# Working Towards Data Privacy Resilience in Government

NATIONAL PRIVACY COMMISSION

MARCH 14, 2018



NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

# Philippine Development Plan 2040

AMBISYON NATIN 2040


http://2040.neda.gov.ph/wp-content/uploads/2016/04/A-Long-Term-Vision-for-the-Philippines.pdf

NATIONAL PRIVACY COMMISSION

*By 2040*, the Philippines is a prosperous middle class society where no one is poor. People live long and healthy lives and are smart and innovative.

The country is a high-trust society where families thrive in vibrant, culturally diverse, and resilient communities.

AMBISYON NATIN 2040



NATIONAL PRIVACY COMMISSION

http://2040.neda.gov.ph/wp-content/uploads/2016/04/A-Long-Term-Vision-for-the-Philippines.pdf

REUTERS

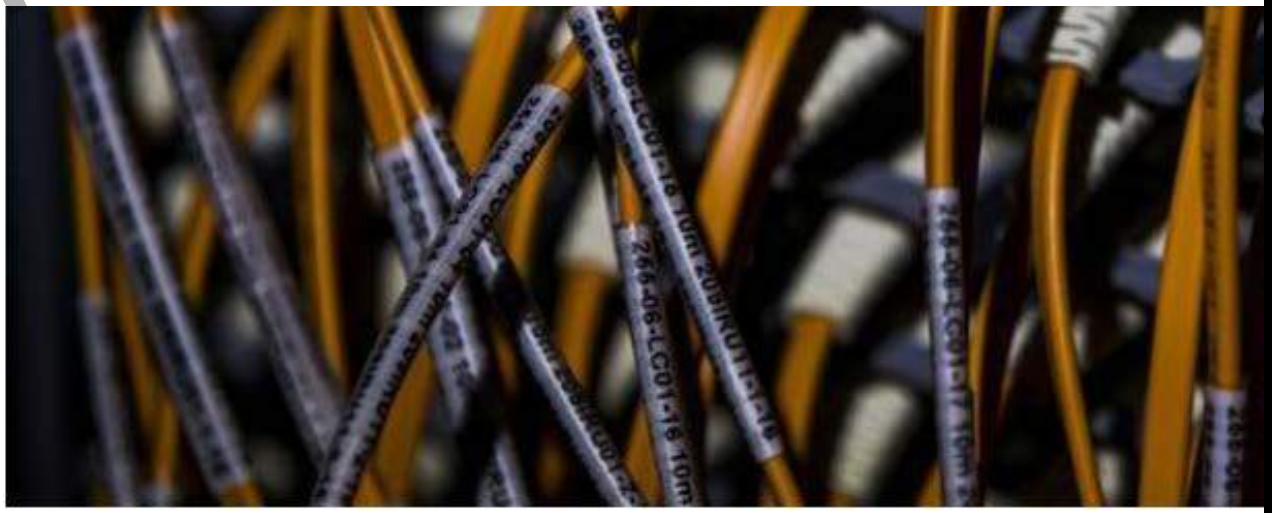
Myanmar | CERAWeek

CYBER RISK

FEBRUARY 14, 2018 / 8:11 PM / 22 DAYS AGO

# Rise of the data protection officer, the hottest tech ticket in town

More than 28,000 will be needed in Europe and U.S. and as many as 75,000 around the globe as a result of GDPR, the International Association of Privacy Professionals (IAPP) estimates. The organization said it did not previously track DPO figures because, prior to GDPR, Germany and the Philippines were the only countries it was aware of with mandatory DPO laws.



FILE PHOTO - A picture shows wires at the back of a super computer at the Konrad-Zuse Centre for applied mathematics and computer science, in Berlin August 13, 2013. REUTERS/Thomas Peter


DP01


DP05


DP09


DP02


DP012


DP03


DP07


DP011


DP04


DP08


DP015


The Data Privacy Act makes it mandatory for all data collectors — whether public or private — to protect the security, integrity and confidentiality of all the personal information they collect. **By doing this, we help usher in a truly knowledge-driven economy.**

