ROADMAP to COMPLIANCE

Data Privacy Act of 2012

DP 6

NATIONAL PRIVACY COMMISSION

Exemptions?
IRR, Section 5-b.

Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;

Key point to remember: the INFORMATION is exempt, but YOU (as information processor) are not.

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

FBI Probing Possible Russian Hack of US Newsrooms: CNN

By AFP on August 23, 2016

Hackers with apparent ties to Russia have conducted a series of cyber attacks on US media outlets including the New York Times, CNN reported Tuesday.

The FBI and other US law enforcement agencies are examining the breaches, US officials told CNN, and investigators believe Russian intelligence is likely to be behind the hacks. The FBI did not immediately respond to a request for comment, and a New York Times spokeswoman did not confirm the investigation to CNN.

Due to negligence, provided access

SEC. 26. (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

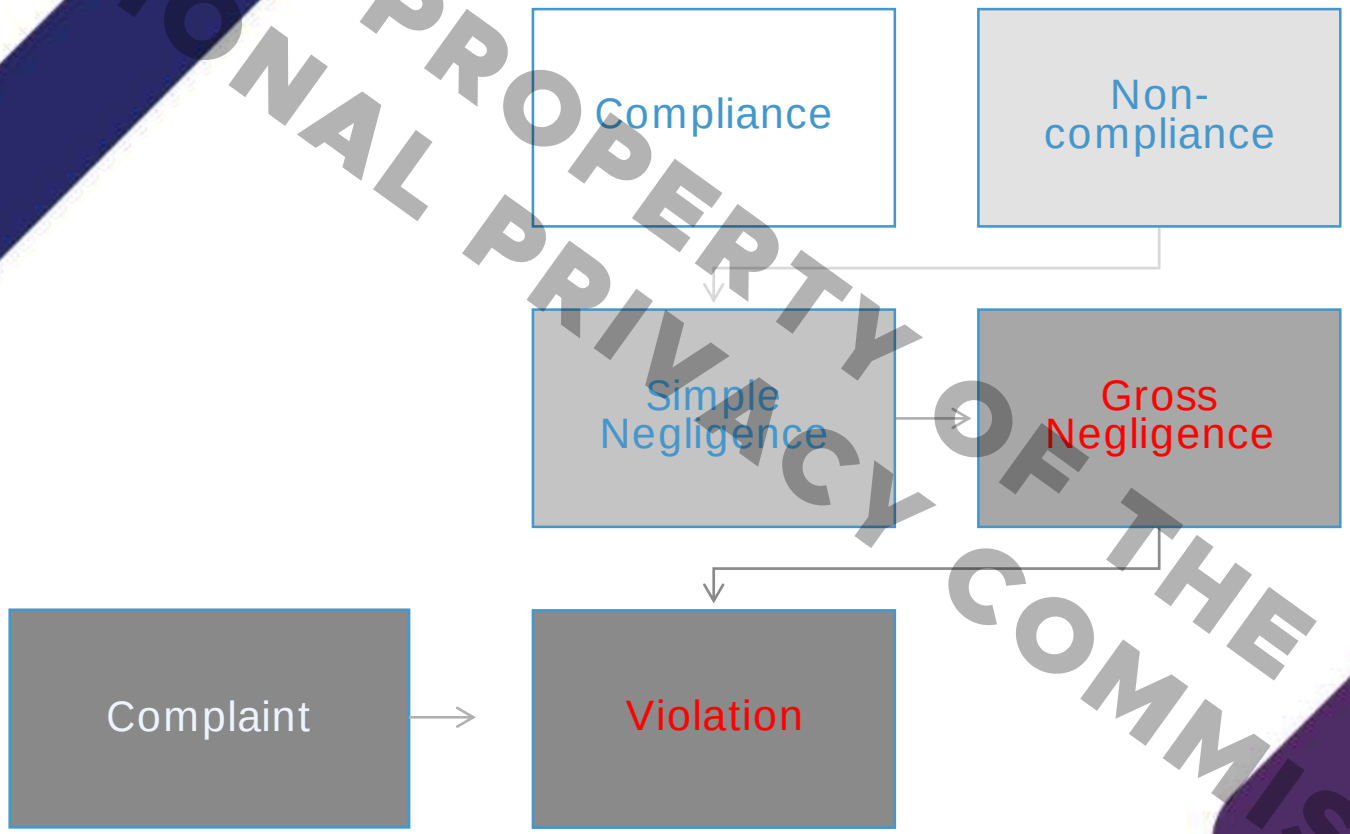
SEC. 35. Large-Scale. – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

Who is liable?

