EBOOK

Addressing the Data Privacy Act of 2012 (Republic Act 10173)

What is it?
Why was it created?
How can organisations prepare for it?
What is it?

The Republic Act No. 10173 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’

Under CHAPTER 1, GENERAL PROVISION, SECTION 1. Short Title. – This Act shall be known as the “Data Privacy Act of 2012”.

The National Privacy Commission (NPC) is set up to ‘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.’

A compliance check by the NPC means an organization will be subjected to a comprehensive compliance validation process based on 10 critical aspects of accountability, which the NPC has termed as the Data Governance Framework. The compliance check involves interviews, operations inspection, documents analysis, and pertinent activities intended to appraise the organization’s culture of privacy.

On September 9, 2016, the final implementing rules and regulations (IIR) came into force, adding specificity to the Privacy Act. Organizations were given one year to prepare for the IIR deadline.

A scanned copy of the document given out at the DPO assembly, organized by NPC.
What does the Implementation of Rules and Regulation (IIR) deadline on 09 September 2017 mean?

Section 47 of the IRR of the Data Privacy Act of 2012 requires personal information controllers (PIC) or personal information processors (PIP) that employs 250 persons or more to register their information processing system with the NPC. Those that employ fewer than 250 persons are also required to register if their operations involve the processing of personal data that may likely pose a risk to the rights and freedoms of data subjects; the processing is not occasional; or the processing includes sensitive personal information of at least one thousand (1,000) individuals\textsuperscript{1}.
Public and private companies that failed to beat the September 9 deadline for the registration of their data processing systems starting with the registration of their Data Protection Officer (DPO) could face compliance checks, the National Privacy Commission (NPC) warned.

In an effort to give organizations ample time to comply, the commission has earlier divided the registration process into two phases and extended the deadline for the more rigorous second phase to March 8, 2018. The first phase, however, which essentially consists of a DPO registration, is not subject to an extension.

**Duties of the DPO**

Sec. 21 (b) The personal information controller (PICs) shall designate an individual or individuals who are accountable for the organization’s compliance with this Act. The first essential step towards compliance is appointing a Data Protection Officer (DPO). Organisations are unable to register their system, or report compliance activities, with the NPC.

[Source: https://privacy.gov.phnpc-late-registrants-may-face-privacy-compliance-checks/]
Appoint a DPO (Data Protection Officer)
Legal Basis: Sec.21, IRR 50, Circ. 16-01, Advisory 17-01

What compliance looks like
- Notarized appointment or designation of a DPO, filed with the NPC
- Evidence of actions taken on basis of DPO recommendations
- Contact details on website (if any)
- Continuing education program

What negligence looks like
- No DPO
- Lack of interaction between DPO and top management, between DPO and functional units
- Inaction on complaints from data subjects
- Non-reporting to NPC

Data Processing adheres to Transparency, Legitimate Purpose, and Proportionality
Legal Basis: Sec. 11-15, IRR 21-23 and 43-45, Circ. 16-01 and 16-02

What compliance looks like
- Privacy policies cascaded throughout the organization and updated as needed
- Data handlers have security clearance and privacy training
- Privacy notice where appropriate, e.g. on website
- Data sharing agreements in place
- Privacy impact assessments conducted and up-to-date
- Service providers in compliance

What negligence looks like
- Privacy policy sits on shelf
- No security clearance or privacy training for data handlers
- No privacy notice when collecting personal data
- Overcollection
- Data sharing without agreements
- No privacy impact assessments
- No compliance obligations for service providers
Maintain Confidentiality, Integrity, Availability
Legal Basis: Sec.20.a-e, Sec. 22 and 24, IRR 25-29, Circ. 16-01

What compliance looks like
- Data protection risks identified, and the appropriate up-to-date controls are in place to manage these risks
- Data protection policies cascaded throughout the organization and updated as needed
- Frequent monitoring and vulnerability scanning
- Regular security and business continuity drills are conducted
- Service providers are in compliance

What negligence looks like
- Generic controls in place
- Controls not updated for new risks/threats
- Controls are not complied with
- Lax cyber-hygiene practices
- No compliance obligations for service providers
- No periodic drills for monitoring
- No venue for data subjects to access or correct/rectify their own data
In today’s environment where competitors can copy your products, pirate your employees, and mirror your algorithms, data is the only sustainable competitive advantage.

Damian Mapa, Deputy Privacy Commissioner
What happens when a breach happens in an organisation?

The law defines “security incident” and “personal data breach” ensuring that the two are not confused. A “security incident” is an event or occurrence that affects or tends to affect data protection, or may compromise availability, integrity or confidentiality. This definition includes incidents that would result in a personal breach, if not for safeguards that have been put in place.

A “personal data breach,” on the other hand, is a subset of a security breach that actually leads to “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed”.

The law further provides that not all “personal data breaches” require notification, which provides several basis for not notifying data subjects or the data protection authority. Section 38 of the IRR provides the requirements of breach notification:

1. The breached information must be sensitive personal information, or information that could be used for identity fraud, and

2. There is a reasonable belief that unauthorized acquisition has occurred, and

3. The risk to the data subject is real, and

4. The potential harm is serious.
Report Breach within 72 hours
Legal Basis: Sec. 20.f and 30, IRR 38-42 and 57, Circ. 16-03

IRR Sec. 38 (a) The Commission and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred

What compliance looks like
- Formation of a data breach response team with clearly defined roles and responsibilities
- Clearly defined and up-to-date incident response procedure that covers assessment, mitigation, notification and recovery actions
- Regular breach drills are conducted
- Service providers in compliance

What negligence looks like
- No response team or procedures
- No drills
- No compliance obligations for service providers
- No post-breach reports
- No notification within 72 hours (an act punishable by 18 months to 5 years of imprisonment and a fine of 500,000 to 1,000,000 pesos)
What are the penalties for failing to comply with the Data Privacy Act of 2012?