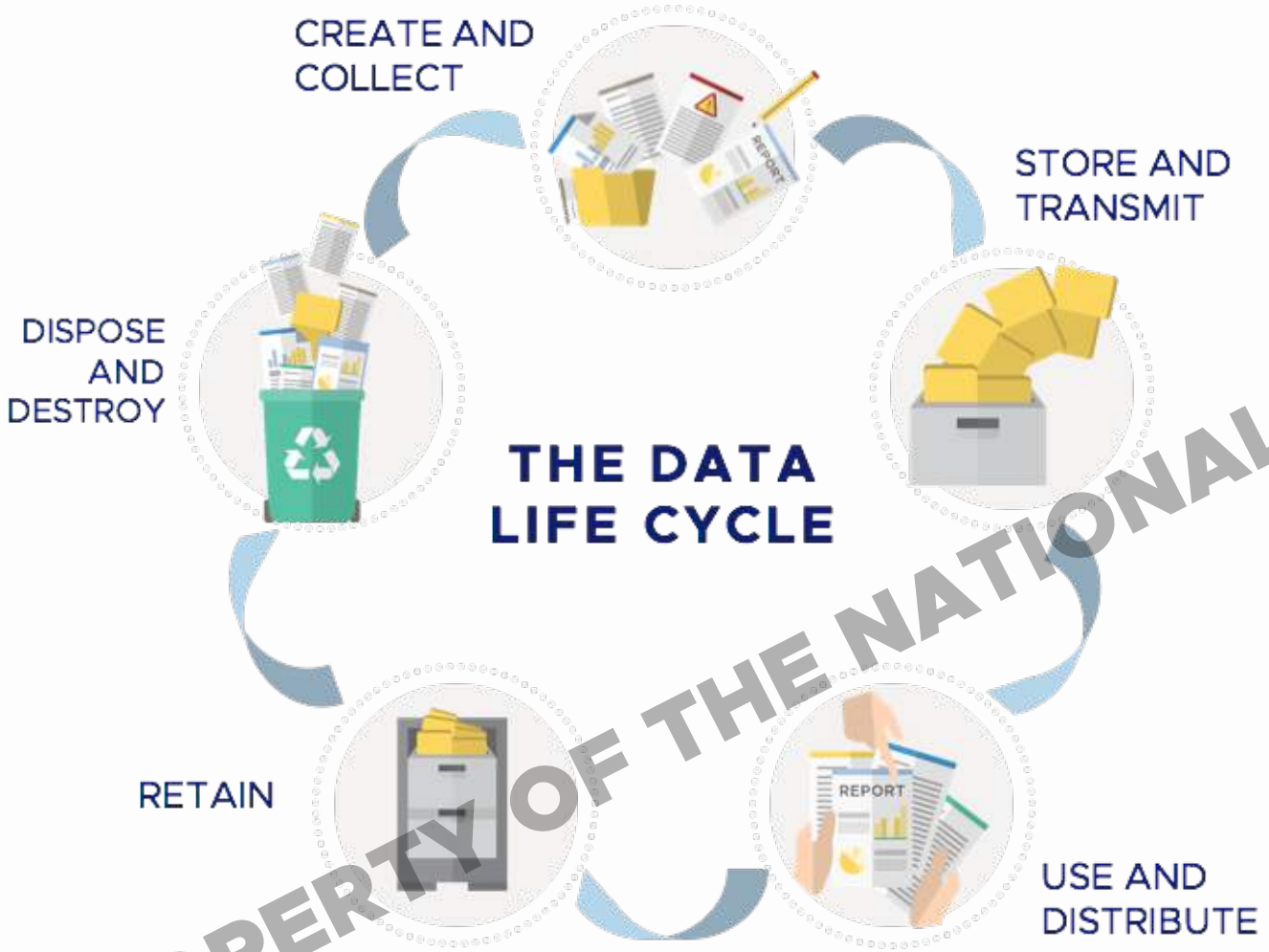
SENATOR EDGARDO ANGARA



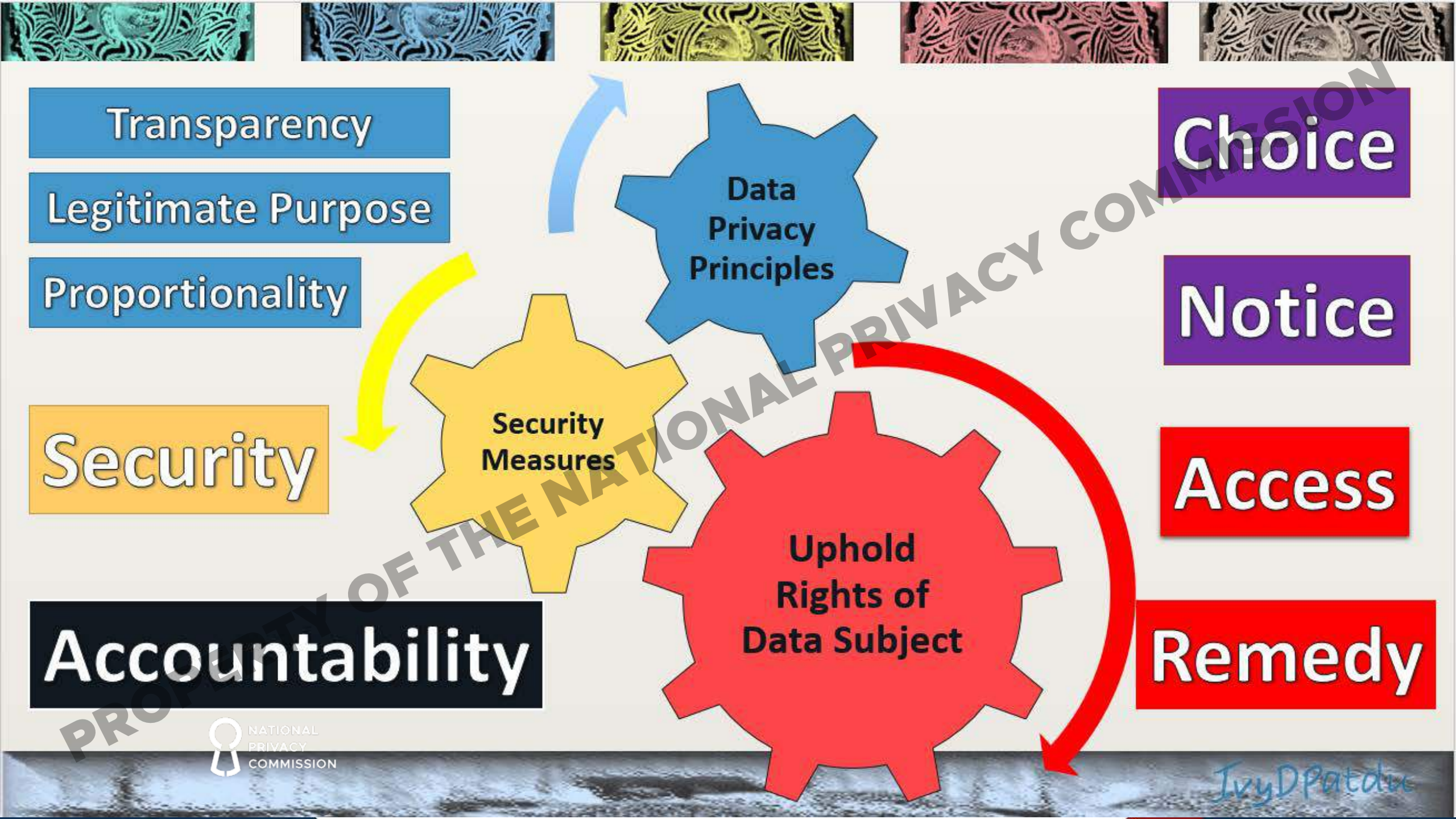
NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

# General Overview for Privacy Resilience in Government




- **Consider and protect an individual's privacy throughout the information lifecycle**
- **Develop and Implement an agency-wide privacy program that includes people, processes, and technologies**
- **Ensure compliance with applicable privacy requirements**
- **Evaluate policies that impact privacy and manage privacy risks**



# Event Program

| | |
|---|---|
| 08:00 - 08:20 | Registration |
| 08:20 - 08:30 | Preliminaries |
| 08:30 - 09:00 | Welcome Remarks |
| 09:00 - 09:30 | Complying with NPC Circular 16-01: Security of Personal Data in Government Agencies |
| 09:30 - 10:00 | Complying with NPC Circular 1 6-02: Data Sharing Agreements involving Government Agencies |
| 10:00 - 10:30 | Data Privacy and Freedom of Information: Guidance for Government |

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

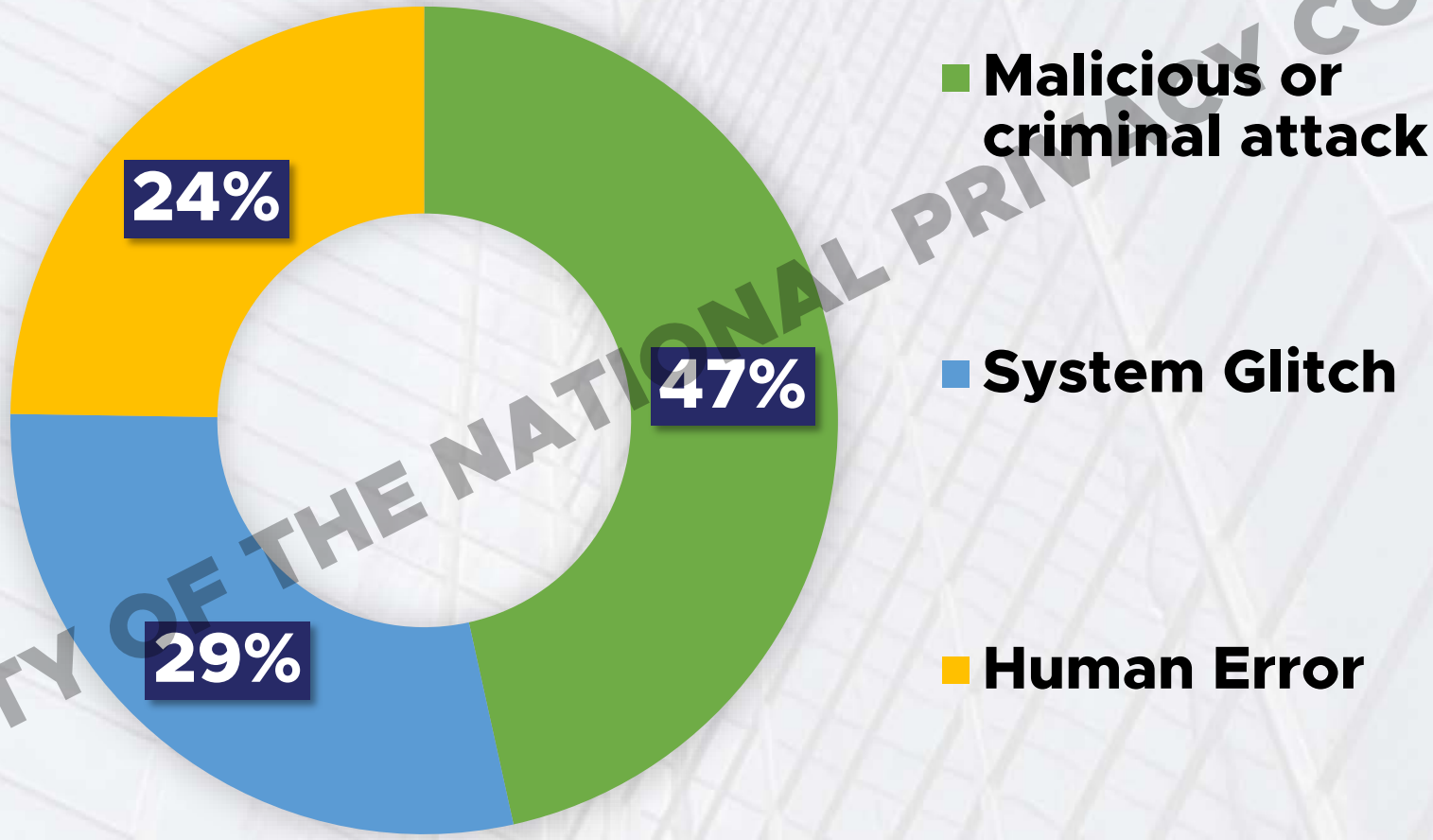
# Event Program

| | |
|---|---|
| 10:30 - 11:30 | Privacy Impact Assessment |
| 11:30 - 12:30 | Privacy Management Program |
| 12:30 - 13:30 | Lunch and Commemorative Photo |
| 13:30 - 14:00 | Lessons in DPA Compliance |
| 14:00 - 14:20 | Building a Community if Government DPOs |
| 14:20 - 15:15 | Break |
| 15:15 - 15:30 | Q&A |
| 15:30 - 16:45 | Closing |

NATIONAL PRIVACY COMMISSION

GOVERNMENT DPO CONFERENCE 2018

# ROOT CAUSES OF BREACH






NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

Ponemon Institute LLC, *2015 Cost of Data Breach Study: Global Analysis*, May 2015, p.10.

