Such security measures can be through encrypting data and having secured data center. (please refer to page 110 For encryption and refer to page 108 for data center)

Retention

What does DPA say about retention of personal data?

> In Section 11.e of the DPA, personal information must be retained only for as long as necessary for the fulfillment of the purposes for which data was obtained, or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law.

In addition, Section 11.f likewise provides that personal information must be 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, That 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: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.

Finally, Section 19.e.3 of the IRR provides that personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

(please refer to Data Privacy Act IRR Rule IV)

Disposal

What does Data Privacy Act say about disposal of personal data?

Section 19.d.3 of the IRR states that personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or public, or prejudice the interests of the data subjects.

Further, NPC Circular 16-01 on Security of Personal Data in Government Agencies provides that procedures must be established regarding the following:

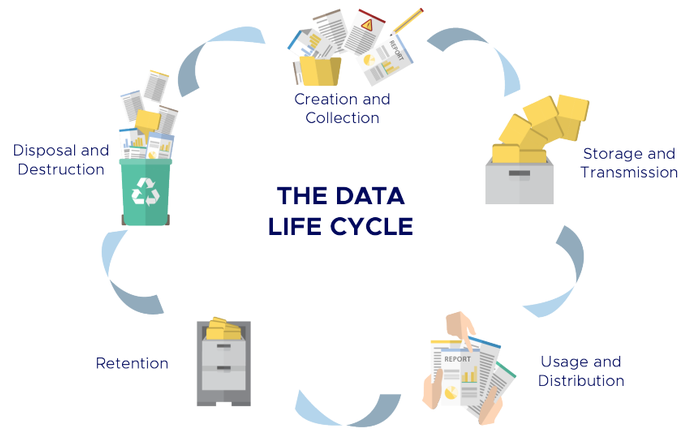
- disposal of files that contain personal data, whether such files are stored on paper, film, optical or magnetic media;
- secure disposal of computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media: Provided, that the procedure shall include the use of degaussers, erasers, and physical destruction devices; and
- disposal of personal data stored offsite.

The circular further provides that government agencies may engage a service provider to carry out the disposal of personal data under its control or custody.

(please refer to Data Privacy Act IRR Rule IV)

What are my responsibilities when disposing personal data?

It is the organization's duty to make sure that data will be disposed properly in a way that the data should be unreadable (for paper) or irretrievable (for digital records). The organization should categorize whether the data they have are high-risk or low-risk. It is recommended that the appropriate data disposal method be used.



V. Data Security

q. Organizational

It is most commonly known that the weakest link in the security of most organizations is human factor and not technology. Even though that it is an obvious weak point, it is frequently overlooked. Designing security measures starts by developing and establishing policies, rules, procedures or guidelines to ensure data protection within the organization. Organizational measures also refer to the system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing. The security policies and procedures will be applied from the collection up to its disposal of personal information. Section 26 of the IRR of the DPA directs personal information controllers and personal information processors to comply with the guidelines for organizational security.

(please refer to Data Privacy Act IRR Rule VI)

r. Physical

Physical security must be implemented properly to prevent unauthorized access. Similar to the "human" factor in data protection, this element is also often overlooked. Hacking into the network system is not the only way that personal or sensitive personal information can be taken or used against an organization or any individual. Designing and implementing physical security must be taken seriously and instituted. Its main focus is to protect physical assets through office designs and layout, environmental components, emergency response readiness, accessibility to the public, security against natural disasters and any other relevant points.

Over the past years, threats to physical security have been significantly increasing. Now that we live in the 21st century, technological advancements have increasing vulnerabilities. Safeguarding personal information (both in digital and paper format) transmitted in networks and systems has been difficult, with emerging mobile or remote users being able to take their devices out of the secured facilities. This is one of the main reasons for the increasing cost of physical security. Managing it through time, becomes tougher because of emerging technologies. The NPC released guidelines in managing physical security for personal information controllers and personal information processors because of their importance.

(please refer to Data Privacy Act IRR Rule VI)

s. Technical

Technical security involves the technological aspect of security in protecting personal information. It includes protecting the network, encrypting personal information in storage and in transit, mitigating data transfer risks, implementing software system designs and having efficient access control policies. The NPC has issued technical security guidelines for the personal information controllers and personal information processors, specifically for Data Center, Encryption and Access Control Policy.

(please refer to Data Privacy Act IRR Rule VI)

Data Center

What is a Data Center?

A data center is a facility housing electronic equipment used for data processing, data storage, and communications networking. It is a centralized repository, which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data including personal data.

The NPC requires personal information controllers and personal information processors to implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.

For government agencies, personal data shall be stored in a data center, which may or may not be owned and controlled by such agency, provided, that the agency must be able to demonstrate to the Commission how its control framework for data protection, and/or, where applicable,

that of its service provider, shall ensure compliance with the Act. Where a service provider is engaged, the Commission may require the agency to submit its contract with its service provider for review.

In addition, the Commission reserves the right to audit a government agency's data center, or, where applicable, that of its service provider.

What are the recommended best practices for data center security?

1. **Include security and compliance objectives as part of the data center design and ensure the security team is involved from day one.** Security controls should be developed for each modular component of the data center—servers, storage, data and network—united by a common policy environment.

2. **Ensure that approach taken will not limit availability and scalability of resources.**

3. **Develop and enforce policies that are context, identity and application-aware for least complexity, and the most flexibility and scalability.** Ensure that they can be applied consistently across physical, virtual and cloud environments. This, along with replacing physical with secure trust zones, will provide seamless and secure user access to applications at all times, regardless of the device used to connect to resources in the data center.

4. **Choose security technologies that are virtualization-aware or enabled, with security working at the network level rather than the server.** Network security should be integrated at the hypervisor level to discover existing and new virtual machines and to follow those devices as they are moved or scaled up so that policy can be dynamically applied and enforced.

5. **Monitor everything continuously at the network level to be able to look at all assets (physical and virtual) that reside on the local area network (even those that are offline) and all inter-connections between them.** This monitoring should be done on a continuous basis and should be capable of tracking dynamic network fabrics. Monitor for missing patches, application, or configuration changes that can introduce vulnerabilities which can be exploited.

6. **Look for integrated families of products with centralized management that are integrated with or aware of the network infrastructure, or common monitoring capabilities for unified management of risk, policy controls, and network security.** This will also give detailed reports across all controls that provide the audit trail necessary for risk management, governance, and compliance objectives. Integrated families of products need not necessarily be procured from just one vendor. Look for those that leverage the needed capabilities of a strong ecosystem of partnerships to provide a consolidated solution across all data center assets.

7. **Consider future as well as current needs and objectives at the design stage such as whether access to public cloud environments is required.**

8. **Define policies and profiles that can be segmented and monitored in multi-tenant environments.** Consider security technologies that provide secure gateway connections to public cloud resources.

What are the security requirements for a computer system?

1. Secure user authentication protocols including:
   a. Control of user IDs and other identifiers;
   b. Reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
   c. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
   d. Restricting access to active users and active user accounts only; and
   e. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. Secure access control measures that:
   a. Restrict access to records and files containing personal information to those who need such information to perform their job duties; and
   b. Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

3. Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;

4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;

5. Encryption of all personal information stored on laptops or other portable devices;

6. For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information;

7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis;

Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Encryption

What does the Commission say about encryption?

In relation to off-site access by government personnel to sensitive personal information, Section 23 of the DPA provides that any technology used to store, transport, or access sensitive personal information for purposes of off-site access approved shall be secured using the most secure encryption standard recognized by the Commission.

What should be encrypted?

All personal data that are digitally processed must be encrypted, whether it is at rest or in transit. According to Section 8 of Memorandum Circulars 16-01, the Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate e ncryption standard.

Emails

Email has become an essential tool for communication. Most of us use emails for either business or personal use, often to transmit files and information, which would inevitably include personal data.

Section 24 of NPC Circular No. 16-01 provides that a government agency that transfers personal data by email must either ensure that the data is encrypted, or use a secure email facility that facilitates the encryption of the data, including any attachments. Passwords should be sent on a separate email. It is also recommended that agencies utilize systems that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.

Portable Media

Using portable devices can increase the risk of data loss (when a physical device is lost), data exposure (when data is exposed to the public or a third party), and increased exposure to network-based attacks to and from any system the device is connected to. Reports say that 25% of malware is spread today through USB devices. Thus, there is a need to reduce these risks associated with the use of portable media.

Section 26 of NPC Circular No. 16-01 provides that a government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.

Links (URL)
Agencies and organizations that utilize online access to process personal data should employ an identity authentication method that uses a secured encrypted link.

Reference:

https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120
https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Access Control Policy

What is access control policy?

Having all the latest software security tools does not mean that your system is safe from any attacks. Continuous improvement in security of information and data processing systems is a fundamental management responsibility.

All applications and processing systems that deal with personal and sensitive personal information should include some form of authorization which is also known as access control policy. As systems grow in size and complexity, access control is a special concern for systems and applications that are distributed across multiple computers.

Access Control Policy sets requirements of credentials and identification that specify how access to computers, systems, or applications is managed, and who may access the information in most circumstances. Authentication, authorization, audit, and access approval are the common aspects of access control policy.

What are the best practices in implementing access control policy?

Personal information controllers and processors are responsible and accountable for protecting the personal data that is being processed.

This may be done by managing the areas, distribution, and life-cycle of authentication and authorization of your organization's processes. Access to any personal data must always be protected, controlled, and managed with sufficient security policies.

Physical and systematic approach in creating and managing access control should also be established by the management. Also, the small to large scale applications of the personal information controllers and personal information processors should be taken into consideration in the design and implementation of the policy.

What does the Commission say about implementing access control policy?

Personal information controllers and personal information processors are obliged to implement appropriate organizational, physical, and technical security measures for the protection of the personal data that they process.

Specifically for government agencies, Section 9 of NPC Circular 16-01 provides that access to all data centers owned and controlled by a government agency shall be restricted to agency personnel that have the appropriate security clearance and enforced by an access control system that records when, where, and by whom the data centers are accessed.
Furthermore, Section 25 of the said circular mandates all government agencies to implement access controls to prevent agency personnel from printing or copying personal data to personal productivity software like word processors and spreadsheets that do not have any security or access controls in place.