- Sec. 22. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein…

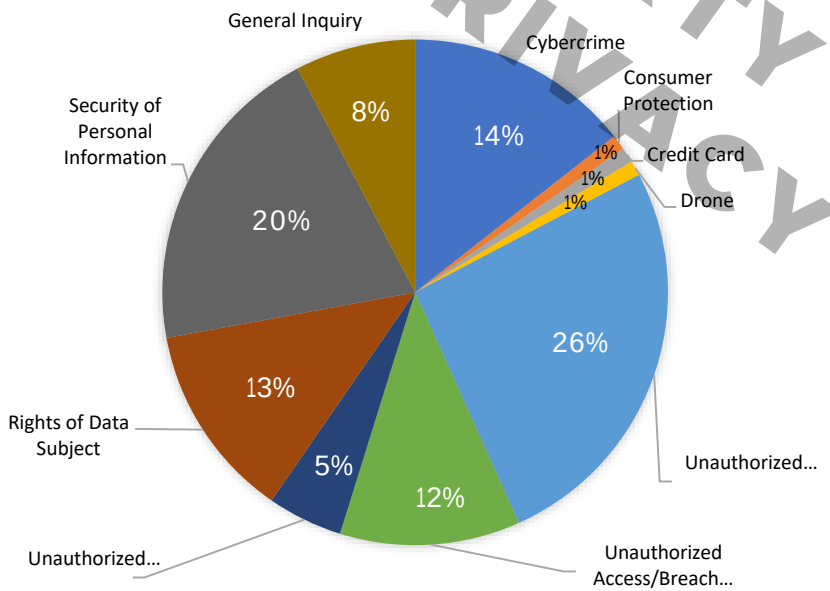
- Sec. 34. Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

Is non-compliance equal to a violation?



Complaints

NATURE OF COMPLAINTS RECEIVED BY NPC AS OF 30 JUNE 2017



REPORTS AS OF 30 JUNE 2017		
CLASSIFICATION	NO. OF COMPLAINTS	PERCENTAGE
Unauthorized Processing	27	26%
Unauthorized Access/Breach Reports	12	12%
Unauthorized Disclosure	5	5%
Rights of Data Subject	13	13%
Security of Personal Information	21	20%
General Inquiry	8	8%
Cybercrime	15	14%
Consumer Protection	1	1%
Credit Card	1	1%
Drone	1	1%
TOTAL	104	100%

DP 6 NATIONAL PRIVACY COMMISSION

The Obligations you must pay heed to

Data Privacy Act of 2012

IRRs (promulgated 2016)

2016 Series

- Circular 16-01 Gov't Agencies
- Circular 16-02 Data Sharing
- Circular 16-03 Breach Mgmt
- Circular 16-04 Rules Procedure

2017 Series

- *Advisory 17-01 DPO Guidelines*
- *Advisory 17-02 PDS Guidelines*
- *Advisory 17-03 PIA Guidelines*
- Circular 17-01 Registration

DP 6 NATIONAL PRIVACY COMMISSION

Data Privacy Act (RA 10173) Checklist

Signs of Compliance, Commitment to Comply, Capacity to Comply vs. Signs of Negligence

Pillar 1: Commit to Comply: Appoint a Data Protection Officer (DPO)

Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

Appoint an individual accountable for compliance	Ineffective data protection governance
☐ Notarized designation of a DPO/COP, filed with the NPC ☐ Evidence that DPO/COP recommendations are taken into consideration when making decisions ☐ Contact details are easy to find (e.g. on website) ☐ Continuing education program for the DPO/COP	☐ No DPO or COP (in which case CEO or HoA is the default DPO) ☐ Lack of interaction between DPO/COP and top management ☐ Lack of interaction between DPO/COP and functional units ☐ Communication from the DPO/COP is largely ignored ☐ No continuing education program for the DPO/COP

