Slide 1

Data Privacy Awareness Training

for Caspo Incorporated

Slide 2

Data Privacy Awareness of Employees

It is a set of understandings to indicate the employee's ability to transfer and apply knowledge, skills, and attitude of handling the privacy of data and security of information in the business process and information systems of the company.

Slide 3

Questions of Understanding

1. What are the mandated goals, of what to achieve, what to maintain, what to prevent, and what to eliminate as stated in RA 10173 – Data Privacy Act of 2012 and NPC advisories?
2. What are the roles, who are the actors representing compliance, oversight, regulations, and interest., and what is the interaction model of accountability and responsibility?
3. What are the actions that violate the privacy of personal data and the security of personal information

Slide 4

Questions of Understanding

4. What are the principles and policies that determine the front office and back-office activities and behavior of assuring data privacy protection in the business regulated data processing of personal information?
5. What are the activities to be performed that enable data subject to exercise their privacy rights?
6. What are the activities to be performed to assure the presence of information security measures?

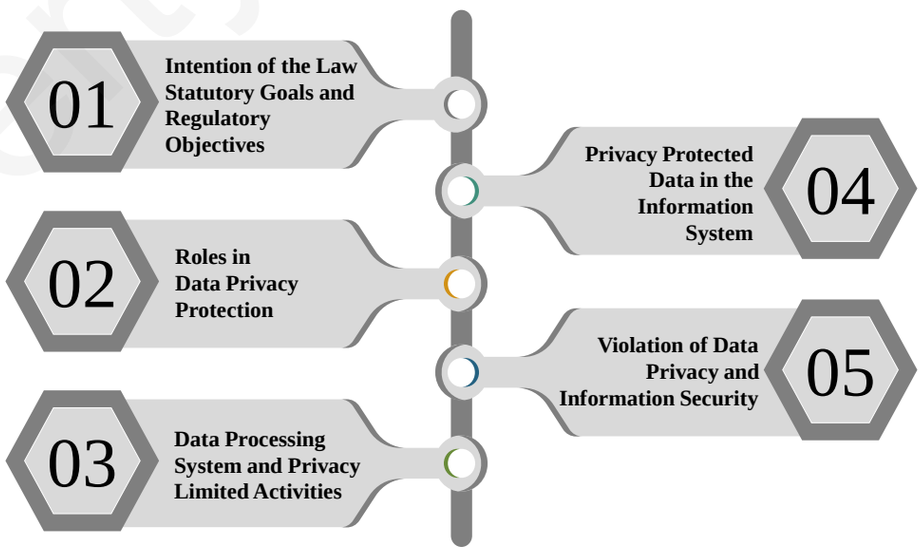
Slide 5

Questions of Understanding

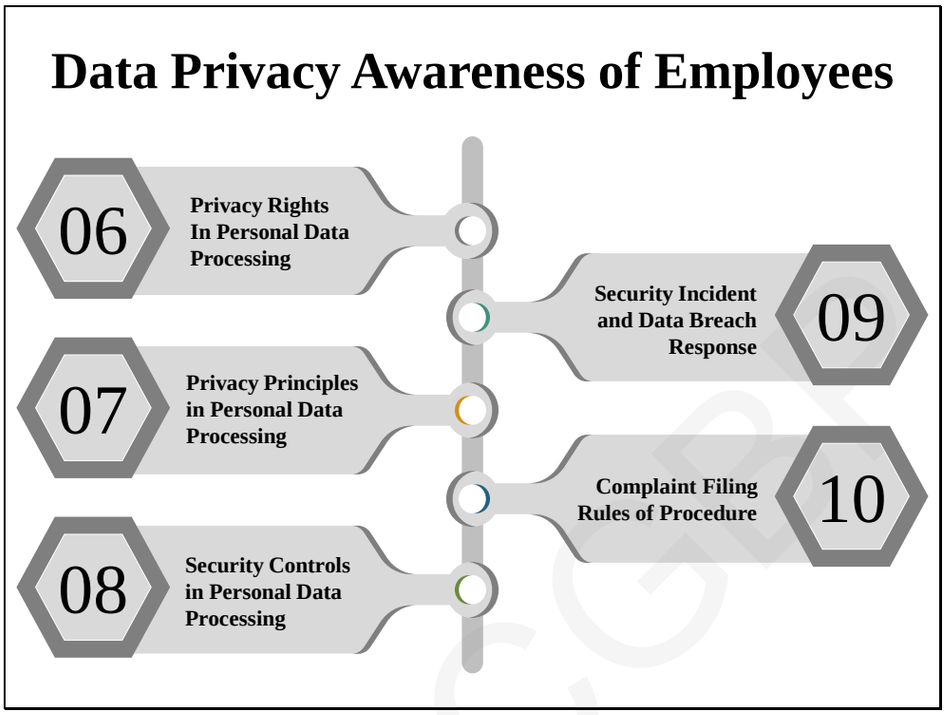
7. What is the information processing map that demonstrates the steps, data flow, roles, and decision associated with data privacy regulatory standards compliance?
8. What are the security incidents associated with data breach, and the incident response procedures
9. Who is the single point of contact to manage data privacy complaint? What is the rule of procedure in filing complaint?
10. What regulatory standards guide understanding and decision on data privacy and information security?