VI. Breaches

t. Data Breach Management

Security Incident Policy

The Security Incident Management Policy
All personal information controllers (PICs) and personal information processors (PIP) must implement a security incident management policy. This policy is for **managing security incidents,** including data breaches.

Data Breach Response Team

NPC Circular 16-03 Sec. 5
A personal information controller or personal information processor shall constitute a data breach response team, which shall have at least one (1) member with the authority to make immediate decision regarding critical action, if necessary. The team may include the Data Protection Officer.

Incident Response Procedure

NPC Circular 16-03 Sec. 8
The personal information controller or personal information processor shall implement policies and procedures for guidance of its data breach response team and other personnel in the event of a security incident.

Breach Documentation

NPC Circular 16-03 Sec. 8
All action taken by a personal information controller or personal information processor shall be properly documented. Reports should include:

a. Description of the personal data breach, its root cause and circumstances regarding its discovery;

b. Actions and decisions of the incident response team;

c. Outcome of the breach management, and difficulties encountered; and

d. Compliance with notification requirements and assistance provided to affected data subjects.

Breach Notification

IRR Sec. 38. Data Breach Notification

a. The Commission and affected data subjects shall be notified by the personal information controller within 72 hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a security breach requiring notification has occurred.

b. Notification of security breach shall be required 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.

c. Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the information security breach. Investigations may include on-site examination of systems and procedures.

VII. Third Parties

u. Third Parties

a. Legal Basis of Disclosure

Sharing of personal information between two entities without any proof or documentary evidence such as data sharing agreement is a big red flag in ensuring data protection. An agreement between two parties is required when sharing personal information especially sensitive personal information. It is an evidence of accountability that ensures the protection of personal data. Organizations should always check the legal basis of sharing the information to other controllers.

There are government agencies or entities that are mandated by law to collect personal information. This is very particular to agencies that are required to collect and share personal information to other agencies or entities to achieve their mandated functions. But this does not mean that they do not need a data sharing agreement. It is essential to acknowledge and manage the concerns regarding confidentiality, costs gained in data sharing, and legitimacy of the request. Personal information controllers and personal information processors should prioritize the protection of the rights of the data subjects and follow the principles of specific, freely given, and informed consent.

b. Data Sharing Agreements

What is a Data Sharing Agreement?
A data sharing agreement refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties. Only personal information controllers shall be made parties to a data sharing agreement. Where a data sharing agreement involves the actual transfer of personal data or a copy from one party to another, such transfer shall comply with the security requirements imposed by the Philippine Data Privacy Act, its IRR, and all applicable issuances of the National Privacy Commission.

What are the things I should see on a Data Sharing Agreement?

- Purpose
- Identity of all PICs party to the agreement
- Term or duration of the agreement
- Operational details of the sharing or transfer of personal data
- General description of the security measures for the protection of personal data, including the policy for retention or disposal of records
- Inform how a data subject can obtain a copy of the data sharing agreement
- Details on online access
- Specify the PIC responsible for addressing any information request, or any complaint filed by a data subject, and/or any investigation by the Commission
- Identify the method that shall be adopted for the secure return, destruction, or disposal of the shared data
- Other terms and conditions

(please refer to page 116)

DATA SHARING AGREEMENT

(Note: Please consider the results of your Privacy Impact Assessment.)

This Data Sharing Agreement, entered into this ____ day of _____ 2018 in _____ by and between

[PERSONAL INFORMATION CONTROLLER A]

and

[PERSONAL INFORMATION CONTROLLER B]

[PERSONAL INFORMATION CONTROLLER A] and [PERSONAL INFORMATION CONTROLLER B], hereinafter collectively referred to as "Parties", have reached the following agreement:

Section 1. Purpose of Data Sharing

1.1. The Parties are entering into this Agreement, and [PERSONAL INFORMATION CONTROLLER A] is granting [PERSONAL INFORMATION CONTROLLER B] access to the personal data described under Section 2 hereof for the following purposes:

a. [MAIN PURPOSE]

b. [PUBLIC FUNCTION, PUBLIC SERVICE OR BUSINESS ACTIVITY THE PERFORMANCE OF WHICH THE AGREEMENT IS MEANT TO FACILITATE]

c. [IF THE PURPOSE INCLUDES THE GRANT OF ONLINE ACCESS TO PERSONAL DATA, OR IF ACCESS IS OPEN TO THE PUBLIC OR PRIVATE ENTITIES, THESE SHALL ALSO BE CLEARLY SPECIFIED HEREIN.]

1.2. 1.2. [PERSONAL INFORMATION CONTROLLER B], on the other hand, is granting [PERSONAL INFORMATION CONTROLLER A] access to the personal data described under Section 2 hereof for the following purposes.

a. [MAIN PURPOSE]

b. [PUBLIC FUNCTION, PUBLIC SERVICE OR BUSINESS ACTIVITY THE PERFORMANCE OF WHICH THE AGREEMENT IS MEANT TO FACILITATE

c. [IF THE PURPOSE INCLUDES THE GRANT OF ONLINE ACCESS TO PERSONAL DATA, OR IF ACCESS IS OPEN TO THE PUBLIC OR PRIVATE ENTITIES, THESE SHALL ALSO BE CLEARLY SPECIFIED HEREIN.]

Section 2. Personal Data to be Shared

[TYPE OF PERSONAL DATA TO BE SHARED UNDER THE AGREEMENT FOR EVERY PARTY]

[CATEGORIES OF PERSONAL DATA WHETHER PERSONAL INFORMATION OR SENSITIVE PERSONAL INFORMATION]

Section 3. Consent of the Data Subject

Parties charged with the collection of personal data directly from the data subjects assure and undertake to obtain the consent of the data subject prior to collection and processing, except where such consent is not required for the lawful processing of personal data, as provided by law.

a. The identity of personal information controllers or personal information processors that will be given access to the personal data;

b. The purpose of data sharing;

c. The categories of personal data concerned;

d. Intended recipients or categories of recipients of the personal data;

e. Existence of the rights of data subjects, including the right to access and correction, and the right to object. However, the other party shall be informed of any request to access or correct personal information which is the subject matter of this sharing agreement; and

f. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

Section 4. Procedures for Use or Process of Personal Data

Parties assure and undertake to inform the data subjects of the following information prior to collection or before personal data is shared:

a. The identity of personal information controllers or personal information processors that will be given access to the personal data;

b. The purpose of data sharing;

c. The categories of personal data concerned;

d. Intended recipients or categories of recipients of the personal data;

e. Existence of the rights of data subjects, including the right to access and correction, and the right to object. However, the other party shall be informed of any request to access or correct personal information which is the subject matter of this sharing agreement; and

f. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

4.1. Manner of Sharing and Processing. [HOW PARTIES MAY USE OR PROCESS THE PERSONAL DATA, INCLUDING, BUT NOT LIMITED TO, ONLINE ACCESS]. Provided that processing and sharing must adhere to the data privacy principles laid down in Republic Act No. 10173, its Implementing Rules and Regulations, and other issuances of the National Privacy Commission.

4.2. Standard of Care. A party to this Agreement who receives personal data from the other party shall exercise at least the same degree of care as it uses with its own personal data and confidential information, but in no event less than reasonable care, to protect the personal data from misuse and unauthorized access or disclosure.

4.3. Safeguards Around Personal Data. A party to this Agreement who receives personal data from the other party shall use appropriate safeguards to protect the personal data from misuse and unauthorized access or disclosure, including maintaining adequate physical controls and password protections for any server or system on which the personal data is stored, ensuring that personal data is not stored on any mobile device (for example, a laptop or smartphone) or transmitted electronically unless encrypted (using encryption standard prescribed by the National Privacy Commission), and taking any other measures reasonably necessary to prevent any use or disclosure of the personal data other than as allowed under this Agreement.

4.4. Permitted Disclosure. Parties may disclose the personal data only to:

a. The extent necessary;
b. To authorized persons only;
c. With notice to the other party; and
d. With the consent of the data subject or when expressly authorized by law.

4.5. Required Disclosure. If a party is compelled by law to disclose any personal data, it shall notify the other party of such fact before disclosing the compelled personal data.

4.6. Breach Management

a. Report. Within twenty-four (24) hours of becoming aware of any unauthorized use or disclosure of the personal data or any security incident or possible security breach, a party shall promptly report such fact to the other party who shared the personal data. Both Parties shall, within seventy-two (72) hours from such occurrence, notify the National Privacy Commission and the concerned data subjects in accordance with NPC Circular 16-03.

b. Cooperation and Mitigation. A party who receives the personal data shall cooperate with any mediation that the other party, in its discretion, determines is necessary to:

i. address any applicable reporting requirements, and
ii. mitigate any effects of such unauthorized use or disclosure of the personal data or any security incident or possible security breach, including

measures necessary to restore goodwill with stakeholders, including research subjects, collaborators, governmental authorities, and the public.

4.7. No Modification of Personal Data. A party shall not copy, decompile, modify, reverse engineer, or create derivative works out of any of the personal data receives from or shared by the other party.

Section 5. Operational Details of the Sharing or Transfer of Personal Data

[OVERVIEW OF THE OPERATIONAL DETAILS OF THE SHARING OR TRANSFER OF PERSONAL DATA AND MUST EXPLAIN TO A DATA SUBJECT THE NEED FOR THE AGREEMENT, AND THE PROCEDURE THAT THE PARTIES INTEND TO OBSERVE IN IMPLEMENTING THE SAME]

Section 6. Security Measures

[GENERAL DESCRIPTION OF THE SECURITY MEASURES TO MAINTAIN THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF PERSONAL DATA AND TO ENSURE THE PROTECTION OF THE PERSONAL DATA OF DATA SUBJECTS, INCLUDING THE POLICY FOR RETENTION OR DISPOSAL OF RECORDS]
[ADEQUATE SAFEGUARDS FOR DATA PRIVACY AND SECURITY MUST BE DETAILED AND REITERATE THE DUTY TO UPHOLD THE RIGHTS OF THE DATA SUBJECTS]

What must be done to safeguard:

Confidentiality: make sure that data are only available to the persons who are to have access to them.