Pillar 2: Know Your Risks: Conduct a Privacy Impact Assessment (PIA)

Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

Know the risks represented by the processing to the rights and freedoms of data subjects	Data processing controls do not take into account the risks to the rights and freedoms of data subjects
☐ Up-to-date organizational inventory of processes that handle personal data, including the list of process owners ☐ PIAs have been conducted, and are owned and kept up-to-date by the process owner ☐ Stakeholders (those involved in the information life cycle) have been consulted as part of the PIA process ☐ PIA includes a privacy risk map, a list of controls, an implementation plan, and a monitoring/evaluation milestone	☐ No PIAs ☐ Process owners do not "own" the PIAs ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process ☐ Stakeholders are not consulted for the PIA ☐ Controls identified during the PIA are not implemented

Pillar 3: Write Your Plan: Create Your Privacy Management Program (PMP)

Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

Processing of data is according to privacy principles of transparency, legitimate purpose, and proportionality	Data processing not according to privacy principles of transparency, legitimate purpose, and proportionality
☐ Personal data is processed as per Sections 12 and 13 of the DPA ☐ Privacy principles are embedded into HR, Marketing, Operations, Security, and IT policies, are cascaded throughout the organization, and are updated as needed ☐ Data handlers have security clearance and privacy training ☐ Privacy notices are posted where appropriate (e.g. on website) ☐ Data sharing agreements are in place ☐ Tools in place to monitor compliance of the organization ☐ Records of data processing are maintained	☐ Processing fails to meet the criteria for lawful processing of personal data ☐ No privacy policy ☐ Privacy policy exists, but is not cascaded throughout the organization ☐ No privacy training or security clearance for data handlers ☐ Data is being shared without data sharing agreements ☐ No records of data processing

Pillar 1: Commit to Comply:
Appoint a Data Protection Officer (DPO)

Legal Basis: Sec. 21 of the DPA, Section 50 of the IRR, Circular 16-01, and Advisory 17-01

Appoint an individual accountable for compliance

Ineffective data protection governance

- ☐ No DPO or COP (in which case CEO or HoA is the default DPO)
- ☐ Lack of interaction between DPO/COP and top management
- ☐ Lack of interaction between DPO/COP and functional units
- ☐ Communication from the DPO/COP is largely ignored
- ☐ No continuing education program for the DPO/COP

Pillar 2: Know Your Risks:
Conduct a Privacy Impact Assessment (PIA)