Slide 6

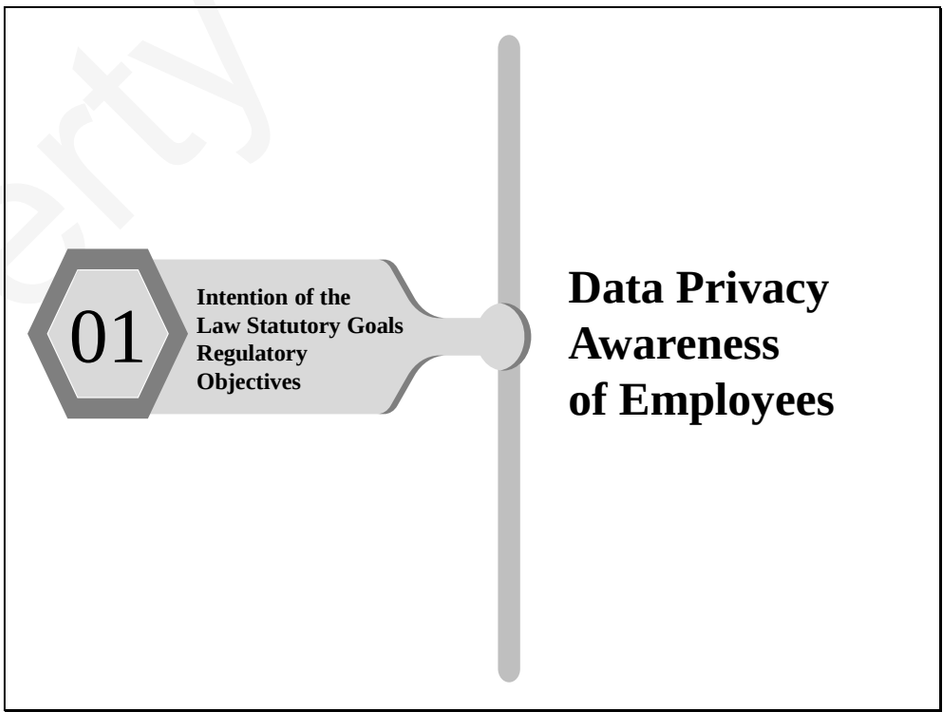
Data Privacy Awareness of Employees



Slide 7



Slide 8



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

https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

Information System Context of Privacy Protection
1
PROVIDER
CONSUMER
REGULATOR
VIOLATOR
ACCESS
DEVICES
2
OPERATING
ENVIRONMENT
Device OS
Network OS
IOT OS
Sensor OS
4
APPLICATION
ENVIRONMENT
Productivity
Office Tools
Image & Video
Sharing
Business & Social
Application
CRM & ERP System
Internet
Browsing
Communication
& Collaboration
Document
Management
Data Creation, Collection, Retention,
Utilization, Disclosure, Dispose
3
NETWORK
ENVIRONMENT
Communication
Services
Internet
Intranet
7. SECURITY &
PRIVACY
ENVIRONMENT
Security
Controls
Privacy
Process
Cyber Security
Methodologies and Technologies
Security
Incident
Management
5
STORAGE
ENVIRONMENT
Net Drive
Device Store
Removable
Drive
6
DATA
ENVIRONMENT
Personal
Information
Conversation
& Streamed Data
Structured/
Unstructured Data

Slide 11

Implementing Rules and Regulations of RA 10173

Rule 1 – Policy and Definitions

Rule 2 – Scope of Application

Rule 3 – National Privacy Commission

Rule 4 – Data Privacy Principles

Rule 5 – Lawful Processing of Personal Data

Rule 6 – Security Measures Protection of Personal Data

Rule 7 – Security of Sensitive Personal

https://privacy.gov.ph/wp-content/uploads/2023/06/IRR_RA-10173-as-amended.pdf

Slide 12

Implementing Rules and Regulations of RA 10173

Rule 8 – Rights of Data Subject

Rule 9 – Data Breach Notification

Rule 10 – Outsourcing and Subcontracting

Rule 11 – Registration and Compliance Requirements

Rule 12 – Rules on Accountability

Rule 13 – Penalties

Rule 14 – Miscellaneous Provisions

https://privacy.gov.ph/wp-content/uploads/2023/06/IRR_RA-10173-as-amended.pdf

Slide 13

Goals of R.A. 10173

What to achieve and maintain?

1. Implementation of rules and standards to respect privacy rights and to assure confidentiality, integrity, and availability of personal information.
2. Compliance governance to lead, direct, and control data privacy assurance and security of personal information protection.
3. Enabling capability for the personal information controller and processor to accomplish the mandated requirements of compliance that are monitored in order to assure privacy protection and information security.
4. Provision of regulation and procedures to create policies, to file complaints, to investigate violation, and to provide remediation.

Slide 14

Goals of R.A. 10173

What to prevent and eliminate?

1. Penalized violation against data privacy of a data subject.
2. Non-conformity of the filing system, automation program and technology services to the data privacy rights, data privacy principles, lawful processing criteria, condition to process sensitive information, and security measures in the personal data collection, processing, retention, sharing, and disposal.
3. Insecure technology infrastructure and negative user behaviour of unlawful access, control, processing, transmission, storage, sharing, and deletion of personal data.

Slide 15

PRIVACY

Freedom from intrusion into the private life or affairs of an individual when that intrusion results from *undue or illegal gathering and use of data about that individual.*

(ISO 2382 – 2126263 - IT Vocabulary)

Slide 16

Information Confidentiality

Information is not made available or disclosed to unauthorized individuals, entities, or *processes.*

(ISO 27000 3.10 – Information Security Vocabulary)

Slide 17

Process Integrity

Information **represents the** property of accuracy and completeness.

(ISO 27000 3.36 – Information Security Vocabulary)

Slide 18

System Availability

Information is accessible and usable on demand by an authorized entity.

(ISO 27000 3.7 Information Security Vocabulary)

Slide 19

Information Security Incident

It is one or multiple related and identified *information security events* that can harm an organization's assets or compromise its operations.