Integrity: prevent unauthorized or inadvertent change to personal data.

Availability: ensuring access to personal data where accessibility is necessary.

[WHERE A DATA SHARING AGREEMENT INVOLVES THE ACTUAL TRANSFER OF PERSONAL DATA OR A COPY THEREOF FROM ONE PARTY TO ANOTHER, SUCH TRANSFER SHALL COMPLY WITH THE SECURITY REQUIREMENTS IMPOSED BY THE ACT, ITS IRR, AND ALL APPLICABLE ISSUANCES OF THE NATIONAL PRIVACY COMMISSION.]

(Note: Please refer to NPC Circular 16-01: Security of Personal Data in Government Agencies.)

Section 7. Online Access to Personal Data

[IF A PARTY SHALL GRANT ONLINE ACCESS (AS REFERRED IN SECTION 4.1) TO PERSONAL DATA UNDER ITS CONTROL OR CUSTODY TO THE OTHER, IT SHALL SPECIFY THE FOLLOWING INFORMATION:

a. JUSTIFICATION FOR ALLOWING ONLINE ACCESS;

b. PARTIES THAT SHALL BE GRANTED ONLINE ACCESS;

c. TYPES OF PERSONAL DATA THAT SHALL BE MADE ACCESSIBLE ONLINE;

d. ESTIMATED FREQUENCY AND VOLUME OF THE PROPOSED ACCESS; AND

e. PROGRAM, MIDDLEWARE AND ENCRYPTION METHOD/ STANDARD THAT WILL BE USED.]

[WHERE A GOVERNMENT AGENCY GRANTS ONLINE ACCESS TO PERSONAL DATA UNDER ITS CONTROL OR CUSTODY, SUCH ACCESS MUST BE DONE VIA A SECURE ENCRYPTED LINK. THE GOVERNMENT AGENCY CONCERNED MUST DEPLOY MIDDLEWARE THAT SHALL HAVE FULL CONTROL OVER SUCH ONLINE ACCESS.]

Section 8. Mutual Representations

a. No Restriction. Neither party is under any restriction or obligation that could affect its performance of its obligations under this Agreement.

b. No Violation, Breach, or Conflict. Neither party's execution, delivery, and performance of this Agreement and the other documents to which it is a party, and the consummation of the transactions contemplated in this Agreement, do or will result in its violation or breach of the Data Privacy Act of 2012, its IRR and other issuances of the National Privacy Commission, and other related and applicable laws, or conflict with, result in a violation or breach of, constitute a default under, or result in the acceleration of any material contract.

c. Ownership. The party sharing personal data has the [exclusive] right to grant the other party use of the personal data.

Section 9. Return, Destruction, or Disposal of Transferred Personal Data

[UNLESS OTHERWISE PROVIDED BY THE DATA SHARING AGREEMENT, ALL PERSONAL DATA TRANSFERRED TO OTHER PARTIES BY VIRTUE
OF SUCH AGREEMENT SHALL BE RETURNED, DESTROYED, OR DISPOSED OF, UPON THE TERMINATION OF THE AGREEMENT.]
[IT SHALL IDENTIFY THE METHOD THAT SHALL BE ADOPTED FOR THE SECURE RETURN, DESTRUCTION OR DISPOSAL OF THE SHARED DATA AND THE TIMELINE THEREFOR.]

On the expiration or termination of the Agreement, or on a party's request, the other party shall promptly:

a. return the personal data and any other property, information, and documents, including confidential information, provided by it;

b. delete all the personal data including confidential information provided by it,

relating to the data processing and sharing;

c. destroy all copies it made of personal data and any other property, information, and documents, including confidential information; and

d. if requested, deliver to the requesting party an affidavit or certification confirming the other party's compliance with the return or destruction obligation under this section.

Upon termination or expiration of this Agreement, the party who receives the personal data shall cease all further use of any personal data, whether in tangible or intangible form.

Section 10. Use of Name

Neither party will use the other party's name, logos, trademarks, or other marks without that party's written consent.

Section 11. Term

[IT SHALL SPECIFY THE TERM OR DURATION OF THE AGREEMENT, WHICH MAY BE RENEWED ON THE GROUND THAT THE PURPOSE/S OF SUCH AGREEMENT CONTINUES TO EXIST: PROVIDED, THAT IN NO CASE SHALL SUCH TERM OR ANY SUBSEQUENT EXTENSIONS THEREOF EXCEED FIVE (5) YEARS, WITHOUT PREJUDICE TO ENTERING INTO A NEW DATA SHARING AGREEMENT.]

11.1. Effectivity. This Agreement is effective upon the date last signed and executed by the duly authorized representatives of the Parties to this Agreement and shall remain in full force and effect until modified or terminated by mutual agreement, in writing, by both Parties.

11.2. Termination on Notice. Either party may terminate this agreement on any valuable cause on through a written notice delivered to the other party [TERMINATION NOTICE DAYS] days prior to the termination date.

11.3. Termination for Material Breach. So long as the rights and welfare of the data subjects will not be prejudiced, each party may terminate this agreement with immediate effect by delivering notice of the termination to the other party, if:

a. the other party fails to perform, has made or makes any inaccuracy in, or otherwise materially breaches, any of its obligations, covenants, or representations, and

b. the failure, inaccuracy, or breach continues for a period of [BREACH CONTINUATION DAYS] days after the injured party delivers notice to the breaching party reasonably detailing the breach.

11.4. This Agreement may likewise be extended, by mutual consent, through a written notice by either party of its intention to extend this Agreement thirty (30) days before the termination period set.

Section 12. Remedies of the Data Subject

[REMEDIES AVAILABLE TO A DATA SUBJECT, IN CASE THE PROCESSING OF PERSONAL DATA VIOLATES HIS OR HER RIGHTS, AND HOW THESE MAY BE EXERCISED]

Section 13. Indemnification

The defaulting party shall indemnify the aggrieved party against all losses and expenses arising out of any proceeding:

a. Brought by either a third party or by the aggrieved party;

b. arising out of the party's breach of its obligations, representations, warranties, or covenants under this agreement; and

c. Arising out of the defaulting party's willful misconduct or gross negligence.

Section 14. Authorized Personal Information Processor

[ANY PERSONAL INFORMATION PROCESSOR, NOT PARTY TO THIS AGREEMENT, THAT WILL HAVE ACCESS TO OR PROCESS THE SAME PERSONAL DATA SHARED TO AND BY ANY OF THE PARTIES INCLUDING THE TYPES OF PROCESSING IT SHALL BE ALLOWED TO PERFORM]

Section 15. Data Protection Officer or Compliance Officer

[DESIGNATED DATA PROTECTION OFFICERS AND COMPLIANCE OFFICERS FOR PRIVACY OF THE PARTIES, THEIR POSITIONS IN THE COMPANY/ AGENCY AND THEIR CONTACT DETAILS]

Section 16. Personal Information Controller Responsible for Information Request, or Any Complaint

[PERSONAL INFORMATION CONTROLLER RESPONSIBLE FOR ADDRESSING ANY INFORMATION REQUEST, OR ANY COMPLAINT FILED BY A DATA SUBJECT AND/ OR ANY INVESTIGATION BY THE NATIONAL PRIVACY COMMISSION]

Section 17. General Provisions

17.1. Security of Personal Data. Data sharing shall only be allowed where there are adequate safeguards for data privacy and security. Parties shall use contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred.

17.2. Access of the Data Sharing Agreement. [STATE HOW A COPY OF THE AGREEMENT MAY BE ACCESSED BY A DATA SUBJECT]

[GOVERNMENT AGENCY MAY REDACT OR PREVENT THE DISCLOSURE OF ANY DETAIL OR INFORMATION THAT COULD ENDANGER ITS COMPUTER NETWORK OR SYSTEM, OR EXPOSE TO HARM THE INTEGRITY, AVAILABILITY OR CONFIDENTIALITY OF PERSONAL DATA UNDER ITS CONTROL OR CUSTODY. SUCH INFORMATION MAY INCLUDE THE PROGRAM, MIDDLEWARE AND ENCRYPTION METHOD IN USE AS PROVIDED IN SECTION 7.]

17.3. Responsibility of the Parties. Parties shall comply with the Act, its IRR, and all applicable issuances of the National Privacy Commission, including putting in place adequate safeguards for data privacy and security.

17.4. Confidentiality Obligations. The party who receives shall hold the other party's personal data in strict confidence. Each party will use the same degree of care to protect the data as it uses to protect its own data of like nature, but in no circumstances less than reasonable care. The party who receives shall ensure that its employees or agents are bound to the same obligations of confidentiality as the other party. The obligation of confidentiality shall be maintained even after the termination of this Agreement but shall not apply with respect to information that is independently developed by the Parties, lawfully becomes a part of the public domain, or of which the Parties gained knowledge or possession free of any confidentiality obligation.

17.5. Accountability for Cross-border Transfer of Personal Data. Each party shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.

17.6. Assignment. Neither party may assign this Agreement or any of their rights or obligations under this Agreement without the other party's written consent and notice to the data subjects.

17.7. Governing Law. This Agreement shall be governed, construed, and enforced in accordance with the laws of the Republic of the Philippines.

17.8. Mandatory Periodic Review. The terms and conditions of this Agreement shall be subject to a mandatory review by the Parties thereto upon the expiration of its term, and any subsequent extensions thereof. The Parties shall document and include in its records:

A. reason for terminating the agreement or, in the alternative, for renewing its term; and

B. in case of renewal, any changes made to the terms and conditions of the agreement.

17.9 Review and Modification. Parties hereby authorizes the National Privacy Commission to review the contents of this Agreement and, whenever it becomes necessary, suggest any amendment or revision hereof.

In such a case, **Parties** shall execute an amended Agreement within fifteen (15) days from Notice of Review by the National Privacy Commission containing its observations and suggestions in order to be compliant with the provisions of the

Data Privacy Act, its Implementing Rules and Regulations and other issuances of the National Privacy Commission.