Legal Basis: Sec. 20(c) of the DPA, Section 29 of the IRR, Advisory 17-03

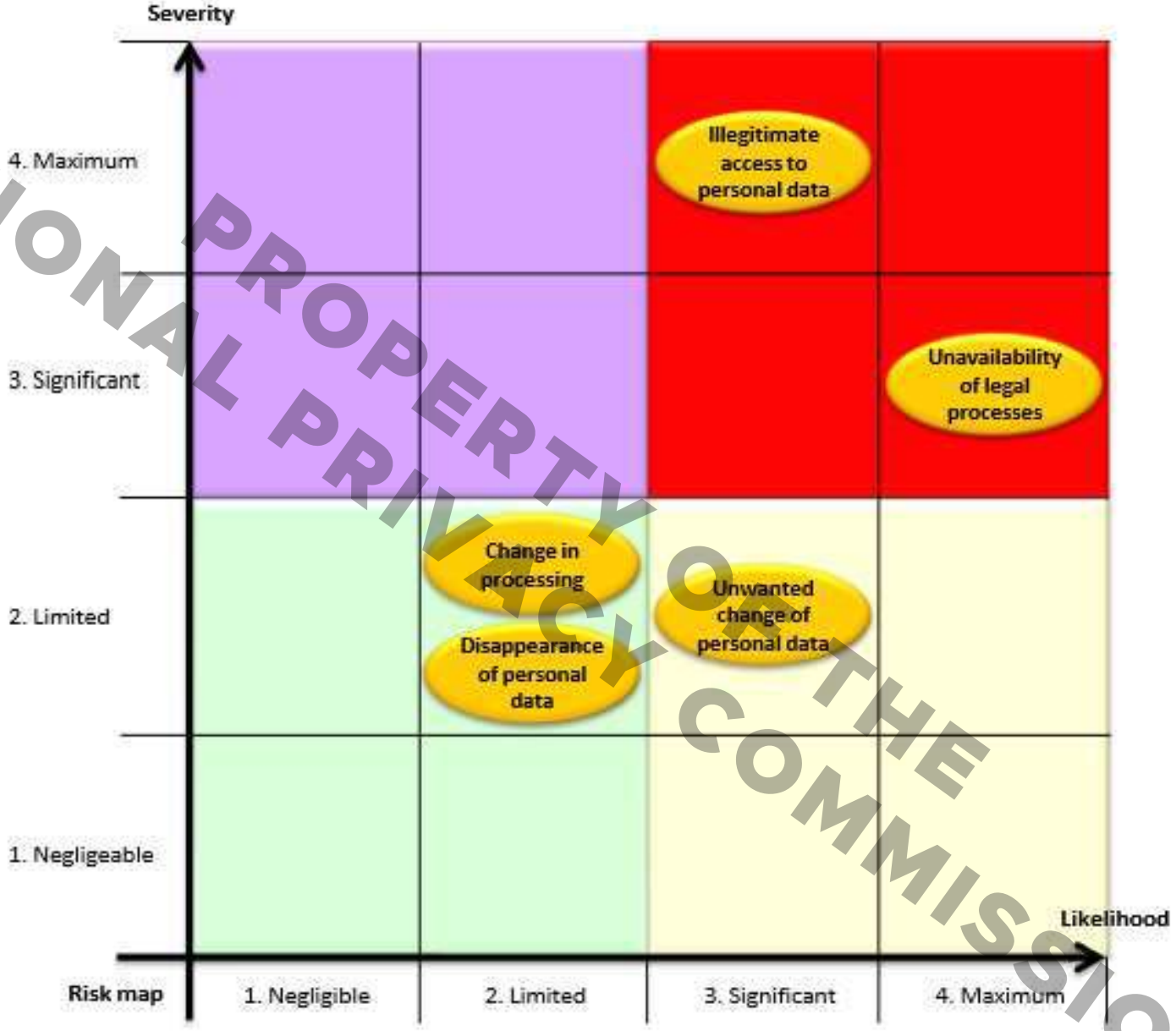
Know the risks represented by the processing to the rights and freedoms of data subjects