# HOW DO PRIVACY BREACHES OCCUR?

- **lost or stolen laptops**, removable storage devices, or paper records containing personal information
- **hard disk drives and other digital storage** media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- **databases containing personal information** being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organization





Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches,* August 2014, p. 5.

# HOW DO PRIVACY BREACHES OCCUR?

- **employees accessing** or disclosing personal information outside the requirements or authorization of their employment
- **paper records stolen** from insecure recycling or garbage bins
- an agency or organization **mistakenly providing personal information** to the wrong person, for example by sending details out to the wrong address, and
- an **individual deceiving an agency** or organization into improperly releasing the personal information of another person.





Office of the Australian Information Commissioner, *Data breach notification guide: A guide to handling personal information security breaches,* August 2014, p. 5.

# HOW DO PRIVACY BREACHES OCCUR

## Most government data breaches caused by employees, says Verizon study

Fri, 2014-04-25 01:48 AM

Fri, 2014-04-25 01:48 AM

About 58 percent of cyber security incidents in the public sector were caused by employees, according to this year's annual Verizon Data Breach Investigations Report. About 34 percent were caused by employee accidents in handling data and about 24 percent by unapproved or malicious data use.

Data handling errors could include emailing documents to the wrong person or forgetting to redact certain parts of a document, for example. They could also include mailing personal information to the wrong person through traditional mail, or not disposing of hard drives properly or shredding sensitive documents, the report says.

One reason employee misuse of data is particularly high compared to the other sectors reviewed in the report could be the public sector's heavy data breach reporting requirements, Kevin Thompson, Verizon senior analyst and report co-author, told *Government Security News*.

## Common Internal Errors:

- -Emails to the wrong people
- -Forgetting to redact details
- -Failure to properly dispose



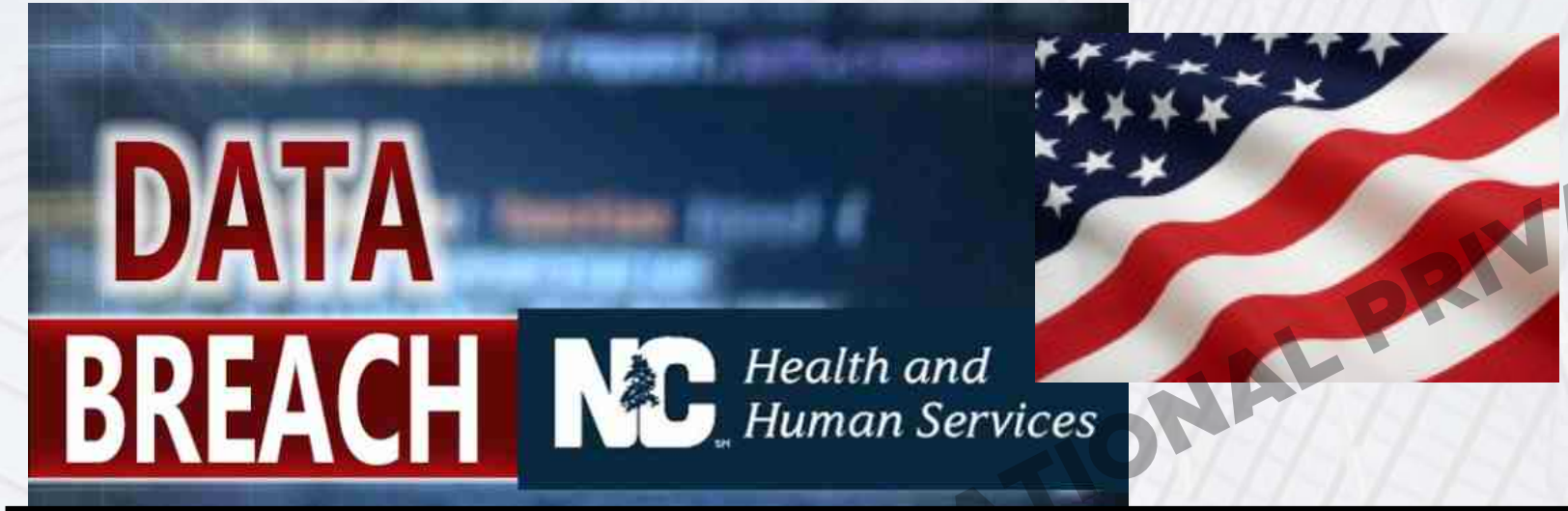
NATIONAL PRIVACY COMMISSION

http://www.fiercegovernment.com/article/41007/most_government_data_breaches_caused_employees_say

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

# HOW DO PRIVACY BREACHES OCCUR




Employees accessing or disclosing personal information **outside the requirements or authorization** of their employment

**RALEIGH, N.C. (AP)** - A North Carolina agency says a spreadsheet containing personal information for nearly 6,000 people was sent in error to a vendor in an unencrypted email.

The spreadsheet includes names, social security numbers and test results for people who underwent routine drug screenings for employment, intern and volunteer opportunities. Inclusion in the spreadsheet reflects only that people sought an employment, intern or volunteer opportunity at DHHS within the affected period.

# HOW DO PRIVACY BREACHES OCCUR

Databases containing personal information being '**hacked**' into or otherwise illegally accessed by individuals outside of the agency or organization

NATIONAL / CRIME & LEGAL

**1.25 million affected by Japan Pension Service hack**

BY TOMOKO OTAKE
STAFF WRITER

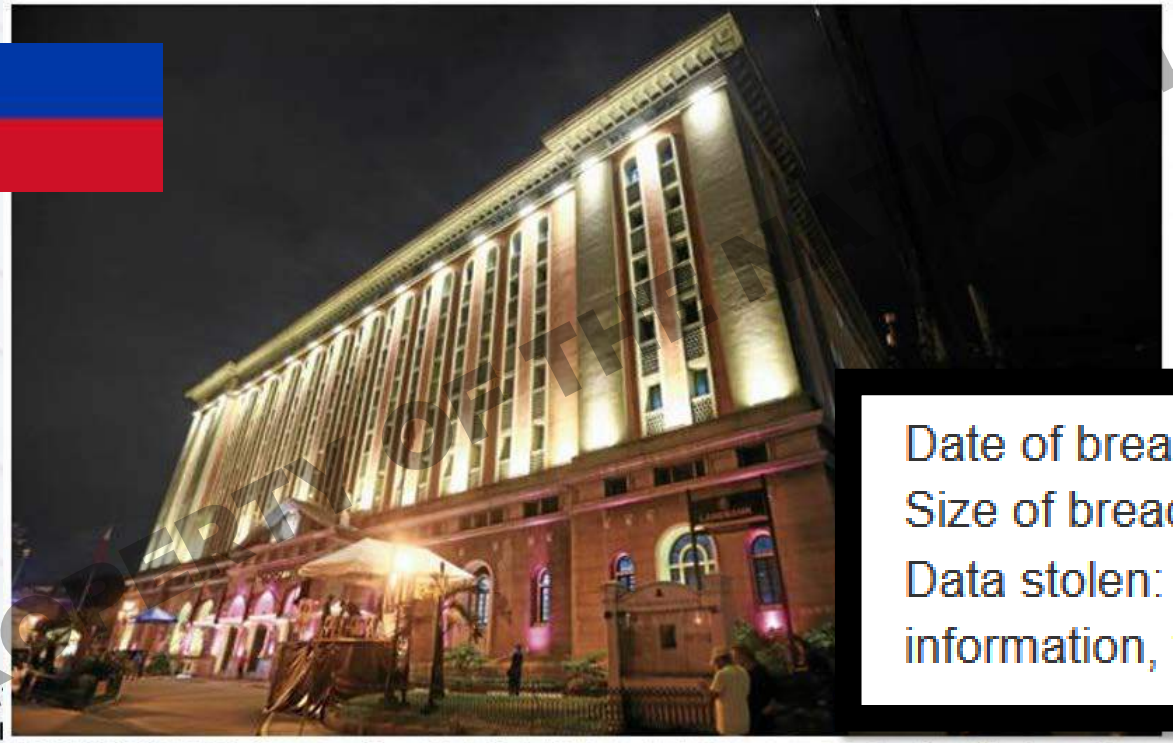
Date of discovery: May 2015
Size of breach: 1.25 million
Data stolen: Pension IDs, names, birth dates and addresses

# HOW DO PRIVACY BREACHES OCCUR

SECTIONS Tuesday, January 3, 2017 INQUIRER.NET

## 55M at risk in 'Comeleak'

By: Tina G. Santos - Reporter / @santostinaINQ Philippine Daily Inquirer / 12:44 AM April 23, 2016



DECEPTIVE CALM The Comelec office at Palacio del Gobernador in Intramuros,Manila, after office hours. The Comelec says the hacking of its website will not compromise the integrity of national elections on May 9. EDWIN BACASMAS