17.10 Severability. If any part of this Agreement is declared unenforceable or invalid, the remainder will continue to be valid and enforceable.

17.11 Alternative Dispute Resolution. In the event of any dispute or difference of any kind whatsoever arising out of or relating to this Agreement, the Parties shall, at first instance, exercise their best efforts to resolve the dispute or difference by mutual consultation as soon as possible. In case best efforts fail, the dispute or difference shall be referred to alternative dispute resolution which shall be governed in accordance with the provisions provided in Republic Act No. 9285, otherwise known as the "Alternative Dispute Resolution Law." The seat of the arbitration shall be the Philippines.

17.12 Venue of Actions. In case of a court suit, the venue shall be the courts of competent jurisdiction in [CITY OR MUNICIPALITY WHERE THE ACTIONS WILL BE FILED] to the exclusion of all other courts subject to prior resort to alternative dispute resolution as herein prescribed.

IN WITNESS WHEREOF, the Parties hereto have affixed their respective signatures this _____ day of _____ 2018 in _____, Philippines.

Name Position Name of Organization/Institution	**Name** Position Name of Organization/Institution

WITNESS
ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
_____) S S

Name Position Name of Organization/Institution	**Name** Position Name of Organization/Institution

Before me this ____ day of _____ 2018 in _____ personally appeared:

Names	Government Issued Identification Document			
	ID No.	Date	Place Issued	Expiry Date

all known to me and to me known to be the same persons who executed the foregoing instrument consisting of _____ pages including this page, and they acknowledged to me that the same is their own free and voluntary act and deed and the entities they represent.

IN WITNESS WHEREOF, I have hereunto set my hand this _____ day of _____, 2018.

Doc No. _____;
Page No. _____;
Book No. _____;
Series of 2018.

c. Cross Border Transfer Agreement

Globally, there is a general recognition that there should be some law regarding cross-border data transfers, but a wide variety of approaches to this issue exist, and there is no single global model for managing it. At the national level, some countries have no restrictions at all on the transfer of personal information to a foreign jurisdiction.

IRR Sec. 50

states that a personal information controller shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. This includes contracting with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

VIII. Manage HR

v. Trainings and Certifications

IRR Sec. 26. enjoins personal information controllers and personal information processors to provide capacity building, orientation or training programs regarding privacy or security policies for employees, agents or representatives, particularly those who will have access to personal data.

In addition, NPC Circular No. 16-01 provides that one of the general obligations of a government agency engaged in the processing of personal data is to conduct a mandatory, agency-wide training on privacy and data protection policies once a year. A similar training shall be provided during all agency personnel orientations.

Note that capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents is also required under NPC Circular No. 16-03 – Personal Data Breach Management.

Likewise, NPC Advisory No. 17-01 on the Designation of DPOs, provides that all personal information controllers or processors should provide sufficient time and resources, including training, necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently.

Recommended Certifications

Currently, there is no certification process for an organization's compliance with the DPA.

Nonetheless, it is advisable for organizations to obtain certifications or accreditations such as those prescribed by the International Standards Organization (ISO), specifically the ISO 27000 family - Information Security Management Systems (ISMS):

- *ISO/IEC 27001:2013.* Information technology -- Security techniques -- Information security management systems – Requirements. This specifies the requirements for

establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

- *ISO/IEC 27002:2013.* Information technology -- Security techniques -- Code of practice for information security controls. This gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

- *ISO/IEC 27018:2014.* Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. This establishes commonly-accepted control objectives, controls, and guidelines for implementing measures to protect personal information in accordance with the privacy principles in ISO/IEC 29100, which, in turn, concerns public cloud computing environments. It also specifies guidelines based on ISO/IEC 27002, taking into account the regulatory requirements for the protection of personal information that might be applicable within the context of the information security risk environment(s) of a (public) cloud service provider. It may be used by organizations of any type and size, including public and private companies, government entities, and non-profit organizations, which provide information processing services as personal information processors via cloud computing under contract to other organizations.

The Commission does not require certifications for key personnel of personal information controllers or personal information processors, such as the latter's Data Protection Officer or Compliance Officer for Privacy.

However, it is considered best practice across jurisdictions for organizations to properly equip their personnel with appropriate trainings that enable them to fulfill their specific roles and functions. Some international certifications or trainings commonly considered for this purpose include the following:

- *Certified Information Systems Auditor (CISA).* CISA is a globally recognized certification for IS audit control, assurance, and security professionals. A person's CISA certification attests to his or her audit experience, skills, and knowledge. It demonstrates one's ability to assess vulnerabilities, report on compliance, and institute controls within a particular enterprise.

- *Certified Information Security Manager (CISM).* A management-focused CISM certification that promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security.

- *Certified in the Governance of Enterprise IT (CGEIT).* This certification recognizes a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices. A CGEIT certified professional has demonstrated his or her ability to bring IT governance into an organization, as well as his or her complete grasp of the complex subject. Thus, he is able to enhance the value of an enterprise.

- *Certified Information Systems Security Professionals (CISSP).* The ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage the overall information security program of their organization, thereby protecting it from the growing number of sophisticated attacks.

- *GIAC Security Essentials (GSEC).* Designed for professionals seeking to demonstrate their understanding of information security terminology and concepts, and their possession of skills and technical expertise necessary for "hands-on" security roles. GSEC credential holders are presumed to demonstrate a knowledge and technical skills in various areas (e.g., identifying and preventing common and wireless attacks, access controls, authentication, password management, DNS, cryptography fundamentals, ICMP, IPv6, public key infrastructure, Linux, network mapping, and network protocols).

- *Project Management Professional (PMP).* This certification is touted as the most important industry-recognized certification for project managers. It signifies that the holder speaks and understands the global language of project management. It connects him or her to a community of professionals, organizations and experts worldwide. Indeed, unlike other certifications that focus on a particular geography or domain, the PMP is truly global and enables its holder to work in virtually any industry, with any methodology, and in any location.

While not explicitly required, certifications and/or accreditations allow for a more efficient verification and monitoring process on the part of the Commission.

w. Security Clearance

A security clearance allows authorized access to personal information that would otherwise be forbidden. In Section 23 of the DPA, requirements relating to access by agency personnel to sensitive personal Information.

> *On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.*

To ensure confidentiality of personal data, PIC or PIP shall only grant security clearance to an employee when the performance of his or her official functions directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

Non-Disclosure Agreement (NDA)

One common way to protect confidential information given to another party is the use of Non-Disclosure Agreement (NDA). A non-disclosure agreement is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes. It should contain a few specific parts: definitions and exclusions of confidential information; obligations form all involved people or parties; and time periods.

IX. Continuity

x. Continuing Assessment and Development

Regular Risk Assessment

Necessity, convenience and continuous improvement are the forefathers of invention. These usher the introduction and adaptation of new systems by organizations to execute necessary business functions. It is imperative to conduct a Privacy Impact Assessment to all data processing systems that are classified as "High" and have "Unreasonable" impact assessment.

A Privacy Impact Assessment to data processing systems in an organization should not be a onetime affair. This shall be conducted regularly, maintaining later updates or upgrades with additional functionality likely to impact the personal information that are handled. Kindly refer to Privacy Impact Assessment for more information.

NPC Circular 16-01 Sec. 4b

States that conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data, Provided, that such assessment shall be updated as necessary.

	LOW	MEDIUM	HIGH
Type of Data	No personal data	Personal Information	Sensitive Personal Information
Volume	Less than 250 records	Less than 1,000 records	1,000 or more records
Origin		Filipino citizens only	includes other nationalities
Access	Limited to onsite	Onsite as well as offsite	External parties
Time of access	Less than 8 hours	8 to 12 hours	24 hours
Number of users	Less than 50	Less than 250	250 or more
Response requirement	None	Sub-minute	Sub-second
Storage media	Non-digital	All digital	Mixed
Storage location		One-site	Multiple sites
Big data projects	No plans	when 3 years	currently operating

Internal Assessments

To make compliance with the Act manageable, organizations are advised to schedule regular compliance monitoring, internal assessments and security audits. The purpose of an internal assessment is to identify and strategically plan the needed maintenance of an organization to align it with the DPA. NPC recommends creation of policies on conduct of internal assessments and security audits.

Review Privacy Management Program (PMP)

Regularly evaluating Privacy Management Program demonstrates accountability of organizations. The Privacy Management Program is maintained through organizational commitment and oversight of coordinated projects and activities implemented throughout the agency, company or organization. It allows efficient use of available resources, implements control measures to assure privacy and data protection, and puts in place a system for review to allow for improvements responsive to data privacy best practices and technological developments.

To properly protect personal data and meet legal obligations, PICs and PIPs should monitor, assess and revise their privacy management framework to ensure it remains relevant and effective.

Accreditations

(please refer to page 126)

X. Privacy Ecosystem

y. New Technologies and Standards

z. New Legal requirements

Monitor Privacy Competency

Technology is fast changing. With the constant rise of trends, this leads to having its own privacy and legal implications. Keeping up to date can become a chore that is easy to delay. Below are some tips on how to be updated with the latest trends in technology.

1. Industry Players

   Participate in workshops, summits and various talks held by accredited associations and government regulators

2. Print Media (Books and Magazines)

   Books and magazines are great information resources. Subscribe to monthly digests on tech magazines for timely reading. While books can be a great resource, make sure the book is based on the correct version of the technology you are researching.

3. Social Media (Twitter, Facebook, Email Subscription, etc.)

   Follow seasoned tech gurus and subscribe for notification on tech news pages, relevant government pages (National Privacy Commission, Department of Information and Communications Technology, Cybercrime Investigation and Coordination Center) to be in the loop for recent trends and advisories in information security, cybercrime and privacy news.

4. Training

Another great resource is the various forms of training and web-based tutorials. If you can afford to get professional training (either online or in-house), this is probably the best approach. However, this can be costly. Nowadays, many sites offer great tutorials that get you knee-deep in the latest technologies for free. There are also many web casts available from various conferences or events where the presenter is conducting a demo on a new technology. Locate these resources through searches and through your blogs and podcasts.

