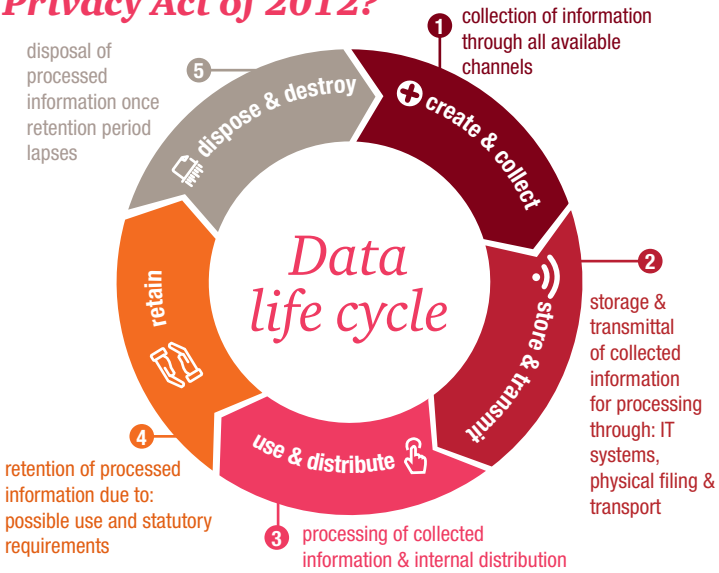
Journey towards DPA compliance

pwc

What is Data Privacy Act of 2012?

Data Privacy Act of 2012 (R.A. 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



Data privacy encompasses the rights of individuals and obligations of organizations with respect to the collection, storage, use, disclosure, retention, and disposal of personal data i.e. across the data life cycle.

Our point of view

Increased expectations

Regulation is evolving and more requirements are being placed on data custodians. If you get it wrong, there are real and serious legal consequences (such as criminal prosecutions, penalties and sanctions) and significant operational challenges (such as business disruption, financial loss and damage to brand and reputation).

Advancing threats

The threat landscape is becoming increasingly sophisticated. Understanding how the relevant threats affect your risk profile is key to protecting what matters most.

One size does not fit all

Every business has unique characteristics requiring a tailored approach to privacy. There is an effective way to approach privacy in any organization and we have developed it. Our approach is built around your special characteristics and uses our multidisciplinary team of privacy professionals to get you where you want to be, no matter what the problem or the solution is.

Privacy as BAU

Privacy should be considered in all business activities, with controls being designed into operations right at the beginning of every new activity. Our approach can help you to embed your privacy program within your organization by focusing on proven methods that ensure changes stick.

How we can help

- We can help demystify what data protection & privacy is, its implications and associated requirements by working with you to understand how it impacts your organization.
- Our unique multidisciplinary team of privacy professionals can help define a strategy for privacy investment and suggest approaches for the management of privacy, including roles and responsibilities, governance and reporting.
- We can use our experience to provide support in identifying what matters most to your organization, where it is and who has access to it.
- Present the threats that are most relevant to your sector and organization supported by a view of how vulnerable you are.
- Provide bespoke training to ensure employees and suppliers are properly engaged, trained and aware of their duties.
- Give you access to a global, multidisciplinary team that encompasses risk assurance, legal and forensics capabilities with cross sector expertise.
- Harmonize existing data protection measures in your business to align not only to the Data Privacy Act of 2012 (DPA) but also to the EU General Data Protection Regulation (GDPR) as necessary.

What's on your mind?

What does privacy mean to you?
You need to better understand the importance of privacy within your organization and how it fits within your overall business strategy.

Are you maximizing the potential of personal data in a legally compliant way?
You want to balance your need to gain a good return on your personal data assets with your need to be compliant with your legal duties and your desire to build and maintain customer trust.

What data is held?
You are not sure what personal data is held and the purposes for which it is being used. Therefore you are unable to ensure that all personal data is being properly protected and used in a legally compliant way.

Where is the data?
Personal data is distributed across the organization, often sitting within numerous divisions and technologies, and as a consequence there are significant challenges in controlling its utilization.

Who has access?
You are unable to determine who has authorized access (including third parties) to personal data versus those who may have accidentally or intentionally elevated their privileges resulting in a breach or loss.

How vulnerable are you and your data?
You are unclear of the internal and external threats to the security of your data and looking for assurance that appropriate controls are in place to ensure compliance with all relevant regulation and standards. In addition, you are not confident that you are well prepared to respond to a breach and you are looking to test your capability.

Where do I begin, to make sense of it all? Where am I today? Where do I need to get to? How do I get there?
You know that you need to have a strategy for handling personal data and for achieving legal compliance, but you do not know where to begin, or how to justify your choices.

We can help.

Our approach

The Five Commandments has been set by the NPC as the baseline for DPA compliance. Collectively, these are used as reference by organizations in crafting their "compliance journey". Having been at the forefront of the conversations with the NPC on DPA compliance, we are able to have a good grasp of the regulator's perspective on what compliance would look like and the specific areas that they will look into when they conduct their compliance monitoring. We have mapped our approach to address each commandments as follows:

The Five Commandments of the National Privacy Commission	Activities where we can assist
1 Commit to comply: Appoint **a Data Protection Officer (DPO)**	Data Protection Officer (DPO) • Data Privacy Charter • Baseline calendar of DPO office
2 Know your risk: Conduct a **Privacy Impact Assessment (PIA)**	Personal data inventory • Data flow narratives (data life cycle) • Privacy Impact Assessment report • Foundational roadmap for remediation
3 Write your plan: Create your **Privacy Management Program (PMP)**	Data Privacy manual
4 Be accountable: Implement your **privacy and data protection (PDP) measures**	Implement Rule VI of Implementing Rules and Regulations - Security Measures for Protection of Personal Data
5 Be prepared for breach: Regularly exercise your **Breach Reporting Procedures (BRP)**	Personal data breach management plan

How PwC can help

For a deeper discussion on data privacy, contact our team:

Geraldine H. Apostol, CPA
Risk Assurance Leader
(+632) 459 3040
geraldine.h.apostol@ph.pwc.com

Maria Rosell S. Gomez, CPA, CISA, CRISC, CRM, CCOBIT 5(F), CCOBIT 5(I)
Risk Assurance Partner
(+632) 459 3184
rosell.s.gomez@ph.pwc.com

Atty. Harold S. Ocampo
Tax Principal
(+632) 459 2029
harold.s.ocampo@ph.pwc.com

Ray Jan P. Roque, CPA, CISA (Passer), CCOBIT 5(F), CCOBIT 5(I)
Risk Assurance Director
(+632) 845 2728 ext. 3194
ray.jan.p.roque@ph.pwc.com

Cecile Marie D. de Leon, CPA
Risk Assurance Director
(+632) 845 2728 ext. 3331
cecile.marie.de.leon@ph.pwc.com

Salvador C. Guarino, CPA, CIA, CISA, CISSP, CEH, LPT, CPTE CompTIA Security+ CE, CompTIA Network
Risk Assurance Senior Manager
(+632) 845-2728 ext. 3096
salvador.c.guarino.jr@ph.pwc.com

Jannick S. Reyes, CPA, CISA, CRISC
Risk Assurance Manager
(+632) 845 2728 ext. 3095
jannick.s.reyes@ph.pwc.com

Atty. Maria Ysidra May Y. Kintanar-Lopez
Tax Manager
(+632) 845 2728 ext. 2034
may.y.kintanar@ph.pwc.com