Databases containing personal information being '**hacked**' into or otherwise illegally accessed by individuals outside of the agency or organization

Date of breach: March 2016
Size of breach: 55 million
Data stolen: Personal information, passport information, fingerprint data

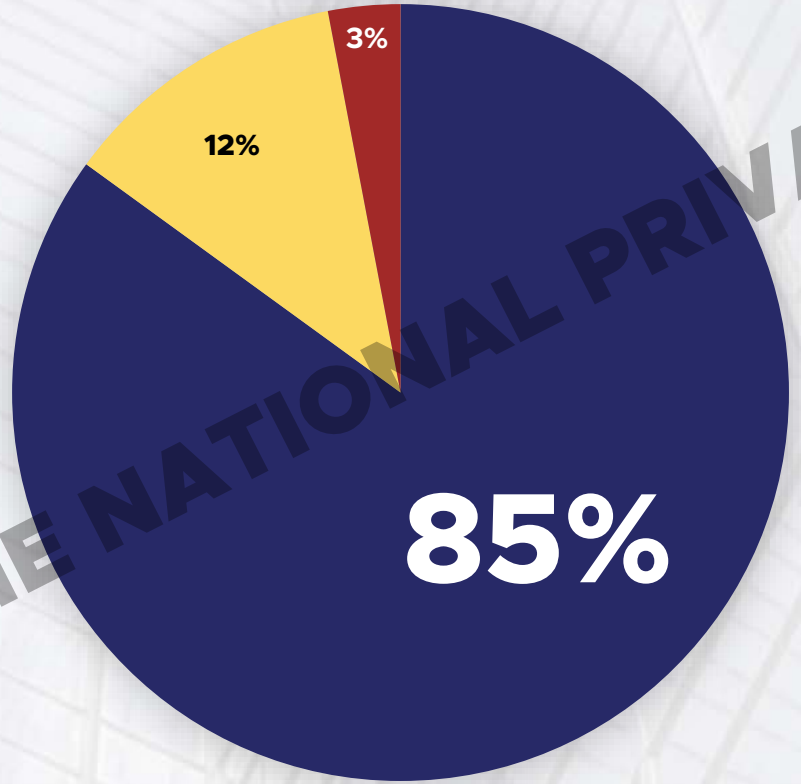
https://www.enterpriseinnovation.net/article/worst-government-data-breaches-2015-2016-1273457573

# PROCESSING PERSONAL INFORMATION CAN CREATE PROBLEMS FOR INDIVIDUALS

- Loss of trust
- Loss of self-determination
  - *Loss of autonomy*
  - *Loss of liberty*
  - *Exclusion*
  - *Physical harm*
- Discrimination
  - *Stigmatization*
  - *Power imbalance*
- Economic loss

# Survey Results

## Importance of The Rights of A Data Subject, Philippines, June 2017




*Net figure % Likes to know minus % Does Not like to Know, correctly rounded

**Net***
**+83**

*% of Adults*

***Based on the SWS Survey "FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE"June 17-21, 2017 National Survey**



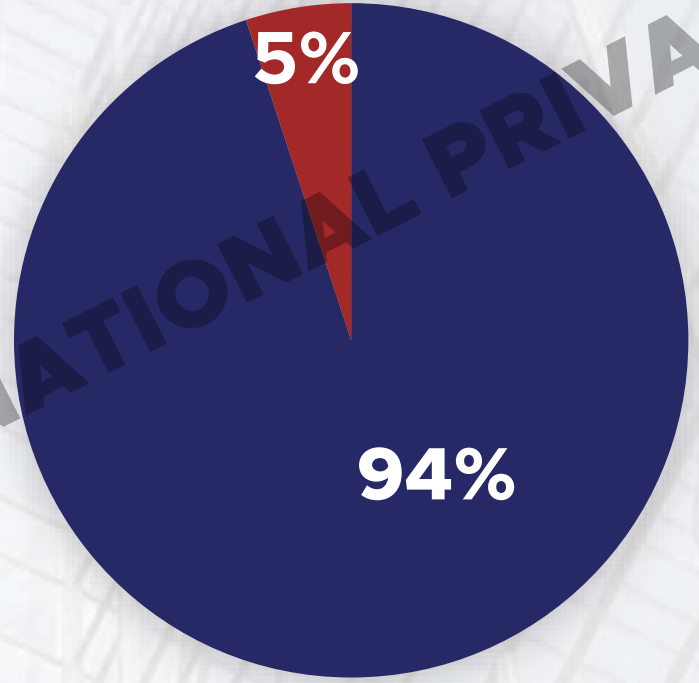
NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

# Survey Results

## Extent of Liking or Not Liking to Know Where The Personal Information They Have Provided During Transaction or Application Will Be Used, Philippines, June 2017




*Note: No answer/Don't know/Refused responses are not shown.*
**Net figure % Likes to know minus % Does Not like to Know, correctly rounded*

***% of Adults***

***Net****
***+89***

****Based on the SWS Survey "FILIPINO PUBLIC OPINION ON DATA PRIVACY AND ATTITUDES AND BEHAVIOUR TOWARDS INTERNET USAGE"***
***June 17-21, 2017 National Survey***

