DP 17

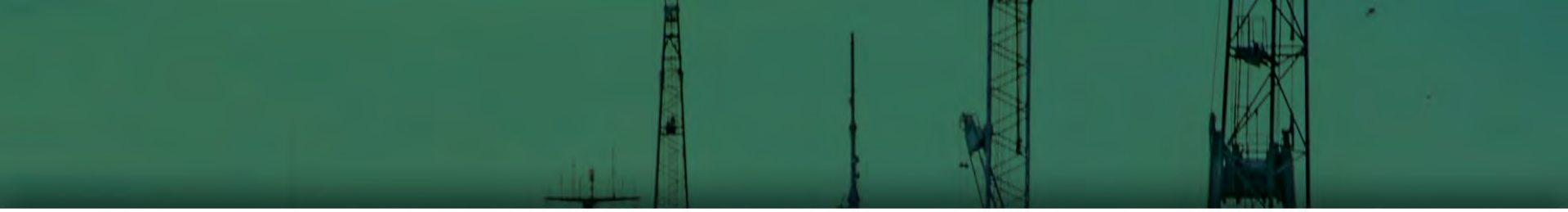
FOR MARITIME SECTOR

BREACH MANAGEMENT AND REPORTING

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

VIDA ZORA G. BOCAR, CIPM

Compliance and Monitoring Division



DP 17

FOR MARITIME SECTOR

WHAT IS A DATA BREACH?

Sec. 3 (k), (s), IRR, R.A. 10173
Sec. 3, NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DEFINITIONS

Security Incident

A **security incident** is:

- An event or occurrence that **affects or tends to affect** data protection; or
- An incident that compromises the **availability, integrity, or confidentiality** of personal data.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DEFINITIONS

Data Breach

A **data breach** is a **security incident** that:

- Leads to **accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of or unauthorized processing** of personal data
- Compromises the **availability, integrity,** or **confidentiality** of personal data

PROPERTY OF THE NATIONAL

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

9,040,592,509

ONLY **4%** of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY

5,378,104

Records

EVERY HOUR

224,088

Records

EVERY MINUTE

3,735

Records

EVERY SECOND

62

Records

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17
FOR MARITIME SECTOR

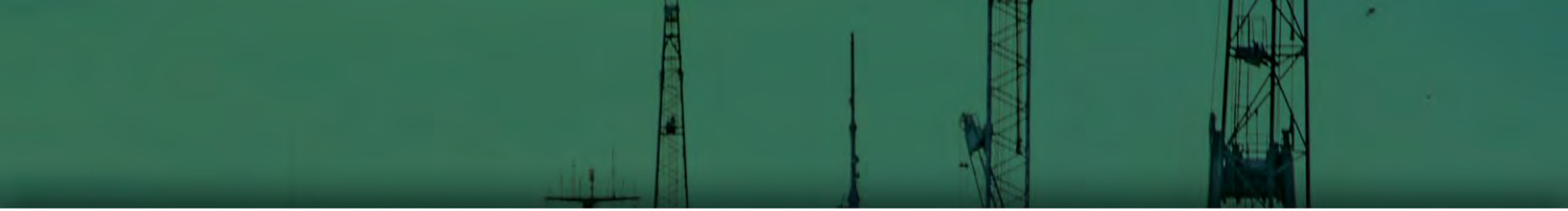
MARITIME CYBERSECURITY

DP 17 FOR MARITIME SECTOR

The recent NotPetya malware attack, which affected Maersk in the shipping sector as well as a large number of other firms, has served as a wake up call to the maritime industry. Cyber security isn't something that just affects land-based businesses; it can have a major impact on maritime operations, too.
There are currently a number of organisations conducting research into preparedness and resilience in order to gain a better overall picture of the current level of security in the maritime industry.