5. Face-to-Face (user group meetings and technical conferences)

User group meetings and forums are usually technology specific and give you a chance to meet people locally that are doing what you are doing, learn about what they are doing, and get great presentations on the latest and greatest happenings in your technology and various processes. This is also a great way to learn about conferences you can attend or hear about from those that did attend. These conferences are showcases for the “new stuff”.

6. Recent Developments

Recently, there are many recent developments in technology and privacy-legal area. Strategies to be updated include by keeping track of local and international Government Issuances, recent local and international government enforcements, International Standards released by ISO, International Organizations’ current practices and relevant frameworks.

5. BE PREPARED FOR BREACH:

REGULARLY EXERCISE YOUR BREACH REPORTING PROCEDURE

Data Breaches and Security Incidents

Assessment

A *security incident* is any event or occurrence that affects or tends to affect data protection, or may compromise the *availability, integrity,* and *confidentiality* of personal data. It includes incidents that may result in a personal data breach, if not for safeguards that have been put in place.

A data breach is a kind of security incident. It happens when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

There are three kinds of data breaches:

- *Availability Breach* – results from the accidental loss or unlawful destruction of personal data;
- *Integrity Breach* – results from the unauthorized alteration of personal data; and
- *Confidentiality Breach* – results from the unauthorized disclosure of or access to personal data.

The Security Incident Management Policy

All personal information controllers (PICs) and personal information processors (PIP) must implement a security incident management policy. This policy is for managing security incidents, including data breaches.

In drafting your security incident management policy and personal data breach management procedure, the following must be included:

- Creation of a *security incident response team*, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- Implementation of organizational, physical and technical security measures, and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- Implementation of an incident response procedure intended to contain a security incident or personal data breach, and restore the integrity of the information and communications system;
- Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- Compliance with the DPA, its IRR, and all related issuances by the NPC pertaining to personal data breach notification.

The Security Incident Management Policy must also include measures intended to prevent or minimize the occurrence of a personal data breach. These measures include:

- *Conduct of a Privacy Impact Assessment* to identify attendant risks in the processing of personal data. It shall take into account the size and sensitivity of the personal data being processed,

the impact and likely harm of a personal data breach;
- *Data governance policy* that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;
- *Implementation of appropriate security measures* that protect the availability, integrity and confidentiality of personal data being processed;
- *Regular monitoring for security breaches* and vulnerability scanning of computer networks;
- *Capacity building of personnel* to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents;
- *Procedure for the regular review of policies and procedures*, including the testing, assessment, and evaluation of the effectiveness of the security measures.

The Security Incident Response Team

The Security Incident Response Team is responsible for:

- *Implementing security incident management policy* of the PIC or PIP;
- *Managing security incidents* and personal data breaches; and
- *Compliance* by the PIC or PIP with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

Although the functions of the Security Incident Response Team may be outsourced, and there is no precise formula for its composition, its members must, as a collective unit, be ready to *assess and evaluate* a security incident, *restore integrity* to the information and communications system, *mitigate and remedy* any resulting damage, and comply with reporting requirements.

Annual Reports

PICs and PIPs are required to submit their Annual Report, where all security incidents and personal data breaches must be documented through *written reports*, including those not covered by the notification requirements.

In the event of a personal data breach, a report shall include:

a. the facts surrounding the incident;
b. the effects of such incident; and
c. the remedial action taken by the PIC. For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation.

Any or all *reports shall be made available when requested* by the Commission: Provided, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the:

1. number of incidents and breach encountered; and
2. information classified according to their impact on the availability, integrity, or confidentiality of personal data.

Not all data breaches have to be reported to the NPC. Only when these are all present are the PICs (or PIPs, as the case may be) required to notify:

- there is a breach of sensitive personal information or other information that may, under the

circumstances, be used to enable identity fraud;
- the data is reasonably believed to have been acquired by an unauthorized person; and
- either the PIC or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

If there is doubt as to whether notification is indeed necessary, consider:

1. the likelihood of harm or negative consequences on the affected data subjects;
2. how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and
3. if the data involves:
   - information that would likely affect national security, public safety, public order, or public health;
   - at least one hundred (100) individuals;
   - information required by all applicable laws or rules to be confidential; or
   - personal data of vulnerable groups.

The failure to notify the NPC or the public may make you criminally liable for Concealment of Security Breaches Involving Sensitive Personal Information, which carries a penalty of imprisonment from one year and six months, to five years, and a fine of Five Hundred Thousand Pesos (₱500,000.00) to One Million Pesos (₱1,000,000.00).

This crime is committed by those, having knowledge of the security breach and with an obligation to inform the NPC of the fact of such a breach, either intentionally or by omission fails to inform the NPC that the breach has happened.

Aside from notifying the NPC, the PIC shall also notify the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the PIC even if the processing of information is outsourced or subcontracted to a PIP.

The Commission shall be notified within *seventy-two (72) hours* upon knowledge of or the reasonable belief by the PIC or PIP that a personal data breach has occurred.

Generally, there shall be no delay in notification however, the notification may only be delayed 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.

There can be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In either case, the Commission must be notified within the 72-hour period based on available information.

The full report of the personal data breach must be submitted within five (5) days from notification, unless the PIC is granted additional time by the Commission to comply.

The following information *must* be included in any Data Breach notification:
- *Nature of the Breach.* – There must be, at the very least, a description of:

a. the nature of the breach;
b. a chronology of events, and
c. an estimate of the number of data subjects affected;

- *Personal data involved.* – stating the description of sensitive personal information or other information involved.

- *Remedial Measures.* – there must be:
  a. description of the measures taken or proposed to be taken to address the breach;
  b. actions being taken to secure or recover the personal data that were compromised;
  c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
  d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification; and
  e. measures being taken to prevent a recurrence of the incident.

- *Name and contact details -* of the Data Protection Officer or contact person designated by the PIC to provide additional information.

Under the Data Privacy Act, the data subject has the right to be notified. Upon knowledge of, or reasonable belief that a personal data breach has occurred, the PIC must notify the data subject within 72 hours, which:

- may be made on the *basis of available information* within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects;
- shall have the *same content* as those made to the National Privacy Commission, but shall include instructions on how data subjects will get further information; and
- shall include recommendations *on how to minimize risks* resulting from breach and to secure any form of assistance.

The notification may be supplemented with additional information at a later stage on the basis of further investigation.

The notification of affected data subjects shall be done individually, using *secure means of communication,* whether written or electronic. Whenever individual notification is not possible or would require a disproportionate effort, the PIC may seek the *approval of the Commission* to use alternative means of notification.

The notification requirement is not absolute; the NPC can allow the *postponement* of notification when it may hinder the progress of a criminal investigation.

The Subsequent Investigation

The NPC will consider these factors in its investigation following the occurrence of a data breach:

- *Security measures* that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;
- *Subsequent measures* that have been taken by the PIC or PIP to ensure that the risk of harm or negative consequence to the data subjects will not materialize;
- *Age or legal capacity* of affected data subjects; provided, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives; and
- *Compliance with the law and existence of good faith* in the collection of personal information.

The Commission may investigate a breach or a security incident depending on the nature, or in case of failure or delay in the notification.

The investigation will:

- include an on-site examination of systems and procedures;
- require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects, if necessary; and
- will be governed by the Rules of Procedure of the Commission.

The Data Privacy Accountability and Compliance Checklist

Compliance Checklist	Evidence of Compliance
1. Establish Data Privacy Governance	
☐ Designate a Data Protection Officer	Designation/Appointment Papers/ Contract of the DPO and/or DPO team ☐ Other means to demonstrate compliance
2. Privacy Risk Assessment	
☐ Maintain records of processing activities, including inventory of personal data, data flow and transfers outside country ☐ Register Data Processing Systems ☐ Conduct a Risk Assessment	☐ Inventory of personal data processing systems ☐ Visible announcement showing the contact details of DPO (e.g. website, privacy notice) ☐ Phase I - Registration Form (Notarized) ☐ Privacy Impact Assessment (PIA) report ☐ Other means to demonstrate compliance

3. Maintain Organization Commitment	
☐ Implement and maintain a privacy management program ☐ Develop a privacy manual and complaints mechanism	☐ Privacy Manual ☐ List of activities on privacy and data protection ☐ List of key personnel assigned responsibilities for privacy and data protection within the organization ☐ Other means to demonstrate compliance
4. Privacy and Data Protection in day to day operations	
☐ Have visible and accessible Privacy Notices with contact details of DPO ☐ Develop, Review or Maintain Policies and Procedures for processing of personal data from collection to retention or disposal (procedure for obtaining consent) ☐ Establish procedures or platform for data subjects to exercise their rights (access, be informed, object, correction, erasure, file a complaint, be indemnified, data portability) ☐ Register Data Processing Systems (Phase II) ☐ Comply with notification and reporting requirements	☐ Privacy Notice in Website and/or within organization (where collection of personal data occurs) ☐ Consent forms for collection and use of personal data ☐ List of Policies and Procedures in place that relate to privacy and data protection (may be in privacy manual) ☐ Policies and Procedure in dealing with requests for information from parties other than the data subjects (media, law enforcement, representatives) ☐ Data subjects informed of rights through privacy notices, and other means ☐ Form or platform for data subjects to request copy of their personal information and request correction ☐ Procedure for addressing complaints of data subjects ☐ Certificate of registration and notification ☐ Other means to demonstrate compliance