Slide 20

Security Incident Handling

The actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents.*

Slide 21

Security Incident Response

The actions taken to mitigate or resolve an *information security incident*, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

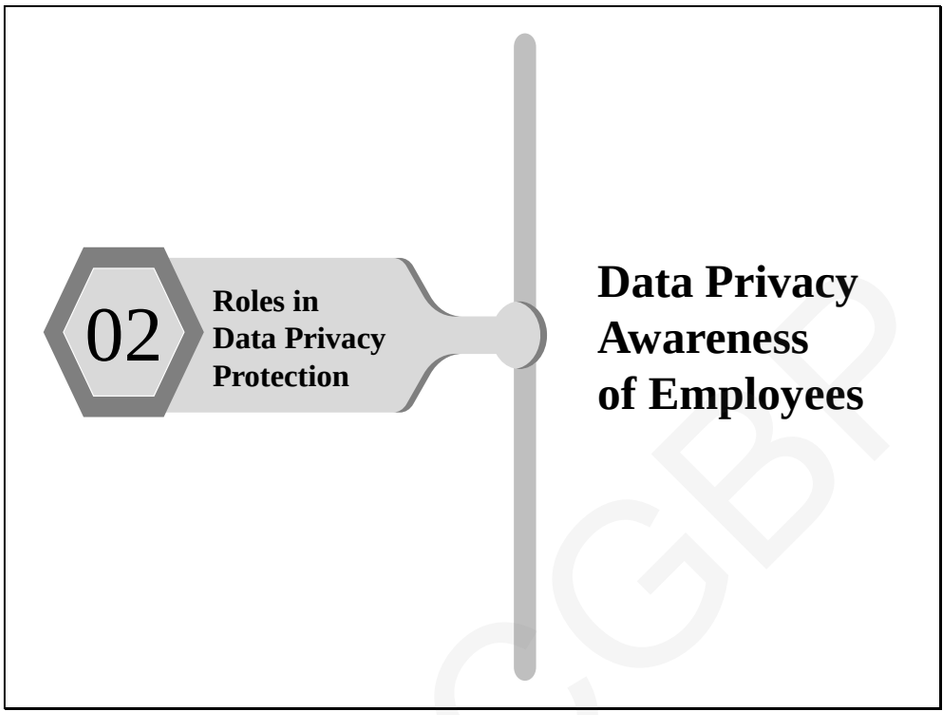
Slide 22

Data Privacy Protection

The ***security measures*** are taken to ensure privacy. It includes *data protection and limitations* on the gathering, combining, and processing of data about individuals.

(ISO 2382 – 2126264 – IT Vocabulary)

Slide 23



Slide 24

Data Privacy Stakeholders

Whose Interest and Benefit is Data Privacy Act of 2012 R.A. 10173	Participation, Accountability and Responsibility
1. Data Subject	Represents the exercise of data privacy rights and main party to associate personal data to be protected with privacy and security
2. National Privacy Commission	Creates regulation; monitor compliance; educate the public; and resolve cases on data privacy
3. Personal Information Controller	Directs and rules the processing of personal information with set limitations on data privacy
4. Personal Information Processor	Performs the instruction to process personal information based on privacy processing agreement with a Personal Information Controller

Slide 25

Data Privacy Stakeholders

Whose Interest and Benefit is Data Privacy Act of 2012 R.A. 10173	Participation, Accountability and Responsibility
5. Data Protection Officer	Perform the oversight function for the Personal Information Controller to achieve the mandated accountability and responsibility on data privacy
6. Compliance Officer for Privacy	Assist in the oversight function to direct, compliance, to monitor breach events, to resolve and report privacy security incidents
7. IT and Infrastructure Service Providers	Provision of the technical measures to secure personal information protection in the location, hardware, software, and services of personal data processing
8. 3rd Party of Data Sharing	Responsible for the transferred or shared data to be used in compliance with data privacy regulation

Slide 26

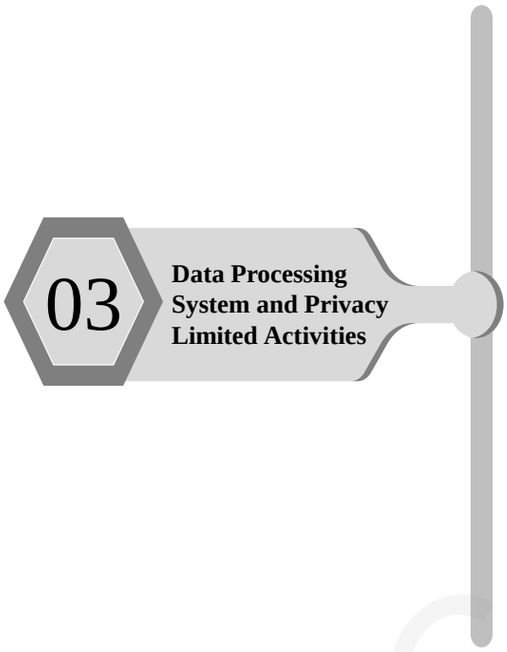
Data Protection Officer of CASPO Incorporated