THE NATIONAL PRIVACY COMMISSION

http://www.marsecreview.com/2017/08/maritime-cyber-security-2/



DP 17

FOR MARITIME SECTOR

HOW TO HANDLE DATA BREACHES

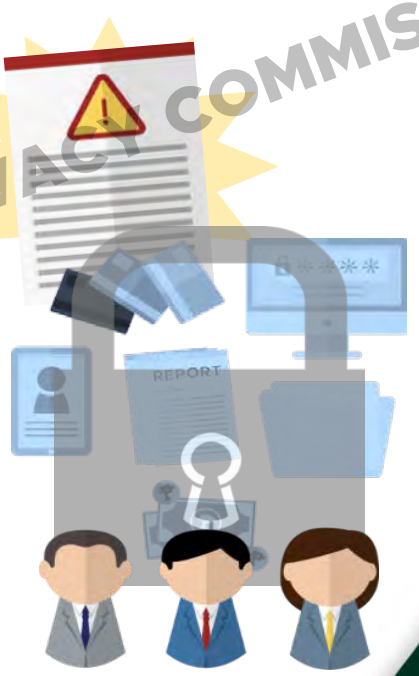
Sec. 20, R.A. 10173

RULE IV, Secs. 8-9, NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

SECURITY INCIDENT MANAGEMENT POLICY

A **security incident management policy** is implemented by the Personal Information Controller or Processor for the purpose of managing security incidents, including personal data breaches.



PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REQUIREMENTS

Every **Personal Information Controller** or **Processor** should have policies and procedures for:

1. The creation of a **data breach response team**

2. Implementation of **security measures and privacy policies**

3. Implementation of an **incident response procedure**

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REQUIREMENTS

4. **Mitigation of possible harm and other negative consequences** of a data breach
5. Compliance with the Data Privacy Act and other data protection laws and regulations

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DATA BREACH RESPONSE TEAM

The data breach response team must have at least **one member** with the authority to make immediate decisions on critical actions.

The team shall be responsible for:

- Compliance with the **security incident management policy**
- **Management** of security incidents and personal data breaches
- Compliance with the **data privacy law and other issuances**

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

*This may be outsourced by the Personal Information Controller or Processor

IMPLEMENTATION OF SECURITY MEASURES AND PRIVACY POLICIES

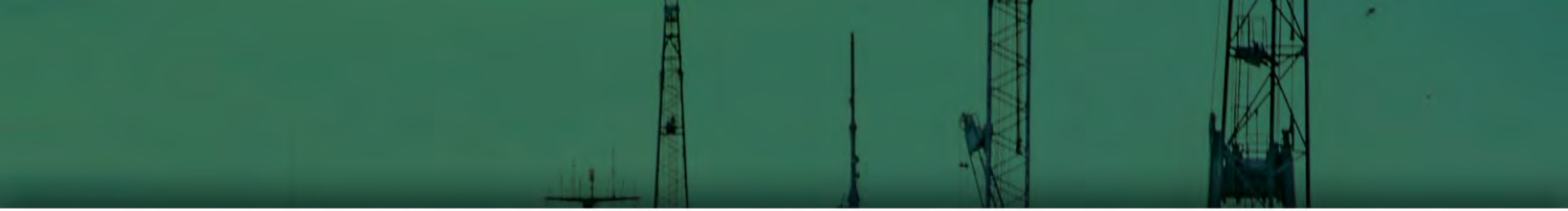
Recommended best practices in personal data breach prevention:

1. Regularly conduct a privacy impact assessment
2. Have a working data governance policy
3. Implement security measures
4. Make sure personnel are trained
5. Regularly review policies and procedures
6. Be aware of threats

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17
FOR MARITIME SECTOR



DP 17

FOR MARITIME SECTOR

MANDATORY NOTIFICATION

Sec. 20, R.A. 10173
Rule V, Sec. 11, NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REQUISITES

Notification of a data breach is **mandatory** when:

1. The personal data involves a. **sensitive personal information** or b. any other information that **may be used to enable identity fraud.**
2. There is reason to believe that the information may have been **acquired by an unauthorized person**; and
3. The unauthorized acquisition is likely to give **rise to a real risk of serious harm** to any affected data subject.