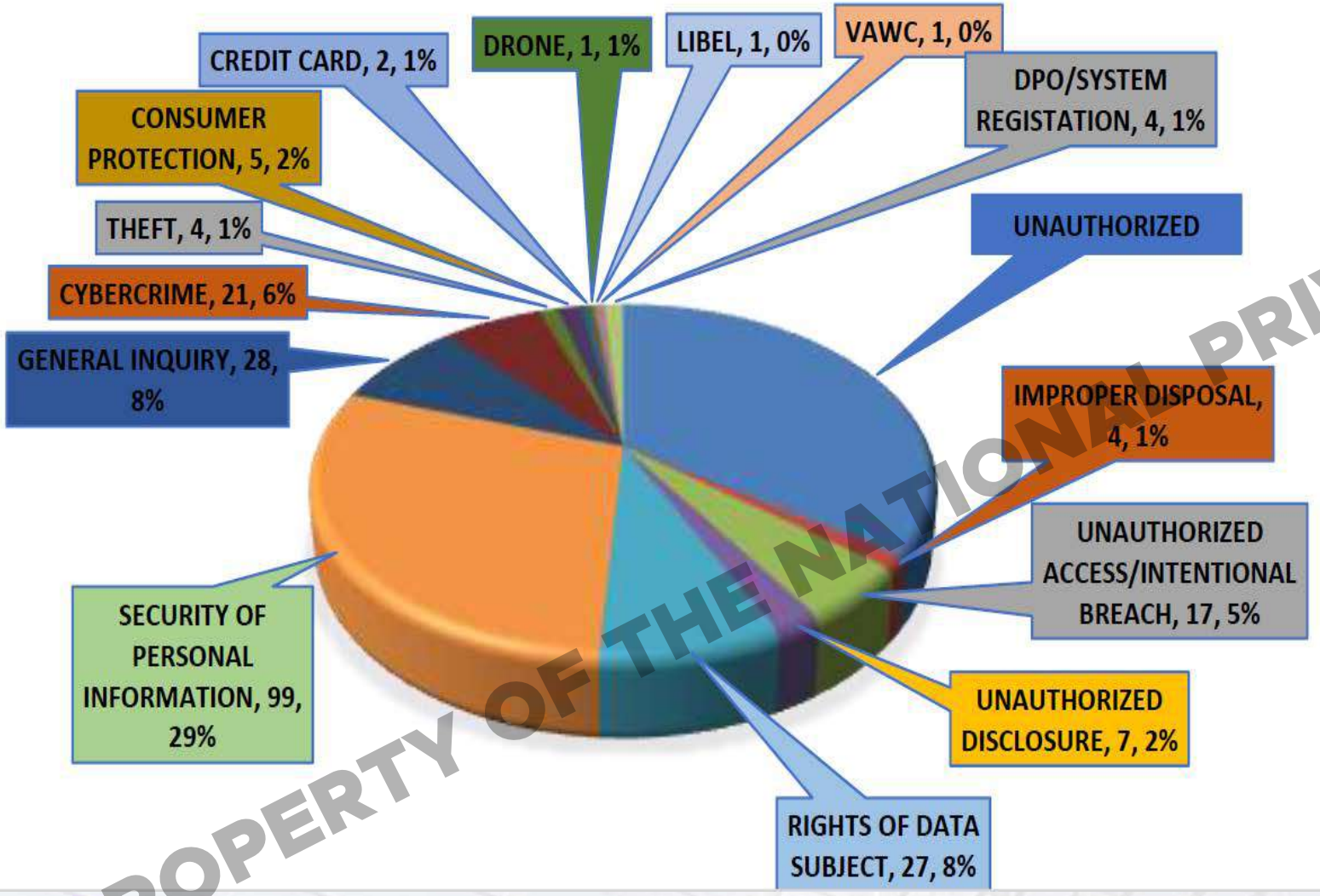


NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

# Nature of Complaints (as of February 28, 2018)




| CLASSIFICATION | NO. OF COMPLAINTS | PERCENTAGE |
|---|---|---|
| UNAUTHORIZED PROCESSING | 118 | 34.81% |
| IMPROPER DISPOSAL | 4 | 1.18% |
| UNAUTHORIZED ACCESS/INTENTIONAL BREACH | 17 | 5.01% |
| UNAUTHORIZED DISCLOSURE | 7 | 2.06% |
| RIGHTS OF DATA SUBJECT | 27 | 7.96% |
| SECURITY OF PERSONAL INFORMATION | 99 | 29.20% |
| GENERAL INQUIRY | 28 | 8.26% |
| CYBERCRIME | 21 | 6.19% |
| THEFT | 4 | 1.18% |
| CONSUMER PROTECTION | 5 | 1.47% |
| CREDIT CARD | 2 | 0.59% |
| DRONE | 1 | 0.29% |
| LIBEL | 1 | 0.29% |
| VAWC | 1 | 0.29% |
| DPO/SYSTEM REGISTATION | 4 | 1.18% |
| TOTAL | 339 | 100.00% |

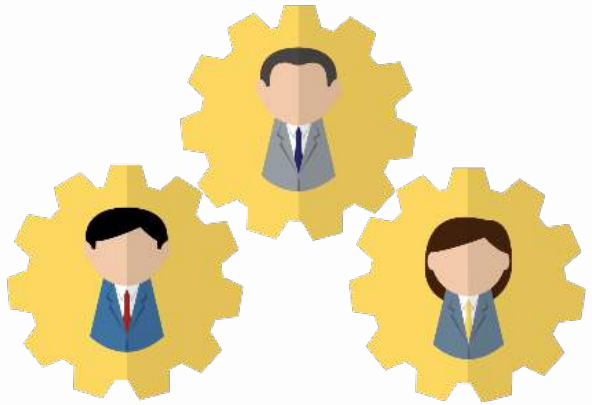
# PERSONAL INFORMATION CONTROLLER

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.

It excludes:

- A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- A natural person who processes personal data in connection with his or her personal, family, or household affairs;

# PERSONAL INFORMATION PROCESSOR



Refers to any natural or juridical person or any other body to whom a personal information controller may **outsource or instruct the processing of personal data** pertaining to a data subject.

# STRUCTURE OF RA 10173

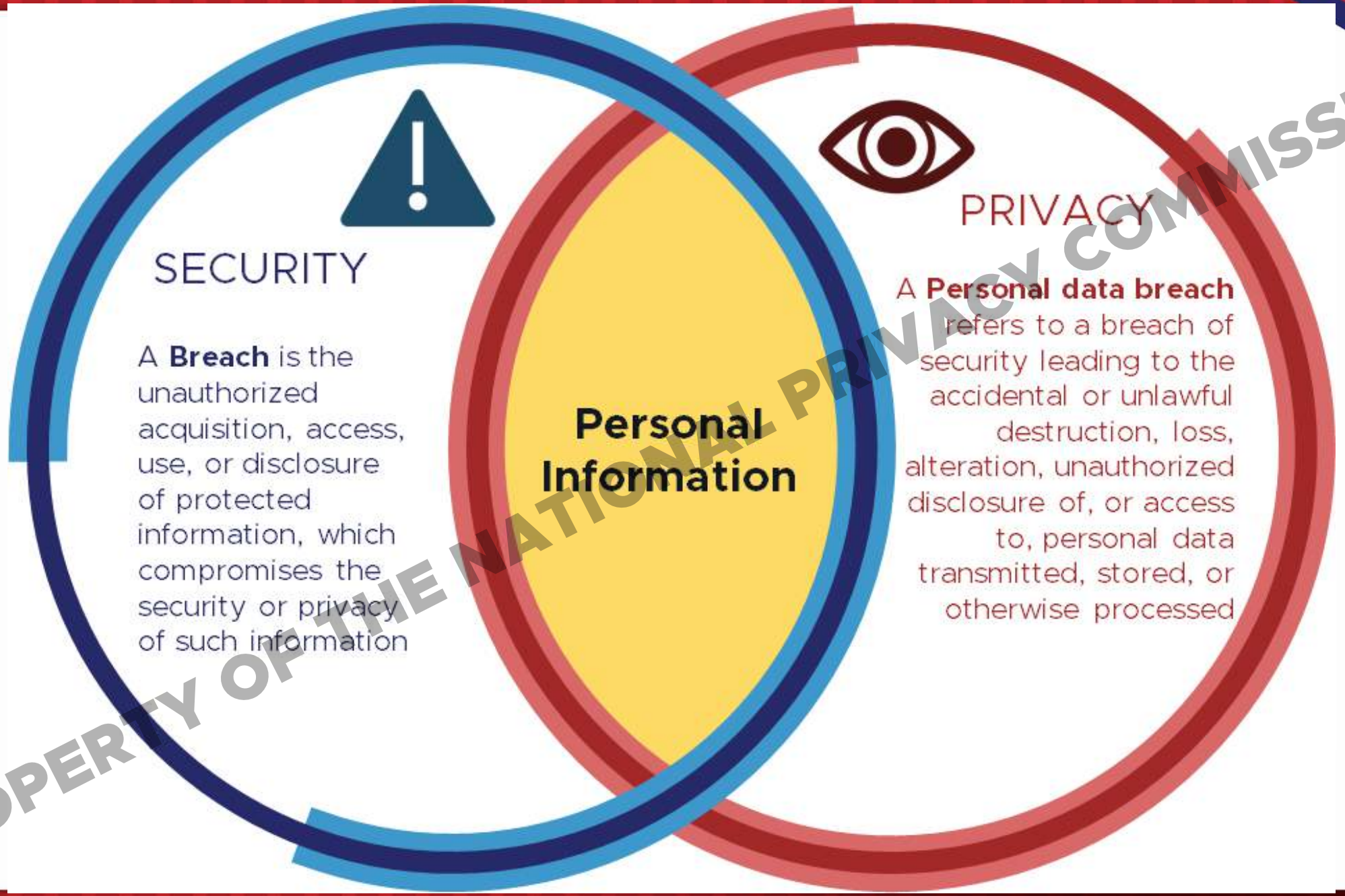
**Sections 1-6.**
Definitions and General Provisions