Atty. Lorelee Margaret T. Granado
Email Address: **dpo@caspo.com**

Slide 27

NPC Advisory No. 2017-01: Designation of Data Protection Officers

Slide 28



Data Privacy Awareness of Employees

Slide 29

Regulated Processes of Information System in R.A. 10173

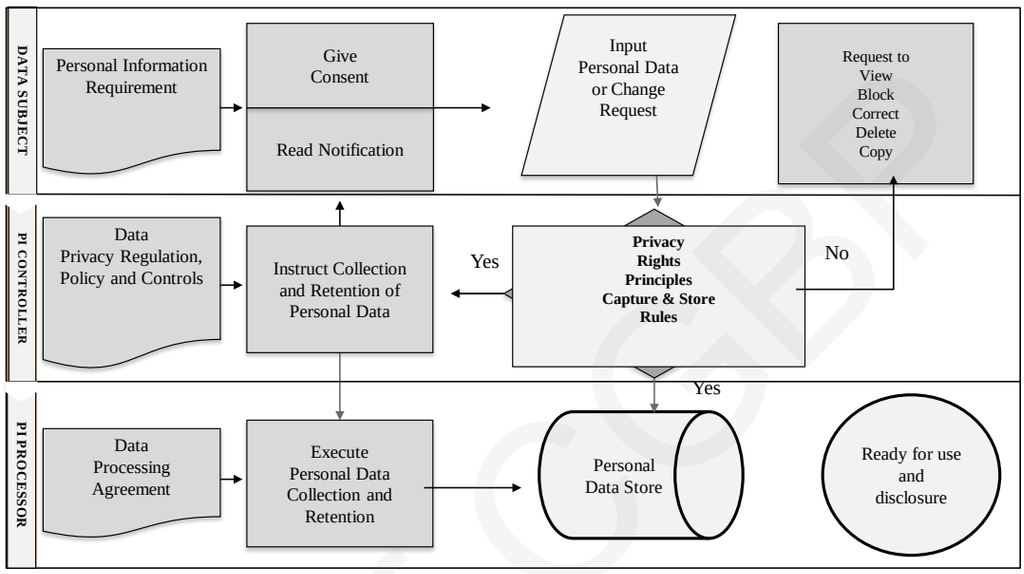
Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

- *Filing system*
- *Information and Communication System*
- *Automation Program*

1. **Collection (Data Gathering)**
2. **Retention (Data Storage)**
3. **Use (Data Processing)**
4. **Sharing (Data Disclosure)**
5. **Disposal (Data Destruction)**

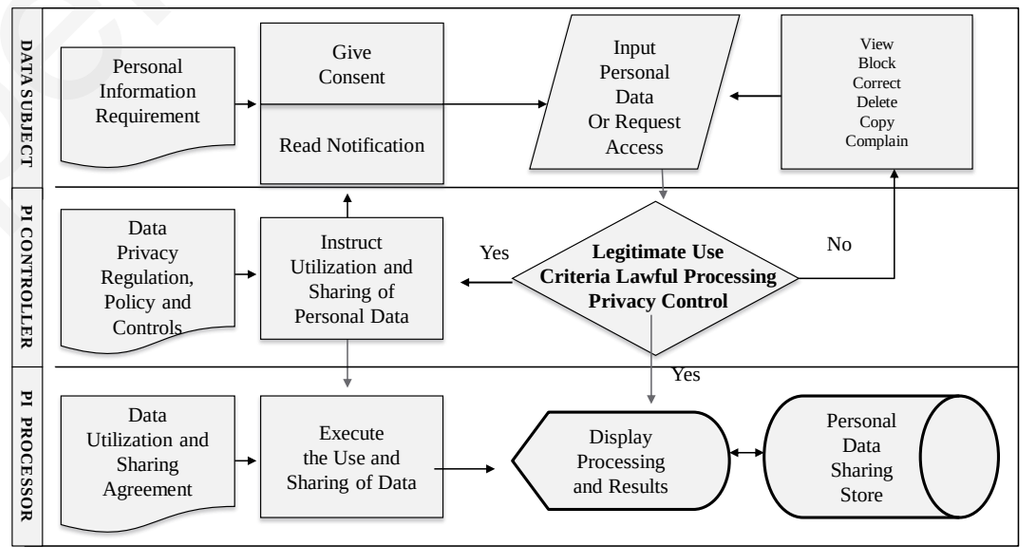
Slide 30

Personal Data Flow
Collection and Retention Process



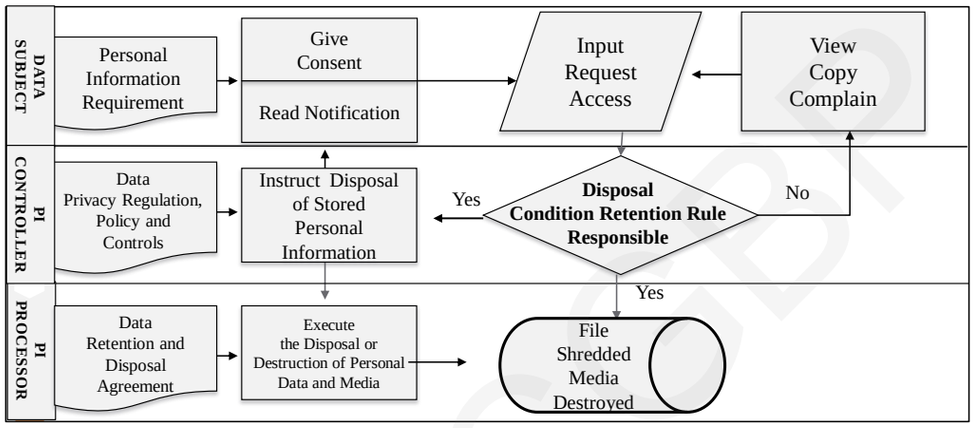
Slide 31

Personal Data Flow
Use and Disclosure Process



Slide 32

Personal Data Flow Disposal Process



Slide 33

NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments

NPC Privacy Toolkit - https://privacy.gov.ph/toolkits/

Slide 34

Data Privacy Awareness of Employees

Privacy Protected Data in the Information System 04

Slide 35

Data Privacy Act of 2012 protects the privacy rights and information security of person or individual identified called:

DATA SUBJECT - *whose personal, sensitive personal, or privileged information is processed by an information and communication system in the government and in the private sector.*

Slide 36

Personal data are facts about the individual, that can directly or indirectly **identify the person** with rights to privacy.