5. Manage Security Risks	
☐ Maintain Organizational Security Measures (Policies and procedures in place) ☐ Maintain Physical Security Measures (Physical Access and Security, Design and Infrastructure) ☐ Maintain Technical Security Measures (Firewalls, Encryption, Access Policy, Security of Data Storage, other Information security tools) ☐ Know your vulnerabilities (Vulnerability Assessments and Penetration Testing)	☐ Data Center and Storage area with limited physical access ☐ Report on technical security measures and information security tools in place ☐ Firewalls used ☐ Encryption used for transmission ☐ Encryption used for storage ☐ Access Policy for onsite, remote and online access ☐ Audit logs ☐ Back-up solutions ☐ Report of Internal Security Audit or other internal assessments ☐ Certifications or accreditations maintained ☐ Vulnerability Assessment ☐ Penetration Testing for applications and network ☐ Other means to demonstrate compliance
6. Data Breach Management	
☐ Implement safeguards to prevent or minimize personal data breach (Breach drills, security policy) ☐ Constitute Data Breach Response Team ☐ Maintain and Review Incident Response Policy and Procedure ☐ Document Security incidents and personal data breaches ☐ Comply with Breach Notification requirements	☐ Schedule of breach drills ☐ Number of Trainings conducted for internal personnel on breach management ☐ Personnel Order constituting the Data Breach Response Team ☐ Incident Response Policy and Procedure (may be in Privacy Manual) ☐ Record of Security incidents and personal data breaches, including notification for personal data breaches ☐ Other means to demonstrate compliance

7. Manage Third Party Risks	
☐ Execute Data Sharing Agreements ☐ Review or enter into contracts and other agreements for transfers of personal data, including cross border transfers to ensure comparable level of data protection, DPA compliance, and security of transfers ☐ Review or enter into outsourcing contracts with PIPs, to ensure comparable level of data protection and DPA compliance ☐ Establish and document legal basis for disclosures of personal data made to third parties	☐ Data Sharing Agreements ☐ List of recipients of personal data (PIPs, other PICs, service providers, government agencies) ☐ Review of Contracts with PIPs ☐ Review of Contracts for cross-border transfers ☐ Other means to demonstrate compliance
8. Human Resources Management	
☐ Regularly train personnel regarding privacy or security policies. ☐ Ongoing training and capacity building for Data Protection Officer ☐ DPOs work towards certifications and applies for membership in DPO organizations ☐ Non-Disclosure Agreements for personnel handling Data ☐ Security Clearance issued for those handling personal data	☐ No. of employees who attended trainings on privacy and data protection ☐ Commitment to comply with Data Privacy Act as part of Code of Conduct or through written document to be part of employee files ☐ Certificate of Training of DPO ☐ Certifications of DPOs ☐ NDAs or confidentiality agreements ☐ Security Clearance Policy ☐ Other means to demonstrate compliance

9. Continuing Assessment and Development	
☐ Schedule Regular Risk Assessment ☐ Review Forms, Contracts, Policies and Procedures on a regular basis ☐ Schedule Regular Compliance monitoring, internal assessments and security audits ☐ Review, Validate and Revise Privacy Manual ☐ Regularly evaluate Privacy Management program	☐ Policy for Conduct of PIA (may be in manual) ☐ Policy on conduct of Internal Assessments and Security Audits ☐ Privacy Manual contains policy for regular review ☐ List of activities to evaluate Privacy Management program (survey of customer, personnel assessment) ☐ Other means to demonstrate compliance
10. Manage Privacy Ecosystem	
☐ Monitor emerging technologies, new risks of data processing, and the privacy ecosystem ☐ Keep track of data privacy best practices, sector specific standards, and international data protection standards ☐ Attend trainings and conferences ☐ Seek guidance and legal opinion on new NPC issuances or requirements	☐ No. of trainings and conferences attended on privacy and data protection ☐ Policy papers, legal or position papers, or other research initiatives on emerging technologies, data privacy best practices, sector specific standards, and international data protection standards ☐ No. of management meetings which included privacy and data protection in the agenda ☐ Other means to demonstrate compliance

CHAPTER III REGISTRATION OF DATA PROCESSING SYSTEMS

NPC Circular 17-01

DATE : 31 July 2017
TO : ALL PERSONAL INFORMATION CONTROLLERS AND PERSONAL INFORMATION PROCESSORS
SUBJECT : REGISTRATION OF DATA PROCESSING SYSTEMS AND NOTIFICATIONS REGARDING AUTOMATED DECISION-MAKING

WHEREAS, Article II, Section 24, of the 1987 Constitution provides that the State recognizes the vital role of communication and information in nation-building. At the same time, Article II, Section 11 thereof emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it 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. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secure and protected;

WHEREAS, Section 16 of the DPA and Section 34 of its Implementing Rules and Regulations (IRR) provide that data subjects shall be furnished with and given access to their personal data that are being processed in data processing systems, as well as the purpose, scope, method, and manner of such processing, including the existence of automated decision-making;

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers (PICs) with the provisions thereof, publishing a compilation of an agency's system of records and notices, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal data, in coordination with other government agencies and private entities;

WHEREAS, Section 9 of the IRR provides that, among the NPC's functions, is to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Section 24 of the DPA states that, when entering into any contract that may involve accessing or requiring sensitive personal information from at least one thousand (1,000) individuals, a government agency shall require the contractor and its employees to register their personal information processing system with the NPC in accordance with the DPA and to comply with the law's provisions. Furthermore, Section 14 of the law mandates that personal information processors (PIPs) shall also comply with all requirements of the DPA and other applicable laws;

WHEREAS, in line with Sections 46 and 47 of the IRR, a PIC or PIP that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, is not occasional, or includes sensitive personal information of at least one thousand (1,000) individuals. Moreover, Section 48 thereof declares that a PIC carrying out any automated processing operation that is intended to serve a single or several related purposes must notify the NPC when said operation becomes the sole basis for making decisions about a data subject, and when such decision would significantly affect the data subject;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the registration of data processing systems and notifications regarding automated decision-making:

RULE I.
PRELIMINARY PROVISIONS

SECTION 1. *Scope.* The provisions of this Circular shall apply to any natural or juridical person in the government or private sector processing personal data and operating in the Philippines, subject to the relevant provisions of the DPA, its IRR, and other applicable issuances of the NPC.

SECTION 2. *Purpose.* This Circular establishes the framework for registration of data processing systems in the Philippines and imposes other requirements for the purpose of achieving the following objectives:

A. ensure that PICs and PIPs keep a record of their data processing activities;

B. make information about data processing systems operating in the country accessible to both the Commission, for compliance monitoring, and data subjects, to facilitate the exercise of their rights under the DPA; and

C. promote transparency and public accountability in the processing of personal data.

SECTION 3. *Definition of Terms.* For the purpose of this Circular, the following terms are defined, as follows:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

B. "Automated Decision-making" refers to a wholly or partially automated processing operation that serves as the sole basis for making decisions that would significantly affect a data subject. It includes the process of profiling based on an individual's economic situation, political or religious beliefs, behavioral or marketing activities, electronic communication data, location data, and financial data, among others;

C. "Commission" or "NPC" refers to the National Privacy Commission;

D. "Compliance Officer for Privacy" or "COP" refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01;

E. "Core Activity" refers to a key operation or process carried out by a PIC or PIP to achieve its mandate or function: Provided, that processing of personal data forms an integral and necessary part of such operations or processes;

F. "Data Processing System" refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

G. "Data Protection Officer" or "DPO" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: Provided, that, except where allowed otherwise by law or

the Commission, the individual must be an organic employee of the government agency or private entity: Provided further, that a government agency or private entity may have more than one DPO;

H. "Data sharing" is the disclosure or transfer to a third party of personal data under the control or custody of a PIC: Provided, that a PIP may be allowed to make such disclosure or transfer if it is upon the instructions of the PIC concerned.
The term excludes outsourcing, or the disclosure or transfer of personal data by a PIC to a PIP;

I. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

J. "Encryption Method" refers to the technique that renders data or information unreadable, ensures that it is not altered in transit, and verifies the identity of its sender;

K. "Filing system" refers to any set of information relating to a natural or juridical person to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible;

L. "Government Agency" refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

M. "Head of agency" refers to: (1) the head of the government entity or body, for national government agencies, constitutional commissions or offices, or branches of the government; (2) the governing board or its duly authorized official for government-owned and -controlled corporations, government financial institutions, and state colleges and universities; (3) the local chief executive, for local government units;

N. "Head of organization" refers to the head or decision-making body of a private entity or organization;

O. "Information and Communications System" refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages, or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document;

P. "IRR" refers to the Implementing Rules and Regulations of the DPA;

Q. "Personal data" refers to all types of personal information;

R. "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, or when put together with other information would directly and certainly identify an individual;

S. "Personal information controller" or "PIC" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. a natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. a natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

T. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

U. "Private entity" or "organization" refers to any natural or juridical person that is not a unit of the government, including, but not limited to, a corporation, partnership, company, non-profit organization or any other legal entity;

V. "Privileged information" refers to all forms of data, which, under the Rules of Court and other pertinent laws, constitute privileged communication;

W. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data, such as a individual's economic situation, political or religious beliefs, behavioral or marketing activities, personal preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others;

X. Sensitive personal information refers to personal information:

1. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such 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.

SECTION 4. *General Principles.* This Circular shall be governed by the following general principles:

A. Registration of its data processing systems with the Commission shall be one of the means through which a PIC or PIP demonstrates its compliance with the DPA, its IRR, and other relevant issuances of the NPC.

B. Registration information submitted by a PIC or PIP to the Commission are presumed to contain all required information on its data processing systems that are active or existing during the validity of such registration. Any information excluded therefrom are deemed

nonexistent.

C. Unless otherwise provided in this Circular, any information, file, or document submitted by a PIC or PIP to the Commission shall be kept confidential.

D. Any doubt in the interpretation of the provisions of this Circular shall be liberally interpreted in a manner that would uphold the rights and interests of data subjects.

RULE II.
REGISTRATION OF DATA PROCESSING SYSTEMS

SECTION 5. *Mandatory Registration.* A PIC or PIP shall register its data processing systems if it is processing personal data and operating in the country under any of the following conditions:

A. the PIC or PIP employs at least two hundred fifty (250) employees;

B. the processing includes sensitive personal information of at least one thousand (1,000) individuals;

C. the processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:

i. information that would likely affect national security, public safety, public order, or public health;
ii. information required by applicable laws or rules to be confidential;
iii. vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP;
iv. automated decision-making; or
v. profiling;

D. the processing is not occasional: Provided, that processing shall be considered occasional if it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional:

In determining the existence of the foregoing conditions, relevant factors, such as the number of employees, or the records of individuals whose sensitive personal information are being processed, shall only be considered if they are physically located in the Philippines.