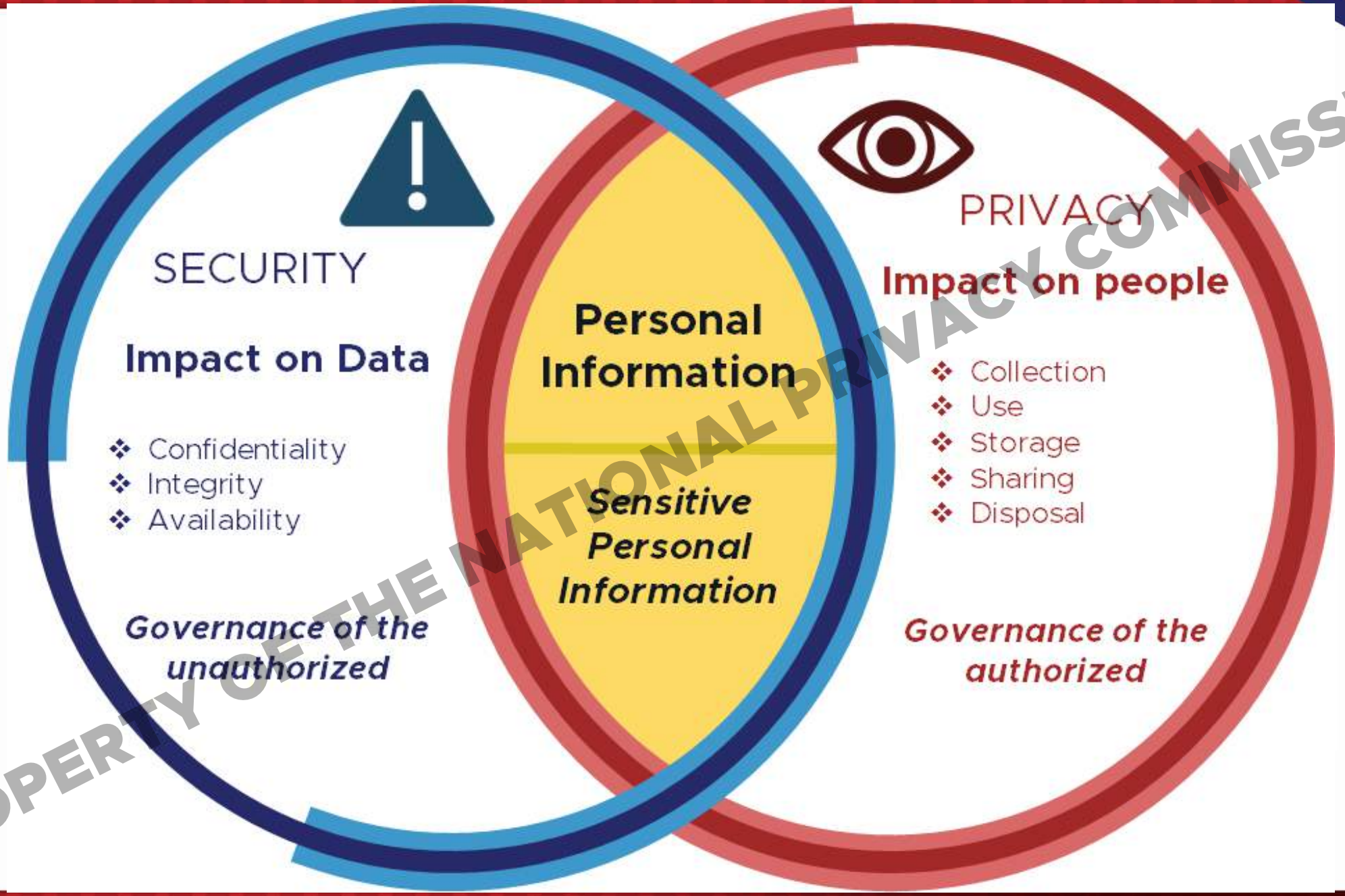
**Sections 25-37.**
Penalties

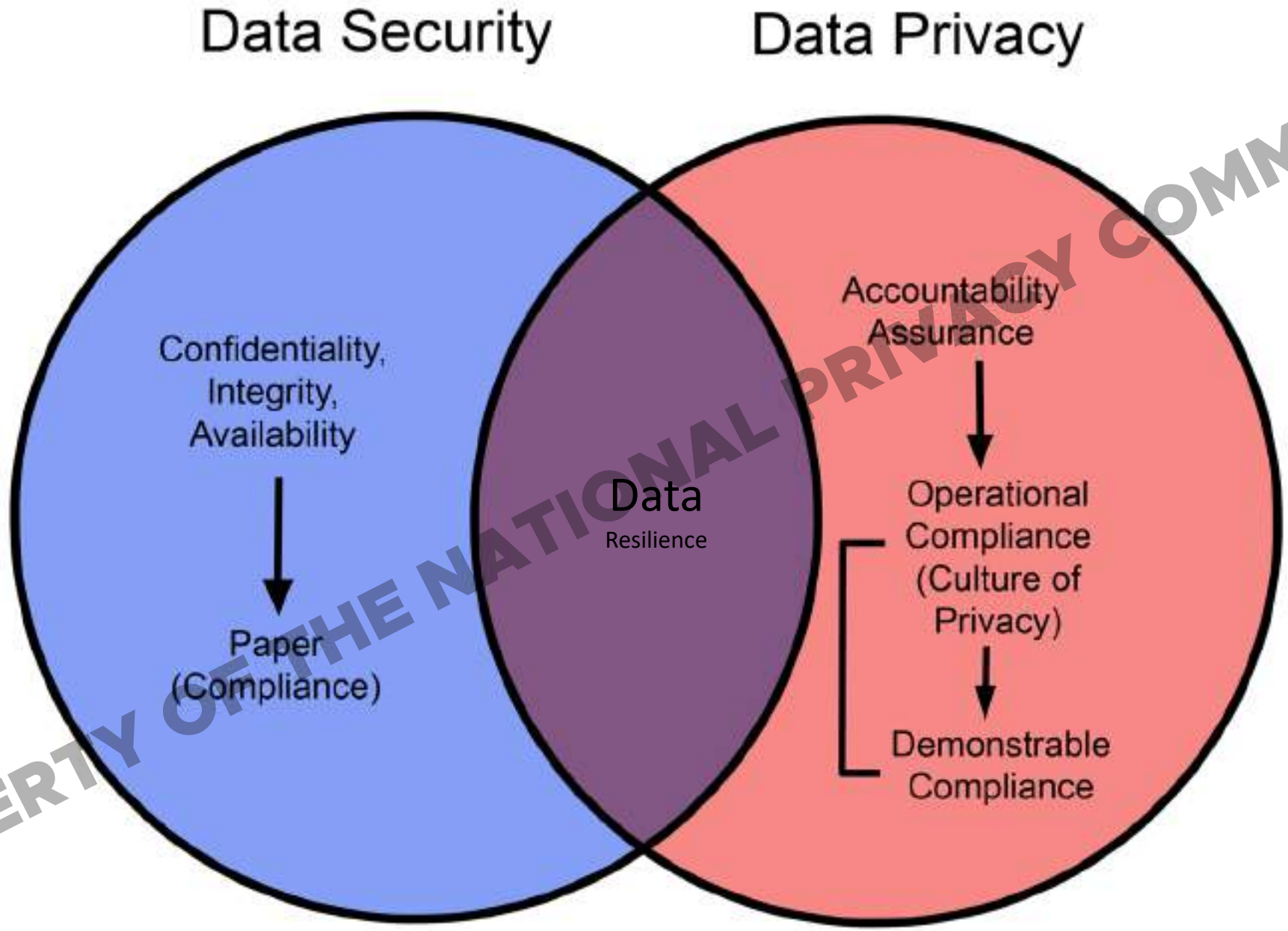

**Sections 7-10.**
The National Privacy Commission

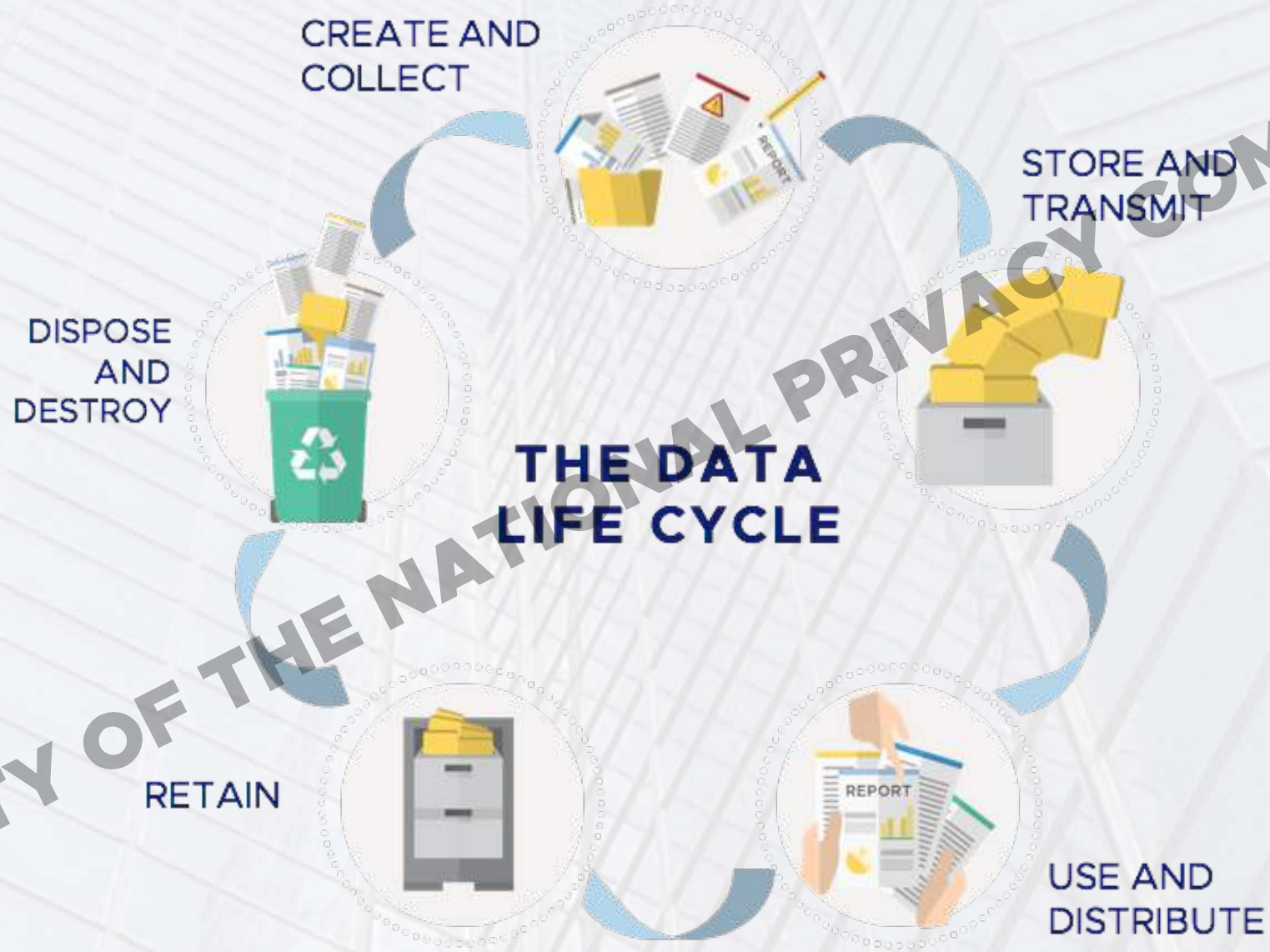
**Sections 22-24.**
Provisions Specific to Government