Slide 37

Personal Data Category

1. Name	Given name, middle name, surname, alias
2. Identification number	License number, tax number
3. Location data	Address, GPS location
4. Online identifier	E-mail, IP address
5. Digital identifier	Biometric, CCTV data
6. Genetic Data	DNA test result
7. Health Data	Diagnostic report
8. Research Data	Research question, enumerator interview logs
9. Physical factor	Height, weight, sex
10. Physiological factor	Body chemistry
11. Mental factor	Intellectual aptitude test results
12. Economic factor	Salary, debts, property
13. Cultural factor	Nationality, tribe
14. Social identity factors	Club membership, titles, legal record

Slide 38

Sensitive Personal Information (RA 10173 sec 3i)

1. Health, education, genetic or sexual life of a person.
2. Proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings.
3. Individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.
4. Identification document issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns.

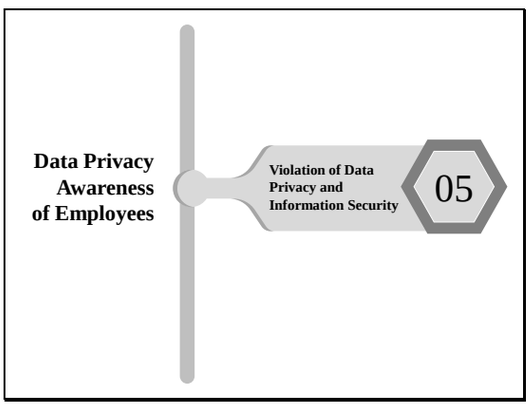
Slide 39

Privileged Personal Information

Privileged information refers to all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

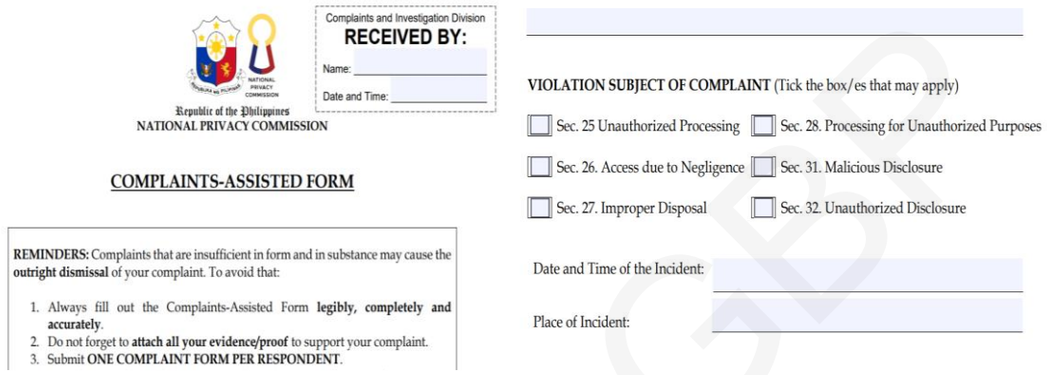
1. Patient and doctor communication
2. Client and lawyer communication
3. Informant and reporter

Slide 40



Slide 41

Data privacy violation in R.A. 10173



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

Complaints and Investigation Division
RECEIVED BY:
Name:
Date and Time:

COMPLAINTS-ASSISTED FORM

REMINDERS: Complaints that are insufficient in form and in substance may cause the **outright dismissal** of your complaint. To avoid that:

1. Always fill out the Complaints-Assisted Form **legibly, completely and accurately**.
2. Do not forget to **attach all your evidence/proof** to support your complaint.
3. Submit **ONE COMPLAINT FORM PER RESPONDENT**.

VIOLATION SUBJECT OF COMPLAINT (Tick the box/es that may apply)

- ☐ Sec. 25 Unauthorized Processing
- ☐ Sec. 26. Access due to Negligence
- ☐ Sec. 27. Improper Disposal
- ☐ Sec. 28. Processing for Unauthorized Purposes
- ☐ Sec. 31. Malicious Disclosure
- ☐ Sec. 32. Unauthorized Disclosure

Date and Time of the Incident:

Place of Incident:

https://www.privacy.gov.ph/wp-content/uploads/2021/04/CAF-Fillable.pdf

Slide 42

Data Privacy Violations and Penalties – Rule XIII

1. Unauthorized processing 3-6 years imprisonment 500K-4M penalty	It is when personal information is processed without the consent of the data subject, or without being authorized using lawful criteria.
2. Negligence in access 1-6 years imprisonment 500K-4M penalty	It is when personal information is made accessible due to negligence and without being authorized by any existing law.

Slide 43

Data Privacy Violations and Penalties – Rule XIII

3. Improper disposal 6 months-3 years imprisonment 100K-1M penalty	It is when personal information is knowingly or negligently disposed, discard, or abandon in an area accessible to the public or has otherwise placed the personal information of an individual in any container for trash collection.
4. Unauthorized purpose 1-7 years imprisonment 500K-2M penalty	It is when personal information is processed for purposes not authorized by the data subject, or otherwise authorized by any existing laws.

Slide 44

Data Privacy Violations and Penalties – Rule XIII

5. **Unauthorized access or intentional breach** 1-3 years imprisonment 500K-2M penalty	It is when an individual handling personal information knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored.
6. Concealed breach 1-5 years imprisonment 500K-1M penalty	It is when an individual or entity who has knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Act, intentionally or by omission conceals the fact of such security breach.