Data processing systems that involve automated decision-making shall, in all instances, be registered with the Commission. For all other data processing systems operating under the conditions set out in subsections C and D, the Commission shall determine the specific sectors, industries, or entities that shall be covered by mandatory registration. Appendix 1 of this Circular shall feature the initial list. It shall be regularly reviewed and updated by the Commission through subsequent issuances.

SECTION 6. *Voluntary Registration.* An application for registration by a PIC or PIP whose data processing system does not operate under any of the conditions set out in the next preceding Section shall be accepted as a voluntary registration.

SECTION 7. *When to Register.* A PIC or PIP covered by this Circular shall register its personal data processing system within two (2) months of the commencement of such system.

SECTION 8. *Authority to Register.* A PIC or PIP shall file its application for registration through its designated or appointed DPO: Provided, that where a PIC or PIP has several DPOs, only one shall be authorized to file the application of the PIC or PIP: Provided further, that where the same individual assumes the role of DPO for two or more PICs or PIPs, he or she shall be allowed to file the applications of all his or her principals.

SECTION 9. *Registration Process.* A PIC or PIP shall register through the Commission's official website in two (2) phases:

A. *Phase I.* A PIC or PIP, through its DPO, shall accomplish the prescribed application form, and submit the same to the Commission together with all supporting documents. Upon review and validation of the submission, the Commission shall provide the PIC or PIP via email an access code, which shall allow it to proceed to Phase II of the registration process.

B. *Phase II.* Using the access code provided by the Commission, a PIC or PIP shall proceed to the online registration platform and provide all relevant information regarding its data processing systems. The Commission shall notify the PIC or PIP via email to confirm the latter's successful completion of the registration process:

Provided, that registration may be done in person at the office of the Commission in the event that online access is not available.

SECTION 10. *Application Form.* An application for registration filed by a PIC or PIP must be duly-notarized and accompanied by the following documents:

A. For government agencies:

1. certified true copy of the Special/Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP; and
2. where applicable, a copy of the charter of the government entity, or any similar document identifying its mandate, powers, and/or functions.

B. For private entities:

1. duly-notarized Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation.
2. certified true copy of the following documents, where applicable:
   a.) General Information Sheet or any similar document;
   b.) Certificate of Registration (SEC Certificate, DTI Certification of Business Name or Sole Proprietorship) or any similar document; and/or
   c.) Franchise, license to operate, or any similar document.

SECTION 11. *Online Registration Platform.* In the Commission's online registration platform, a PIC or PIP shall provide the following registration information:

A. Name and contact details of the PIC or PIP, head of agency or organization, and DPO;

B. Purpose or mandate of the government agency or private entity;

C. Identification of all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;

D. Attestation regarding certifications attained by the PIC or PIP, including its relevant personnel, that are related to personal data processing;

E. Brief description of data processing system or systems:

1. Name of the system;
2. Purpose or purposes of the processing;
3. Whether processing is being done as a PIC, PIP, or both;
4. Whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
5. Description of the category or categories of data subjects, and their personal data or categories thereof;
6. Recipients or categories of recipients to whom the personal data might be disclosed; and
7. Whether personal data is transferred outside of the Philippines;

F. Notification regarding any automated decision-making operation.

This same set of information shall be given when registration is done in person at the office of the Commission.

SECTION 12. *Certificate of Registration.* The Commission shall issue a certificate of registration in favor of a PIC or PIP that has successfully completed the registration process: Provided, that such certificate shall only be considered as proof of registration and not a verification of the contents thereof.

SECTION 13. *Validity.* A certificate of registration, once issued, shall be valid only until the 8th day of March of the next following year: Provided, that the certificate may be revoked by the Commission at any time upon service of a Notice of Revocation to the PIC or PIP.

SECTION 14. *Verification.* The Commission may, at any time, verify any or all registration information provided by a PIC or PIP through on-site examination of its data processing systems. Policies and documents identified in the registration, including proof of certifications attained, shall be made available to the Commission upon request.

SECTION 15. *Amendments or Updates.* Amendments or updates to registration information, including significant changes in the description of registered data processing systems, shall be made within two (2) months from the date such changes take into effect. For this purpose, a significant change shall include:

A. Name and contact details of the PIC or PIP, head of agency or organization, and DPO;

B. A new or additional data processing system;

C. An amendment or update to the description of a registered data processing system, particularly:

1. Purpose or purposes of processing;
2. Description of the category or categories of data subjects, and of their personal data or categories thereof;
3. Recipients or categories of recipients to whom the personal data might be disclosed;

D. A new or additional automated decision-making process;

Amendments or updates to the registration information may be undertaken through the online registration platform, subject to the approval of the Commission: Provided, that where the change consists of the appointment or designation of a new DPO, the submission of the appropriate supporting document must be undertaken.

SECTION 16. *Non-Registration.* A PIC or PIP shall be considered as unregistered under the following circumstances:

A. Failure to register with the Commission;
B. Expiration and non-renewal of certificate of registration;

C. Rejection or disapproval of an application for registration, or an application for renewal of registration; or

D. Revocation of the certificate of registration.

SECTION 17. *Renewal.* A PIC or PIP may file an application for the renewal of its certificate of registration within two (2) months prior to, but not later than the 8th day of March every year. Any registration relative to which no application for renewal has been filed within the prescribed period is deemed revoked: Provided, that a PIC or PIP may be allowed to file an application for renewal beyond the prescribed period upon approval of the Commission, and only for good cause shown. For this purpose, the PIC or PIP shall notify the Commission of its intention to renew its registration and the reason for its delay.

SECTION 18. *Reasonable Fees.* To recover administrative costs, the Commission may require the payment of reasonable fees for registration, renewal, and other purposes in accordance with a schedule that shall be provided in a separate issuance.

RULE III.
REGISTRY OF DATA PROCESSING SYSTEMS

SECTION 19. *Maintenance of Registry.* The Commission shall maintain a registry of data processing systems in electronic format.

SECTION 20. *Public Access to Registry.* Any person may inspect the registry during regular office hours: Provided, that the Commission shall regulate such access to protect the legitimate interests of PICs and PIPs.

Subject to reasonable fees and regulations that may be prescribed by the Commission, any person may also secure a duly certified copy of any entry from the registry relating to a particular PIC or PIP.

SECTION 21. *Amendments to Registry.* Amendments or updates to the registry shall be made by the Commission every two (2) months, or as often as necessary, in order to incorporate changes to the registration information filed by PICs or PIPs.

SECTION 22. *Removal from Registry.* The registration information of a PIC or PIP may be removed by the Commission from the registry on any of the following grounds:

A. Incomplete registration;

B. Expiration and non-renewal of registration;

C. Revocation of certificate of registration; or

D. Expired and void registration.

SECTION 23. *Non-inclusion of Confidential Information.* Information classified by the Constitution or any statute as confidential shall not be included in the registry.

RULE IV.
NOTIFICATIONS REGARDING AUTOMATED DECISION-MAKING

SECTION 24. *Notification of Automated Decision-Making.* A PIC or PIC that carries out any automated decision-making operation shall notify the Commission via the mandatory registration process.

SECTION 25. *When to Notify.* Notifications regarding automated decision-making shall be included in the registration information that will be provided by a PIC or PIP, as indicated in Section 11 of this Circular, or through amendments or updates to such registration information, as per Section 15 of this Circular, within the prescribed periods.

SECTION 26. *Availability of Additional Information.* Upon request by the Commission, a PIC or PIP shall make available additional information and supporting documents pertaining to its automated decision-making operation, including:

1. Consent forms or manner of obtaining consent;
2. Retention period for the data collected and processed;
3. Methods and logic utilized for automated processing; and
4. Possible decisions relating to the data subject based on the processed data, particularly if they would significantly affect his or her rights and freedoms.

RULE V.
SANCTIONS AND PENALTIES

SECTION 27. *Revocation of Certificate of Registration.* The Commission may revoke the registration of a PIC or PIP on any of the following grounds:

A. Failure to comply with any of the provisions of the DPA, its IRR, or any relevant issuances of the Commission;

B. Failure to comply with any order, conditions, or restrictions imposed by the Commission;

C. Loss of authority to operate or conduct business, due to the revocation of its license, permit, franchise, or any other similar requirement provided by law;

D. Cessation of operations or of personal data processing;

E. Lack of capacity to process personal data in accordance with the DPA; or

F. Issuance by the Commission of a temporary or permanent ban on data processing against the PIC or PIP: Provided, that in the case of a temporary ban, such prohibition is still in effect at the time of filing of the application for renewal of registration:

Provided, that, prior to revocation, the Commission shall give the PIC or PIP an opportunity to explain why its certificate of registration should not be revoked.

SECTION 28. *Notice of Revocation.* Where the registration of a PIC or PIP is revoked, the Commission shall issue a Notice of Revocation of Registration, which shall be served upon the PIC or PIP.

SECTION 29. *Penalties and Fines.* A PIC or PIP whose certificate of registration has been revoked or that is determined to have violated the registration requirements provided in this Circular may, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent bans on the processing of personal data, or payment of fines in accordance with a schedule to be issued by the Commission. For this purpose, the registration requirements shall pertain to the provisions on mandatory registration, amendments and updates, and renewal of registration.

Under the voluntary registration system, failure to comply by a PIC or PIP with the requirements on amendments and renewal, shall render its certificate of registration void.

SECTION 30. *Cease and Desist Order.* When the Commission, upon notice and hearing, has determined that a PIC or PIP failed to disclose its automated decision-making operation through the appropriate notification processes set out in this Circular, it shall cause the service upon the PIC or PIP a Cease and Desist Order on the processing of personal data: Provided, that this is without prejudice to any other administrative, civil, or criminal penalties that the PIC or PIP may incur under the DPA and other applicable laws.

RULE VI.
MISCELLANEOUS PROVISIONS

SECTION 31. *Transitory Period.* Notwithstanding the deadline for registration provided in the IRR, all PICs and PIPs covered by this Circular shall complete Phase I of the registration process by 9 September 2017. Phase II of the registration may be completed until 8 March 2018.