**Sections 11-21.**
Rights of Data Subjects, and Obligations of Personal Information Controllers and Processors










# THE DATA LIFE CYCLE



NATIONAL PRIVACY COMMISSION

Government DPO Conference 2018

GOVERNMENT DPO CONFERENCE 2018

# COMMON EXPOSURES OF DATA

## I. CREATE AND COLLECT



- No consent given
- Illegal/unfair/excessive collection
- Forced Consent/no choice
- Unsecured Collection
- Misleading purpose
- Unauthorized Secondary Purpose
- Indiscreet Conversation
- Tracking of Usage

Capability Development Grant (CDG) Funding for PDPA Services; taken from the Personal Data Protection Commission; 88 Privacy Breaches to Beware of (Marshall Cavendish copyright 2016)

# I. CREATE AND COLLECT

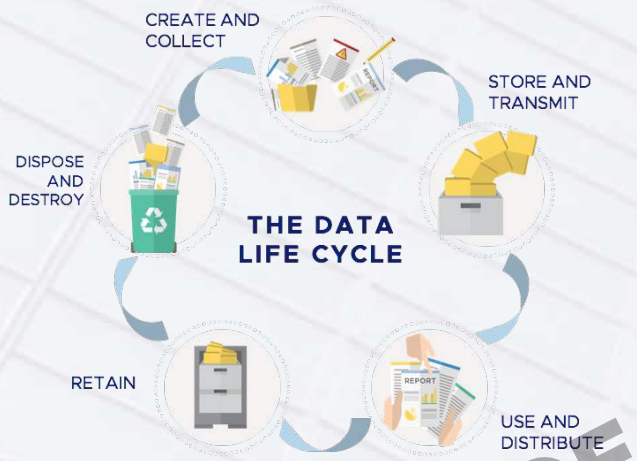

| Punishable Act | Imprisonment | Fine (PHP) |
|---|---|---|
| Unauthorized Purposes | 18 months to 5 years — 2 years to 7 years | 500 thousand to 2 million |
| Unauthorized Processing of Personal Information/Records | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |

# II. STORE AND TRANSMIT

| Punishable Act | Imprisonment | Fine (PHP) |
|---|---|---|
| Accessing of Personal Information and Sensitive Personal Information due to Negligence | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Intentional Breach | 1 year to 3 years | 500 thousand to 2 million |
| Malicious Disclosure | 18 months to 5 years | 500 thousand to 1 million |
| Unauthorized Disclosure | 1 year to 3 years — 3 years to 5 years | 500 thousand to 2 million |

# COMMON EXPOSURES OF DATA

## II. STORE AND TRANSMIT
## III. USE AND DISTRIBUTE




Capability Development Grant (CDG) Funding for PDPA Services; taken from the Personal Data Protection Commission; 88 Privacy Breaches to Beware of (Marshall Cavendish copyright 2016)


- Illegal access/usage
- Sale of data
- Negligent usage/misuse
- Invasion of Privacy/analytics
- Error in Processing
- Inaccurate/outdated Data
- Data was hacked/Account hacked
- Phishing

# III. USE AND DISTRIBUTE


| Punishable Act | Imprisonment | Fine (PHP) |
|---|---|---|
| Unauthorized Processing of Personal Information and Sensitive Personal Information | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Unauthorized Purposes | 18 months to 5 years — 2 years to 7 years | 500 thousand to 2 million |
| Intentional Breach | 1 year to 3 years | 500 thousand to 2 million |
| Concealing Breach | 18 months to 5 years | 500 thousand to 1 million |
| Malicious Disclosure | 18 months to 5 years | 500 thousand to 1 million |
| Unauthorized Disclosure | 1 year to 3 years — 3 years to 5 years | 500 thousand to 2 million |

# COMMON EXPOSURES OF DATA

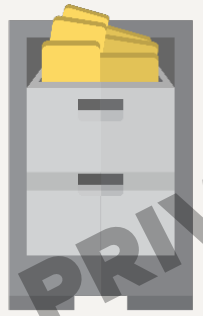
## IV. RETAIN



- Loss of Data
- Unlimited Retention
- Unsecured Data
- Virus/Malware/Ransomware
- Data Compromised
- Lost Device
- Unprotected Device
- Lost archives
- Identity Theft

Capability Development Grant (CDG) Funding for PDPA Services; taken from the Personal Data Protection Commission; 88 Privacy Breaches to Beware of (Marshall Cavendish copyright 2016)

# IV. RETAIN



| Punishable Act | Imprisonment | Fine (PHP) |
|---|---|---|
| Access due to Negligence of Records | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Malicious Disclosure | 18 months to 5 years | 500 thousand to 1 million |
| Unauthorized Disclosure | 1 year to 3 years — 3 years to 5 years | 500 thousand to 1 million |

# COMMON EXPOSURES OF DATA

## V. RETAIN
## (DISCLOSURE/TRANSFER)



Capability Development Grant (CDG) Funding for PDPA Services; taken from the Personal Data Protection Commission; 88 Privacy Breaches to Beware of (Marshall Cavendish copyright 2016)

- Improper Disposal
- Unauthorized Disclosure to Third Parties
- Social Engineering
- Misrepresentation
- Confidentiality Breach
- Illegal Access
- Denial of Access
- Insecure Transmission

# V. DISPOSE AND DESTROY

| Punishable Act | Imprisonment | Fine (PHP) |
|---|---|---|
| Improper Disposal of Records | 6 months 2 years — 1 year to 3 years | 100 thousand to 1 million |
| Access due to Negligence | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Concealing Breach | 18 months to 5 years | 500 thousand to 1 million |

NATIONAL
PRIVACY
COMMISSION

# Storage of Data in Paper Files

- "Clear-Desk-Policy" – sensitive papers are locked up when employees are not actively working on them.
- Shred paper files on disposal
- Access by authorized personnel on a need-to-know basis.
- Files under Lock and Key or in a secure area

# Transmission of Data by Mail

- Make use of sealed envelopes
- Make sure no sensitive data is visible through the envelope window
- Mark mail “private and confidential” if intended for the eyed of the addressee only.

# Transmission of Data by Fax

- Make sure dedicated fax machine is used at the receiving end
- Notify fax recipients in advance of transmission.
- Check accuracy of the fax number before dialing.

# Electronic Storage and Transmission

- Restrict indiscriminate uploading or downloading of data
- Automate routing to a dedicated computer directory
- Use encryption
- Password Protection
- “Confidential Mail Boxes”

# Portable Electronic Storage Device

- Password-Protect portable storage devices
- Encrypt portable storage devices

# Remote Access Account Data

- Avoid setting “obvious”/ default passwords on accounts
- Change Passwords regularly

# Service of Legal Processes

- Documents should be contained in sealed envelopes except where personal service is to be affected directly on the individual

# Server Security

- Keep Servers and Network switch boards in a locked room, with controlled access
- Unplug unused network extensions
- Consider hiring a knowledgeable IT Manager
- Equip desktop units and servers with a firewall, regular updates, and anti-virus software
- Restrict the number of administrator passwords

# Server Security Cont.

- Read server reports and security logs to monitor for changes and anomalies
- Rapid Response maintenance contract for any servers
- Do not use servers as an employee workstation
- Treat backups with the same level of security as complete copies.

# Accessing the Database

- Regularly review and update who has access to which information.
- Limit the number and scope of administrative users
- Allot access based on an individual's role, restricted to only the data they need
- Each employee should have their own private user ID

# Accessing the Database Cont.

- Secure the network with a firewall
- Set all computers attached to the network to log out after a few minutes of inactivity, and to require secure login.
- Delete a user's access privileges once they stop working for the organization
- Review firewall and server logs to monitor remote access.