Slide 45

Data Privacy Violations and Penalties – Rule XIII

7. Malicious disclosure 1-65years imprisonment 500K-1M penalty	It is when an individual or entity with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her.
8. Unauthorized disclosure 1-5 years imprisonment 500K-2M penalty	It is when an individual or entity discloses to third party personal information not covered by legitimate purpose, lawful criteria, and without the consent of the data subject.

Slide 46

Cyber Crime (R.A. 10175)

1. It is offense against the confidentiality, integrity and availability of computer data and systems.

1.1 Illegal Access	Access to the whole or any part of a computer system without right.
1.2 Illegal Interception	Interception made by technical means without right.
1.3 Data Interference	Intentional or reckless alteration, damaging, deletion of computer data.
1.4 System Interference	Intentional alteration or reckless interference with the functioning of a computer or computer network.
1.5 Misuse of Devices	Use, production, sale, procurement, importation, distribution, or otherwise making available, without right.
1.6 Cyber Squatting	Acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation and deprive others from registering the same.

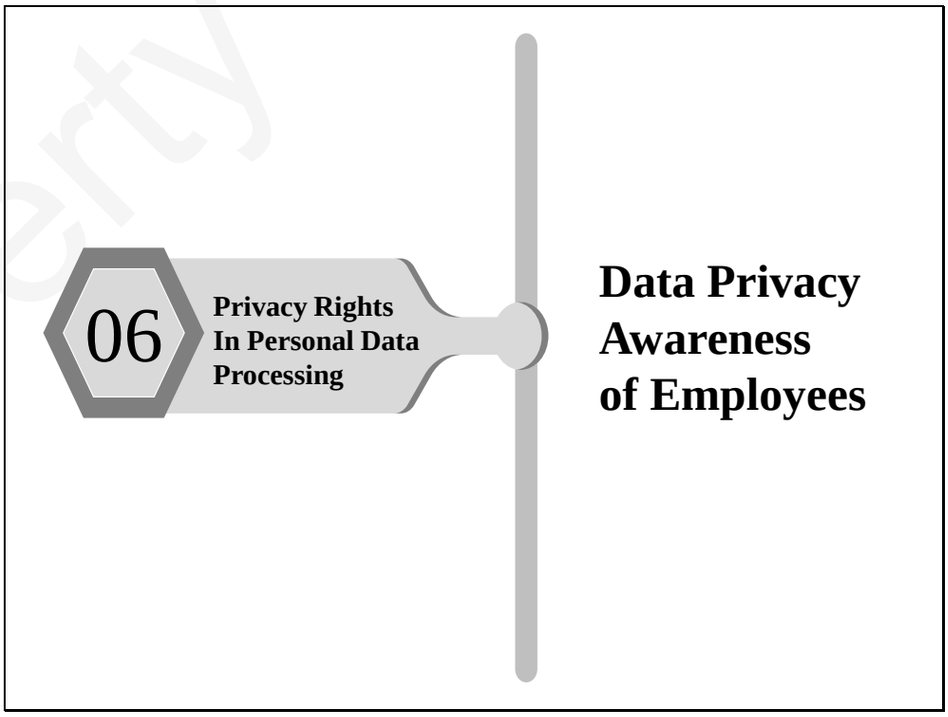
Slide 47

Cyber Crime (R.A. 10175)

2. It is offense related with the use of computer.

2.1 Forgery	Input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.
2.2 Fraud	Unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent.
2.3 Identity Theft	Intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right.

Slide 48



Slide 49

Privacy Rights on Personal Data – Rule VIII

Privacy Rights of Data Subject	Respect Indicators
1. The right to be informed	*Privacy Notification*
2. The right to give consent	*Written or recorded agreement to process personal data*
3. The right to access	*Permission to view and participate*
4. The right to object	*Procedure to withhold or refuse*

Slide 50

Privacy Rights on Personal Data – Rule VIII

Privacy Rights of Data Subject	Respect Indicators
5. The right to erasure or blocking	*Permission to withdraw and delete personal data*
6. The right to rectify	*Permission to check accuracy and to correct*
7. The right to data portability	*Ability to request and download personal data*
8. The right to complain	*Rules of procedure to file complaint*
9. The right to claim damages	*Rule of procedure to claim damages*

Slide 51

NPC Advisory No. 2021-01: Data Subject Rights

Slide 52

07 **Privacy Principles in Personal Data Processing**

Data Privacy Awareness of Employees

Slide 53

PRIVACY PRINCIPLES

The foundational belief of data processing system that is privacy by design and by default.

ISO 29100 – Privacy Framework

Transparency
Consent and choice
Participation
Accuracy
Legitimate Purpose
Accountability
Proportionality
Anonymity
Fairness
Lawfulness
Minimization

Slide 54

Privacy Principles of Personal Data Processing (Rule IV)

Principles of Transparency, Legitimate Purpose and Proportionality	
1. Transparency	The **data subject must be aware** of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
2. Legitimate purpose	The processing of information shall be compatible with a **declared and specified purpose** which must not be contrary to law, morals, or public policy.
3. Proportionality	The processing of information shall be **adequate, relevant, suitable, necessary, and not excessive** in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Slide 55

Privacy Principles of Personal Data Processing (Rule IV)

General principles in collection, processing and retention	
1. Collection must be for a declared, specified, and legitimate purpose.	**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 i**s required, it must **be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.**
	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.
	Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
	Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

Slide 56

Privacy Principles of Personal Data Processing (Rule IV)

2. Personal data shall be processed fairly and lawfully.	Processing shall 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.
	Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
	Processing must be in a manner compatible with declared, specified, and legitimate purpose
	Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
	Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.
3. Processing should ensure data quality.	Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
	Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

Slide 57

Privacy Principles of Personal Data Processing (Rule IV)

4. Personal Data shall not be retained longer than necessary.	Retention of personal data shall only for as long as necessary: (a) For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated. (b) For the establishment, exercise or defense of legal claims. (c) For legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
	Retention of personal data shall be allowed in cases provided by law.
	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 the public, or prejudice the interests of the data subjects.