SECTION 32. *Repealing Clause.* All other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 33. *Separability Clause.* If any portion or provision of this Circular is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 34. *Effectivity.* This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or two (2) newspapers of general circulation.

Approved:

(Sgd) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd) DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner

Appendix 1.

Re: Initial determination of the National Privacy Commission on sectors or institutions requiring Registration of Data Processing Systems under Sections 5(C) and 5(D) of NPC Circular 17-01 on the "Registration of Data Processing Systems and Notifications regarding automated decision-making."

The sectors or institutions provided herein that are processing personal data and operating in the country are subject to mandatory registration as provided in Sections 5(C) and 5(D) of NPC Circular 17-01. **ALL OTHER PICS OR PIPS SHOULD REGISTER IF IT EMPLOYS AT LEAST 250 PERSONS OR PROCESSING AT LEAST 1,000 RECORDS INVOLVING SENSITIVE PERSONAL INFORMATION.**

The National Privacy Commission determines, for the limited purpose of mandatory registration under NPC Circular 17-01, that the following sectors or institutions are considered PICs or PIPs involved in the processing of personal data that is likely to pose a risk to the rights and freedoms of data subjects and/or where the processing is not occasional:

1. Government ranches, bodies or entities, including national government agencies, bureaus or offices, constitutional commissions, local government units, government-owned and-controlled corporations.
2. Banks and non-bank, financial institutions, including pawnshops Non-stock Savings and Loan Associations (NSSLAS)
3. Telecommunications networks, internet service providers and other entities or organizations providing similar services
4. Business Processing Outsourcing companies
5. Universities, colleges and other institutions of higher learning, all other schools and training institutions
6. Hospitals including primary care facilities, multi-specialty clinics, custodial care facilities, diagnostic or therapeutic facilities, specialized out patient facilities, and other organizations processing genetic data
7. Providers of insurance undertakings, including life and non-life companies, pre-need companies and insurance brokers
8. Business involved mainly in direct marketing, networking, and companies providing reward cards and loyalty programs
9. Pharmaceutical companies engaged in research
10. Personal information processors processing personal data for a personal information controller included in the preceding items, and data processing systems involving automated decision-making.

SAMPLE FORM

Republic of the Philippines
National Privacy Commission
REGISTRATION OF DATA PROCESSING SYSTEM
DATA PROTECTION OFFICER – DPO

Note: The personal information submitted herein shall be used for the initial phase of the Data Processing System Online Registration and supporting documents should be attached along with this form. Once this form has been validated by the NPC, you will be given an access code via email and SMS to continue with your registration with the online system. You may find the list of supporting documents in our guidelines forwarded to you via email and posted in our website.

All the information submitted herein shall be used for the purpose stated above and other legitimate interest of NPC as mandated by law. Information that are matters of public interest may be disclosed to the public. Rest assured that security controls are implemented to protect all the information in this document.

PERSONAL INFORMATION CONTROLLER / PERSONAL INFORMATION PROCESSOR

NAME OF ORGANIZATION	
WEBSITE (URL)	EMAIL ADDRESS
COMPANY ADDRESS	CONTACT NO.

HEAD OF THE ORGANIZATION

LAST NAME	EMAIL ADDRESS
FIRST NAME	CONTACT NO.
MIDDLE INITIAL	
OFFICIAL DESIGNATION	

DATA PROTECTION OFFICER

LAST NAME	EMAIL ADDRESS
FIRST NAME	TEL. NO.
MIDDLE INITIAL	MOBILE. NO.
OFFICIAL DESIGNATION	DATE OF DESIGNATION AS DPO

SWORN STATEMENT

I declare under oath that this Registration Form is accomplished by Data Protection Officer, and is a true, correct and complete statement and pursuant to the provision of the pertinent laws, rules and regulations of the Republic of the Philippines. I also authorize the National Privacy Commission to verify/validate the contents stated herein.

_____ Head of Agency (Signature over Printed Name)

_____ Data Protection Officer (Signature over Printed Name)

SUBSCRIBE and SWORN to before me, this _____, who exhibited to me (his/her) Government Issued ID No. _____ issued at _____ on _____.

Notary Public

Doc. No. _____ ;
Page No. _____ ;
Book No. _____ ;
Series of _____ ;

*** TO BE FILLED UP BY NPC-COMPLIANCE AND MONITORING DIVISION ***	
NPC ACCESS CODE	**APPROVED BY (SIGNATURE OVER PRINTED NAME)**
DATE GIVEN (MM/DD/YYYY)	

ANNEX

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

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

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It 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. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *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.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

(e) *Filing system* refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

(f) *Information and Communications System* refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic

document.

(g) *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, or when put together with other information would directly and certainly identify an individual.

(h) *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.

(i) *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.

(j) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

(k) Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

(l) *Sensitive personal information* refers to personal information:

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

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such 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 cm-rent 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.

SEC. 4. *Scope.* – This Act 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 subject to the immediately succeeding paragraph: Provided, That the requirements of Section 5 are complied with.

This Act does not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) 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;

(c) 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;

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

(e) 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 this Act 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);

(f) 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.

SEC. 5. *Protection Afforded to Journalists and Their Sources.* – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act 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.

SEC. 6. *Extraterritorial Application.* – This Act 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.

CHAPTER II
THE NATIONAL PRIVACY COMMISSION

SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) 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: Provided, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers:Provided, That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: Provided, further,That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with

respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: Provided, finally. That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;

(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

SEC. 8. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made.

The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.

The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: Provided, That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

SEC. 10. *The Secretariat.* – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

CHAPTER III
PROCESSING OF PERSONAL INFORMATION

SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must, 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;

(b) Processed fairly and lawfully;

(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;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(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, That 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,That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing principles set out herein.

SEC. 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(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.

SEC. 13. *Sensitive Personal Information and Privileged Information.* -The processing of 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 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.

SEC. 14. *Subcontract of Personal Information.* – A personal information controller may subcontract the processing of personal information: Provided, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

SEC. 15. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, 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;

(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.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or 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 or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c) 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;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) 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; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 17. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 18. *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.

SEC. 19. *Non-Applicability.* – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

CHAPTER V
SECURITY OF PERSONAL INFORMATION

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. 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 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 (bat 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.

CHAPTER VI
ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 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.

CHAPTER VII
SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

SEC. 22. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall 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 to satisfy the minimum standards.

SEC. 23. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, 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.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 24. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

CHAPTER VIII
PENALTIES

SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 27. *Improper Disposal of Personal Information and Sensitive Personal Information.* – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

(b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

SEC. 29. *Unauthorized Access or Intentional Breach.* – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

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 (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed

on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

SEC. 31. *Malicious Disclosure.* – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If 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. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 35. *Large-Scale.* – The 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.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

CHAPTER IX
MISCELLANEOUS PROVISIONS

SEC. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

SEC. 39. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 40. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 41. *Appropriations Clause.* – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

SEC. 42. *Transitory Provision.* – Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.

In case that the DICT has not yet been created by the time the law takes full force and effect, the National Privacy Commission shall be attached to the Office of the President.

SEC. 43. *Separability Clause.* – If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

SEC. 44. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 45. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Approved,

(Sgd.) FELICIANO BELMONTE JR.
Speaker of the House of Representatives

(Sgd.) JUAN PONCE ENRILE
President of the Senate

This Act which is a consolidation of Senate Bill No. 2965 and House Bill No. 4115 was finally passed by the Senate and the House of Representatives on June 6, 2012.

(Sgd.) MARILYN B. BARUA-YAP
Secretary General
House of Representatives

(Sgd.) EMMA LIRIO-REYES
Secretary of the Senate

Approved: AUG 15 2012

(Sgd.) BENIGNO S. AQUINO III
President of the Philippines

A Guide for the Data Subject

1. Do you have a concern about a privacy violation, personal data breach or matters related to personal data protection, or any other violation the Data Privacy Act and other issuances of the National Privacy Commission?

    a. Yes. Proceed to the next section (No.2).
    b. No. The National Privacy Commission may have no power to act on your complaint. The Commission can only act on matters that relate to the Data Privacy Act.
    c. I am not sure. Request for an Advisory Opinion or request for information (No.5).

2. Does your concern affect you personally or involve your personal data?

    a. Yes. If it is a matter affecting your own personal data, you may file a Complaint with the National Privacy Commission.
    b. No. If it is about another person, or is a matter of general concern, request instead for an Advisory Opinion.

3. How do you file a complaint?

    a. First, give an opportunity to the individual or company to address your concerns. Send a written letter to the individual or company you believe has committed a privacy violation or personal data breach, and request the said company for appropriate action.
    b. If the company does not act on your letter within 15 days, or has failed to take appropriate action on your concern, you may file your complaint with the Commission. File the complaint within 30 days from last communication. If you have an important reason why you think it would be hard to write to the individual company, you may explain this to the Commission.
    c. The complaint should be in an affidavit form and should include:
        1. all information relevant to your concern, including any other evidence or affidavits of witnesses, if any;
        2. your communications with the individual or company;
        3. the relief you are demanding, whether you want specific action from the individual or company, or whether you want to claim for damages; and
        4. your contact details and contact details of the individual or company.
    d. You may file it with the office of the National Privacy Commission, where you may be asked to pay filing fees, depending on the relief you are asking. You may file it online through e-mail at complaints@privacy.gov.ph . In case of electronic mail, wait for instructions on how filing fees can be filed. If you qualify as an indigent, no filing fee is necessary.
    e. An investigating officer will evaluate your complaint and when sufficient in form and substance, the Commission may call on you to confer with the respondent on matters like discovery of evidence or schedules of the proceedings.
    f. Upon completion of the investigation, the investigating officer shall refer the case to the Office of the Commissioner for final decision.

4. How do you request for Advisory Opinion?

    a. File your request for advisory opinion in the same manner as a complaint.
    b. You request should include all facts necessary for the Commission to evaluate your concern and render an opinion.
    c. Provide the National Privacy Commission a way to contact you.
    d. Remember that if your request is for an advisory opinion, the National Privacy Commission will not award damages.

5. Can I get additional information on this circular?

    You may request for additional information on the procedure through info@privacy.gov.ph