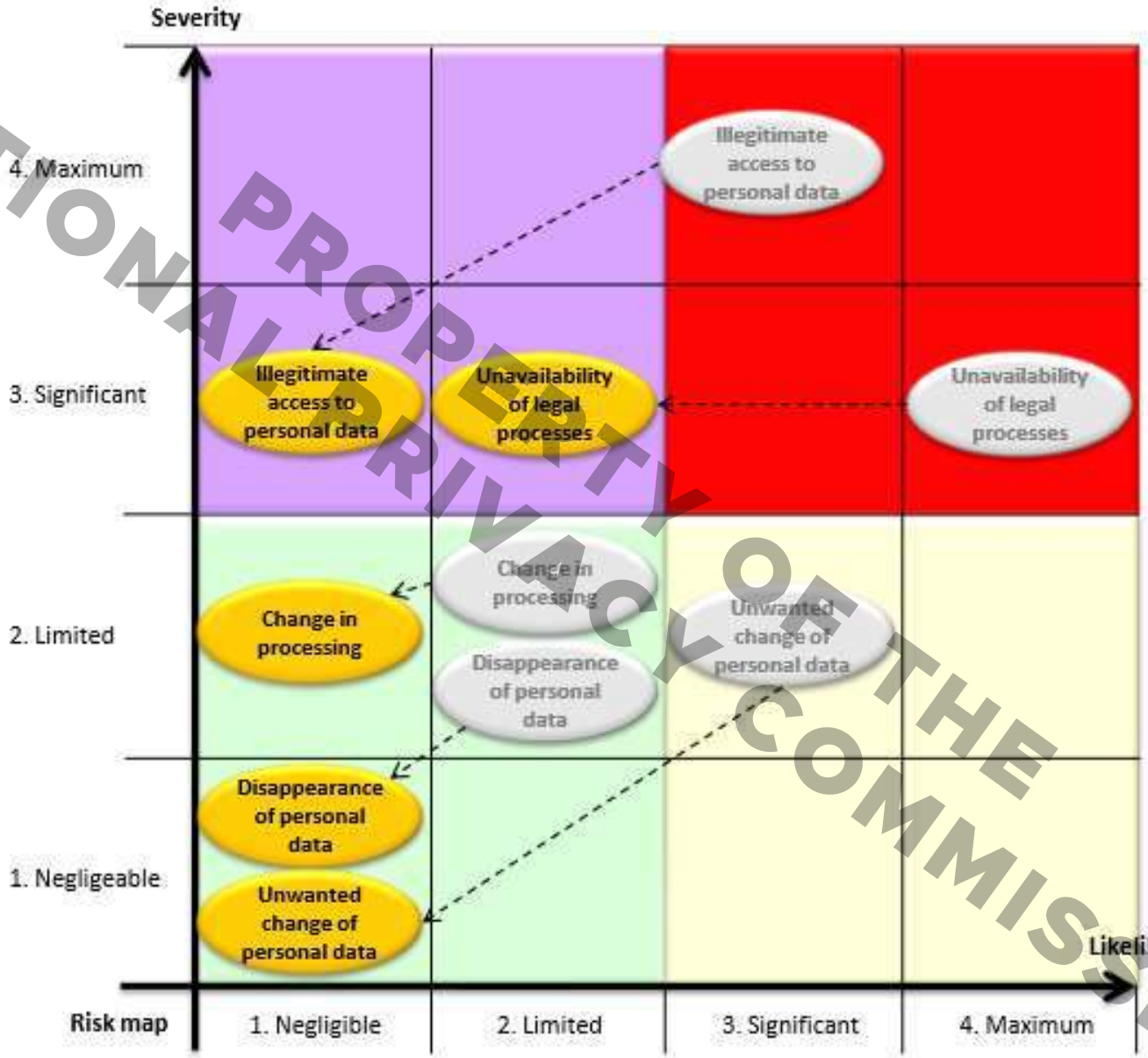
Data processing controls do not take into account the risks to the rights and freedoms of data subjects

- ☐ No PIAs
- ☐ Process owners do not "own" the PIAs
- ☐ PIAs are not updated when changes are made to the process, or to the technologies being used in the process
- ☐ Stakeholders are not consulted for the PIA
- ☐ Controls identified during the PIA are not implemented

PIA Components

- Ownership
- Stakeholder Involvement
- Privacy Risk Map
- Controls/Measures Framework
- Sign-off
- Implementation Plan





Pillar 3: Write Your Plan:
Create Your Privacy Management Program

Legal Basis: Sec. 11-15 of the DPA, Sections 21-23 and 43-45 of the IRR, Circulars 16-01 and 16-02

Processing of data is according to privacy principles of transparency, leg

Data processing not according to privacy principles of transparency, legitimate purpose, and proportionality

- ☐ Processing fails to meet the criteria for lawful processing of personal data
- ☐ No privacy policy
- ☐ Privacy policy exists, but is not cascaded throughout the organization
- ☐ No privacy training or security clearance for data handlers
- ☐ Data is being shared without data sharing agreements
- ☐ No records of data processing

Pillar 4: Be Accountable: Implement your Privacy & Data Protection (PDP) Measures

Upholding the rights of data subjects	Neglecting the rights of data subjects
☐ Data subjects are apprised of their rights through a privacy notice ☐ Consent is obtained prior to the collection and processing of data ☐ Data subjects are provided a means to access their data ☐ Data subjects are provided a venue to correct/rectify their data ☐ Data subjects know who to complain to if their rights are violated ☐ Complaints are acted upon quickly (within 30 days) ☐ These rights are upheld when invoked by the lawful heirs or assigns of the data subject	☐ No privacy notice when collecting personal data ☐ Consent is not obtained prior to the collection/processing of data ☐ No venue for data subjects to access their data ☐ No venue for data subjects to correct/rectify their data ☐ No contact details on how to lodge a complaint ☐ Complaints take a long time to be remedied ☐ Inaction on complaints from data subjects ☐ Overcollection of personal data