# Accessing the Database Cont.

- Keep firewall and VPN software updated.
- Regulate programs that are used and installed by employees to prevent possible firewall breaches.

# DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK


A. Choose a DPO

B. Register
C. Records of processing activities
D. Conduct PIA

E. Privacy Management Program
F. Privacy Manual

G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy


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. Trainings and Certifications
W. Security Clearance

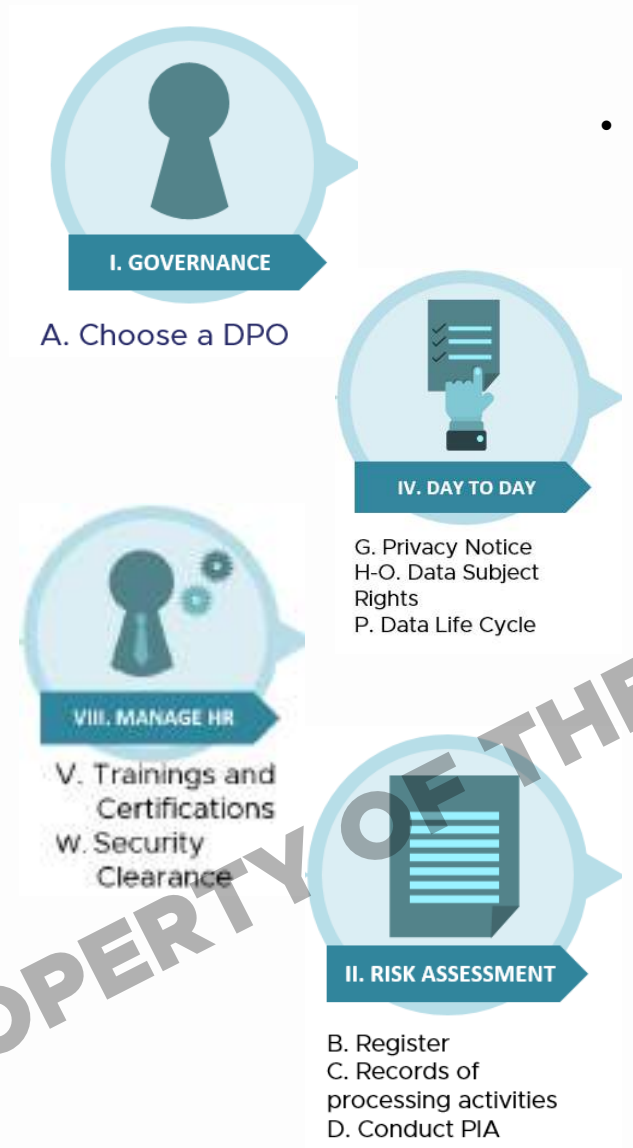
X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

Y. New technologies and standards
Z. New legal requirements



NATIONAL PRIVACY COMMISSION

# Government Requirements based on Memo Circular 16-01




## Section 4

- **Appointment Papers of a Data Protection Officer**: I
  - *A designated individual(s) who is accountable for the organization's compliance with the DPA*

- **Privacy and data protection policies**: IV
  - *Create privacy and data protection policies*

- **Data Privacy Awareness Trainings**: VIII
  - *Conduct an agency-wide training awareness campaign on privacy and data protection*

- **Registration of data processing system**: II
  - *Create an inventory of records of data processing systems to get ready for registration with the NPC*

# Government Requirements based on Memo Circular 16-01


B. Register
C. Records of processing activities
D. Conduct PIA


Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy

## Section 5

**Privacy Impact Assessments**: II

*-Conduct a privacy impact assessment for each program or process to determine the privacy risks*

## Section 6

- **Control Framework for RISKS**: V

*- Address the risks identified in the privacy impact assessments by creating a control framework with proper organizational, physical and technical security measures*

-

- **ISO/IEC 27002** (recommended): V

*- For large-scale agencies (more than 1,000 employees), it is recommended to implement the use of ISO/IEC 27002 – Code of practice for information security controls*



NATIONAL PRIVACY COMMISSION

# Government Requirements based on Memo Circular 16-01


## Section 7

**Data Center**: V

*Personal data being processed by a government agency shall be stored in a data center with the appropriate control framework for data protection*

## Section 8

**Encryption of personal data at rest and in transit** (AES-256):

*Personal data that are processed digitally, at rest and in transit, must be encrypted using Advanced Encryption Standard with a key size of 256 bits as minimum standard*

**Password policy**:

*Enforcement of a strong and sufficient password policy to deter passwords attacks*

# Government Requirements based on Memo Circular 16-01


Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy


U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

## Section 9

**Access Control Policy:** V

*Access to all applications, processing systems and facilities owned and controlled by an agency shall be restricted to its personnel that have the appropriate security clearance*

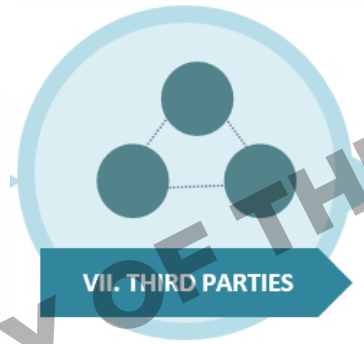
## Section 10

**Outsourcing Contracts**: VII

*When dealing with personal information processors, ensure that proper organizational, physical and technical security measures are in place to ensure the confidentiality, integrity and availability of personal data*

# Government Requirements based on Memo Circular 16-01


X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations




U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

## Section 11

**Third Party Audits**: IX

*To further ensure personal data protection, an audit by the NPC or independent verification/certification by a reputable third party is recommended*

## Section 12

**ISO/IEC 27018 certification (recommended):** VII

*An ISO/IEC 27018 certification is recommended when the agency have cloud service processors*



NATIONAL PRIVACY COMMISSION

# Government Requirements based on Memo Circular 16-01


## Section 13

**Archives**: V

*Apply organizational, physical and technical security measures to protect archived personal data*

## Section 14 - 15

**Access Control and Security Clearance for Database Modification or Personal Data Access**

*Strictly regulate access to personal data by having a security clearance policy for personal data that are in the agency's custody*

# Government Requirements based on Memo Circular 16-01


## Section 16

**Access Control Policy on Outsourced Providers**

*Contractors, consultants and service providers that have access to personal data shall be governed by strict procedures stated in their contracts*

## Section 17 - 18

**Acceptable Use Policy**

*Have an up-to-date acceptable use policy regarding the use of ICT resources*

- **Secure Encrypted link and Multi-Factor Authentication for Online Access**
  - *Agency personnel who access personal data online should authenticate their identity through a secure encrypted link and use multi-factor authentication*

# Government Requirements based on Memo Circular 16-01


## Section 19

**Automatic Deletion**

*Provide for the automatic deletion of temporary files that may be stored on a local machine*

**Network Drive**

*Personnel shall only be permitted to save personal data to an allocated network drive whenever applicable*

**Drives and USB ports (disabling policy)**

*Establish policies to prevent unlawful personal data distribution through portable media*

# Government Requirements based on Memo Circular 16-01


**Section 20**: V

- **Authorized Devices Policy**

*- Ensure that only authorized devices are being used*

**Section 21**: V

- **Remote Wipe/Deletion Policy**

*- Adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency or the deletion of personal data in it*

**Section 22**: V

- **Paper-based Filing System**

*- Maintain a log for personal data that are stored in paper files or any physical media*

# Government Requirements based on Memo Circular 16-01


**Section 24**: V

- **Email Encryption**

*- If personal data are transferred by email, data must be encrypted*

**Section 25**: V

- **Policies on printing personal data**

*- Controls must be in place to prevent personnel from printing or copying personal data to personal productivity software like word processors and spreadsheets*

**Section 26:** V

- **Full Disk Drive Encryption**

*- Ensure that the agency utilizes full disk encryption whenever portable media are used for personal data processing*

**Section 27**: V

- **One-time PIN for CD or DVD usage or distribution**

*- If the use of compact discs in personal data transfer is unavoidable, an authentication technology such as one-time PIN (OTP) must be in place*

# Government Requirements based on Memo Circular 16-01


**Section 28**: V

- **Fax Machines**

*- Facsimile technology shall not be used for transmitting documents containing personal data*

**Section 29**: V

- Email or Post Mail usage policy

*- Organizational, physical and technical measures should be adopted in transmitting documents or media containing personal data by mail or post*


**Section 31**: IV

- Disposal Policy

*- Procedures must be established regarding secure disposal of personal data stored onsite (files and computer equipment) and offsite*

**Section 33:** VI

- Data Breach Management

*- Establish data breach management procedures*



NATIONAL PRIVACY COMMISSION