<table>
<thead>
<tr>
<th>Punishable Act</th>
<th>Jail Terms</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access due to negligence</td>
<td>1y to 3y - 3 to 6y</td>
<td>500k to 4m</td>
</tr>
<tr>
<td>Unauthorized processing</td>
<td>1y to 3y - 3 to 6y</td>
<td>500k to 4m</td>
</tr>
<tr>
<td>Improper disposal</td>
<td>6m to 2y - 3y to 6y</td>
<td>100k to 1m</td>
</tr>
<tr>
<td>Unauthorized purposes</td>
<td>18m to 5y - 2y to 7y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Intentional breach</td>
<td>1y to 3y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Concealing breach</td>
<td>18m to 5y</td>
<td>500k to 1m</td>
</tr>
<tr>
<td>Malicious disclosure</td>
<td>18m to 5y</td>
<td>500k to 1m</td>
</tr>
<tr>
<td>Unauthorized disclosure</td>
<td>1y to 3y - 3y to 5y</td>
<td>500k to 2m</td>
</tr>
<tr>
<td>Combination of acts</td>
<td>3y to 6y</td>
<td>1m to 5m</td>
</tr>
</tbody>
</table>
Key Steps for Addressing Data Privacy Compliance (Data Privacy Act 2012)?

1. Identify Where Sensitive Data Resides
   A critical first step will be establishing a complete, accurate picture of where sensitive personal data resides.
   > For each system or service, who has access to data? How will access and other activities be tracked and assigned to specific individuals?

   > How many different locations and environments does the data reside in? This includes detailing geographic locations as well as locations within a data center or extended data center (including virtual and cloud environments), and whether data resides on servers (whether file servers, databases, or virtual machines), storage volumes or shares, or disk drives, tapes, or other media.

   > How many different data types need to be secured? Are sensitive data elements solely housed in structured data formats, for example as fields in a database, or are they housed in unstructured files like PDFs, images, or word processing documents?

   > Where does data get transmitted? This can include data traversing networks between data centers, whether in point-to-point or multi-point environments.
2. Minimise the Number of Data Repositories Where Possible
Once data locations are identified and understood, it’s important to take steps to minimise the number of locations housing sensitive data wherever possible. Particularly with respect to Data Privacy Act 2012, if a business could reduce the number of environments or systems that contain personal data, they could potentially significantly streamline their compliance efforts.

3. Safeguard Data Leveraging Encryption and Key Management
Encryption represents an essential way to establish data confidentiality and integrity. In fact, the Data Privacy Act 2012 will only intensify the demand for encryption.

> Encryption offers the possibility of obviating the need for breach notification, as required by the Data Privacy Act 2012 unless proper technological protection measures are implemented. If a breach occurs but data was encrypted and keys were protected, a cyber attacker would be unable to decrypt the data and access the actual information.

> Organisations can ensure that, even if another government issues a subpoena or is secretly accessing a private repository, an organisation can retain control over who can ultimately decrypt the data.

> By deleting a key associated with a consumer’s encrypted records, a business could ensure that data will never be accessed in the clear.

4. Control Access
Repeatedly, it is weak, static credentials that are exploited to gain unauthorised access to sensitive resources or perpetuate a full-blown data breach. It is therefore essential for organisations to eliminate this vulnerability by establishing strong, multi-factor authentication to any resource that holds value, be it a network, portal, or application.
Protect What Matters, Where it Matters

> **Encryption.** Gemalto data-at-rest encryption solutions deliver transparent, efficient data protection at all levels of the enterprise data stack, including the application, database (column or file), file system, full disk (virtual machine), and network-attached storage levels. In addition, SafeNet High Speed Encryptors deliver proven and certified Layer 2 encryption capabilities that secure data in transit, while addressing business requirements for real-time response and high throughput.

> **Key management.** With Gemalto solutions, organisations can centrally, efficiently, and securely manage and store cryptographic keys and policies—across the key management lifecycle. These solutions can manage keys across heterogeneous encryption platforms, offering support for the KMIP standard as well as proprietary interfaces. Gemalto offers enterprise key management solutions as well as a range of hardware security modules (HSMs).

> **Identity and access management (IAM).** Gemalto’s portfolio of IAM solutions feature market-leading strong authentication and digital signing products. These offerings enable organisations to secure access to online resources and protect the digital interactions of employees, partners, and customers.

For more information on complying with the ‘Data Privacy Act 2012’, please contact our Security Consultants at InfoAPAC@gemalto.com
Look for an experienced vendor who can offer you a complete solution.

Gemalto delivers the breadth of solutions that enable global enterprises to effectively address their evolving business, security, and privacy objectives. With Gemalto solutions, security teams can centrally employ defence-in-depth strategies that deliver holistic, persistent security.

5. https://twitter.com/inquirer_libre/status/839337443140616192
ABOUT GEMALTO’S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilising innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organisations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.