Maintaining confidentiality, integrity, and availability	Insufficient controls to maintain confidentiality, integrity, and availability
☐ Data protection risks have been identified and documented ☐ Appropriate and up-to-date organizational, physical, and technical controls are in place to manage these risks (e.g ISO:IEC 27002) ☐ Data protection policies are cascaded throughout the organization and updated as needed ☐ Vulnerability scanning is conducted at least once a year ☐ Business continuity drills are conducted at least once a year ☐ For data stored outside the Philippines, location of foreign country is defined ☐ For personal data stored in the cloud, NPC recommends that provider is ISO:IEC 27018 compliant (from Circular 16-01) ☐ For digitized personal data, NPC recommends 256-bit AES for data at rest and in transit (from Circular 16-01)	☐ Controls for data protection are not appropriate for the risks identified ☐ Controls for data protection are not updated for new risks/threats ☐ Controls for data protection are not complied with ☐ Cyber-hygiene practices are lax ☐ Business continuity drill has not been conducted in the last 12 months ☐ Security vulnerability scanning has not been conducted in the last 12 months

Remember: CIA

- SEC. 20 (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

- Guard against: Destruction, Alteration, Disclosure
- Objective/Goal: Availability, Integrity, Confidentiality (CIA)

- Measures: Organizational, Physical, Technical

Pillar 5: Be Prepared: Regularly exercise your Breach Reporting Procedures

Legal Basis: Sec. 20.f and 30 of the DPA, Sections 38-42 and 57 of the IRR, Circular 16-03

Able to report breach within 72 hours

Unable/unwilling to report breach within 72 hours

- ☐ No breach response team
- ☐ No breach response policy or procedures
- ☐ Breach drill has not been conducted in the last 12 months
- ☐ No notification of the NPC within 72 hours of discovery of a breach of personal data (possible criminal offense)

Pillar 6: Registration

Legal Basis: Circular 17-01

Sec. 24 of the DPA, and Sections 33 and 46-49 of the IRR, Circular 17-01

Register with the NPC	Non-registration with the NPC
☐ Registration with the NPC is up-to-date and contains all necessary compliance documentation ☐ Registration of all automated processing operations that have legal effect on the data subject ☐ Annual report summarizing documented security incidents and personal data breaches ☐ Service providers are also registered	☐ No registration (must be renewed annually) ☐ Out-of-date registration (must be updated within two months of any change) ☐ Non-reporting to NPC of documented security incidents and personal data breaches

Sec. 14 of the DPA, Sections 43-45 of the IRR, Circular 17-01

Service providers agree to honor their compliance obligations	Service providers in default of their compliance obligations
☐ All service providers are contractually bound to comply with the DPA, the IRR, and NPC issuances	☐ Service providers are not honoring their compliance obligations (includes registering with the NPC)

Registration Deadlines

NOTE on Registration (from Circular 17-01):

PIC or PIP shall provide the following registration information to the NPC by Sept. 9, 2017:

name and contact details of the PIC or PIP, head of agency or organization, and DPO.

PIC or PIP shall provide the following registration information to the NPC by March 8, 2018:

A. purpose or mandate of the government agency or private entity;
B. identification of all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;
C. attestation regarding certifications attained by the PIC or PIP, including its relevant personnel, that are related to personal data processing;
D. brief description of data processing system or systems:
    a. name of the system;
    b. purpose or purposes of the processing;
    c. whether processing is being done as a PIC, PIP, or both;
    d. whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
    e. description of the category or categories of data subjects, and their personal data or categories thereof;
    f. recipients or categories of recipients to whom the personal data might be disclosed; and
    g. whether personal data is transferred outside of the Philippines;
E. notification regarding any automated decision-making operation.

Thank you!

For your compliance.

DP 6

NATIONAL PRIVACY COMMISSION