Slide 58

Privacy Principles of Personal Data Processing (Rule IV)

5. Any authorized further processing shall have adequate safeguards.	Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.
	Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.
	Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Slide 59

Privacy Principles of Personal Data Processing (Rule IV)

General Principles for Data Sharing	
1. Data sharing shall be allowed when it is expressly authorized by law:	**Provided,** that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality

Slide 60

Privacy Principles of Personal Data Processing (Rule IV)

General Principles for Data Sharing	
2. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:	1. Consent for data sharing shall be required even when the data is to shared with an affiliate or mother company, or similar relationships 2. Data sharing for commercial purposes, including direct marketing, be covered by a data sharing agreement. 3. The data subject shall be provided with the following information p to collection or before data is shared: (a) Identity of the personal information controllers or personal information processors that will be given access to the personal data (b) Purpose of data sharing (c) 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 (f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing. 4. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.

Slide 61

Privacy Principles of Personal Data Processing (Rule IV)

Data collected from parties other than the data subject for purpose of research shall be allowed	When the personal data is publicly available or has the consent of the data subject for purpose of research: Provided, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.
Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement	1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security. 2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject

Slide 62

Sensitive Personal Information Processing (Rule V)

1. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose.
2. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing and guarantee the protection of personal data.
3. 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.
4. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations.
5. The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.
6. The processing concerns sensitive personal information or privileged information 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 pursuant to a constitutional or statutory mandate.

Slide 63

Lawful Criteria In Personal Information Processing – Rule V	**Valid Element**
1. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable.	Consent
2. The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement.	Contractual Agreement
3. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject.	Legal Obligation

Slide 64

Lawful Criteria in Personal Information Processing – Rule V	Valid Element
4. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health.	Vitally Important Interest
5. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law.	National Emergency, Public Order and Safety

Slide 65

Lawful Criteria in Personal Information Processing – Rule V	Valid Element
6. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority	Constitutional or Statutory Mandate
7. The processing is necessary to pursue the legitimate interests of 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	Legitimate Interest

Slide 66

1. NPC Circular No. 2023-04 - Guidelines on Consent

2. NPC Circular No. 2023-07 - Guidelines on Legitimate Interest
- FAQ Guidelines on Legitimate Interest

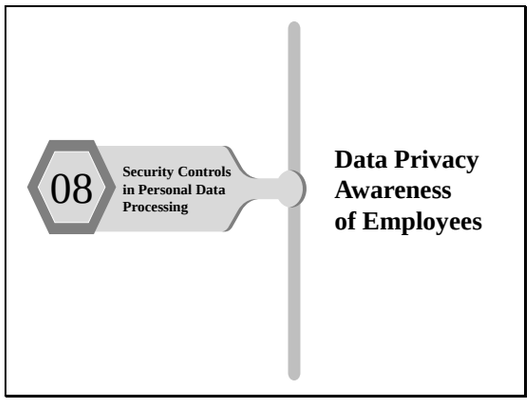
3. NPC Circular 2020-03 - Data Sharing Agreements

Slide 67

4. **NPC Circular 20-01 -** Guidelines on the Processing of Personal Data for Loan-Related Transactions

5. **NPC Circular No. 2022-03 -** Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information

Slide 68



Slide 69

Security Control Framework

It is the comprehensive enumeration of measures a personal information controller or processor 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.

(ISO 27701 3.2 Privacy Information Management System)

Slide 70

SECURITY MEASURES (RA 10173 Rule VI)

Organizational Security	Physical Security	Technical Security
1. Compliance Officers.	1. Policies and Procedures on Limited Physical Access	1. Security policy in processing personal data.
2. Data Protection Policies	2. Security Design of Office Space and Room	2. Safeguards to protect computer network again unlawful, illegitimate, and destructive activities.
3. Records of Processing Activities	3. Person Duties, Responsibility and Schedule Information	3. Confidentiality, integrity, availability, and resilience of the processing systems and services.
4. Processing of Personal Data	4. Policies on transfer, removal, disposal, and re-use of electronic media	4. Vulnerability assessment and regular monitoring for security breaches.
5. Personal Information Processor Contracts	5. Prevention policies against mechanical destruction of files and equipment	5. Ability to restore the availability and access to personal data.
		6. Regularly testing, assessing, and evaluating the effectiveness of security measures.
Reference Standard: ISO 27002 – Information Security Controls		7. Encryption of personal data during storage and while in transit, authentication process.

Slide 71

NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector

Slide 72

Data Privacy Awareness of Employees

Security Incident and Data Breach Response 09

Slide 73

Privacy Violation, Threat Sources and Security Control

Privacy Breach

Privacy Law
R.A. 10173

1. Unauthorized processing
2. Negligence in access
3. Improper disposal
4. Unauthorized purpose
5. Unauthorized access
6. Intentional breach
7. Concealed breach
8. Malicious disclosure
9. Unauthorized disclosure
10. Combination of unwanted act

Threats to Personal Data
(SANS Threat Survey)

1. Ransomware
2. Elevation of privilege into sensitive systems
3. Breaches in cloud-based, multitenant architectures
4. Denial of service
5. Data tampering
6. Identity theft
7. Insider threat
8. Questionable transactions
9. Corporate or foreign government espionage
10. Information disclosure
11. Compromise of DNS infrastructure enabling stealing and exfiltration of data
12. Anti-malware/Antivirus
13. Spoofing of identity or access credential
14. Drive-by Download

Security Controls
(R.A. 10173 and GDPR)

1. Security Policy
2. Network Protection
3. Confidentiality, Integrity, Availability, and Resilience Assurance of Processing System
4. Intrusion Detection and Prevention
5. Network Security Monitoring
6. Vulnerability Assessment and Penetration Testing
7. Backup and Data Recovery
8. Identity, Access, Privilege Management
9. Security Incident Management System
10. Data Loss Prevention
11. Encryption and Pseudonymization, Host-based encryption
12. Insider Threat Control
13. Third-Party Risk Management
14. Firewall/ UTM
15. End-Point Protection
16. Email security

Slide 74

Cyber Crime Against Privacy and Security of Personal Data

Violation/ Threat	Vulnerability/ Exploitation (ETSI ISG ISI)	Control Measures (CIS Security Controls)
Cyber Crime Prevention Law - R.A. 10175 1. Illegal access 2. Illegal interception 3. Data interference 4. System interference 5. Misuse of device 6. Fraud 7. Forgery 8. Identity Theft 9. Cyber-squatting 10. Libel 	1. Website Forgery 2. Spam 3. Phishing 4. Intrusion 5. Website Defacement 6. Misappropriation of Resources 7. Denial of Service 8. Malware 9. Physical Intrusion 10. Malfunction 11. Loss or theft of mobile device 12. Trace Malfunction 13. Internal Deviant Behavior 14. Rights or Privileges Usurpation or Abuse 15. Unauthorized access to servers through remote access points 16. Illicit Access to Internet 17. Deactivating of Logs Recording 18. Non-patched or poorly patched vulnerability exploitation 19. Configuration vulnerability exploitation 20. Security incidents on non-inventoried and/ or not managed assets	1. Inventory and Control of Enterprise Assets 2. Inventory and Control of Software Assets 3. Data Protection 4. Secure Configuration of Enterprise Assets and Software 5. Account Management 6. Access Control Management 7. Continuous Vulnerability Management 8. Audit Log Management 9. Email and Web Browser Protections 10. Malware Defenses 11. Data Recovery 12. Network Infrastructure Management 13. Network Monitoring and Defense 14. Security Awareness and Skills Training 15. Service Provider Management 16. Application Software Security 17. Incident Response Management 18. Penetration Testing

Slide 75

Security Incident Handling

Phase	Question of Understanding
1. Preparation	• Do you know the Incident Response Team of the company? • Are you aware of the security policies and incident response plan? • Do you know the incident reporting requirements and documentation templates of incidents?

Slide 76

Security Incident Handling

Phase	Question of Understanding
2. Identification	• When did the event happen? • How was it discovered? • Who discovered it? • Have any other areas been impacted? • What is the scope of the compromise? • Does it affect operations? • Has the source (point of entry) of the event been discovered?

Slide 77

Security Incident Handling

Phase	Question of Understanding
3. Containment	• What's been done to contain the breach short term? • What's been done to contain the breach long term? • Has any discovered malware been quarantined from the rest of the environment? • What sort of backups are in place? • Does your remote access require true multi-factor authentication? • Have all access credentials been reviewed for legitimacy, hardened and changed? • Have you applied all recent security patches and updates?

Slide 78

Security Incident Handling

Phase	Question of Understanding
4. Eradication	• Have artifacts/ malware from the attacker been securely removed? • Has the system been hardened, patched, and updates applied? • Can the system be re-imaged?

Slide 79

Security Incident Handling

Phase	Question of Understanding
5. Recovery	• When can systems be returned to production? • Have systems been patched, hardened and tested? • Can the system be restored from a trusted back-up? • How long will the affected systems be monitored and what will you look for when monitoring? • What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/ protection, etc)

Slide 80

Security Incident Handling

Phase	Question of Understanding
6. Lesson	• What changes need to be made to the security? • How should employee be trained differently? • What weakness did the breach exploit? • How will you ensure a similar breach doesn't happen again?

Slide 81

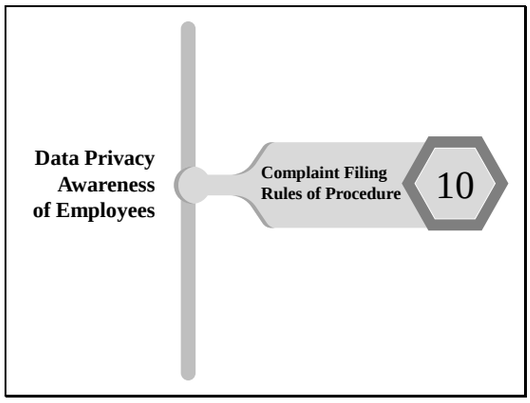
Data breach on personal information in the information and communication systems of the government and private sector has to be disclosed to the affected Data subjects, who may be harmed by identity fraud.

NPC Circular 16-03 - Personal Data Breach Management

- Breach reporting – 72 hours
- Breach notification content

ISO 27035 - Information Security Incident Management

Slide 82



Slide 83

References to handle privacy complaints

1. **NPC Circular 2021-01 -** 2021 Rules of Procedure of the National Privacy Commission
2. **NPC Circular 18-01 -** Rules of procedure on requests for Advisory Opinions
3. **NPC Circular 18-02 -** Guidelines on Compliance Checks

Slide 84

CENTER FOR GLOBAL BEST PRACTICES

THANK YOU!

For your queries, consulting requirements or request for in-house training programs, please contact:

Manila lines: (+63 2) 8556-8968 or 69
Telefax: (+63 2) 8842-7148 or 59

We invite you to visit our website **www.cgbp.org** for upcoming best practices programs.