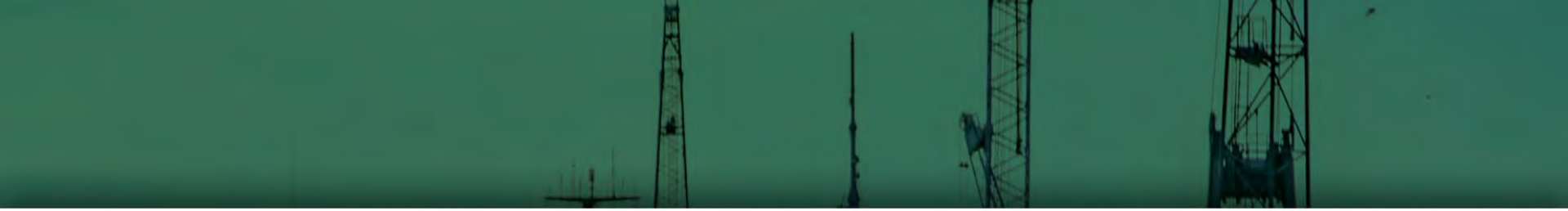
PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17

REQUISITES

All three elements must be present!

PROPERTY OF THE NATIONAL PRIVACY COMMISSION



DP 17

FOR MARITIME SECTOR

NOTIFICATION REQUIREMENTS

Rule IX, Secs. 38-42, IRR, R.A. 10173
Rule V, Secs. 15-18, 23 NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

WHO SHOULD NOTIFY?

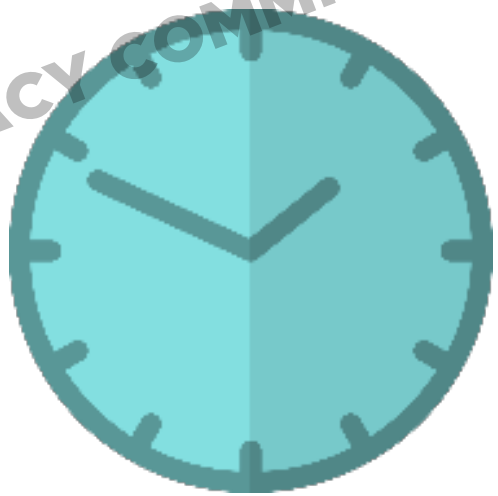
The **Personal Information Controller** through the data breach response team.

Note: The obligation to notify remains with the Personal Information Controller even if the processing of information is outsourced or subcontracted to a Personal Information Processor.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

WHEN SHOULD WE NOTIFY?

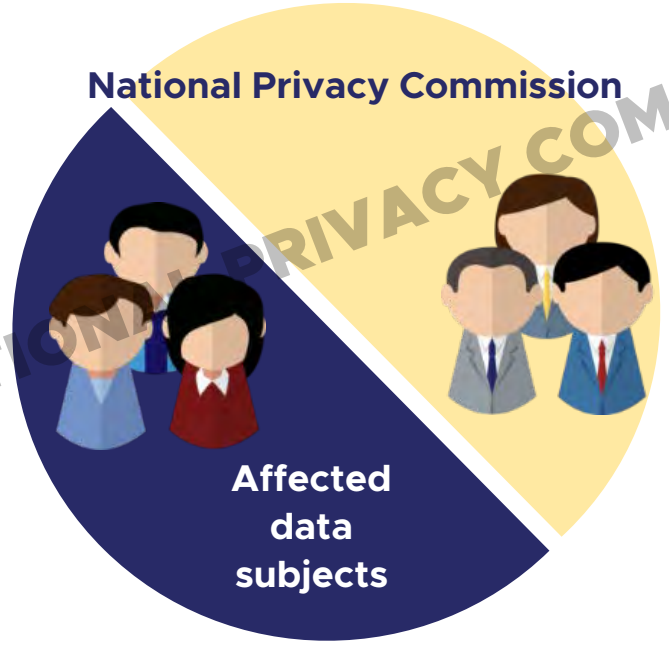
The notification must be made within 72 hours **upon knowledge of**, or when there is **reasonable belief** that a personal data breach has occurred.



PROPERTY OF THE NATIONAL PRIVACY COMMISSION

WHO SHOULD BE NOTIFIED?

Notification must be made to the **Commission** and to any **affected data subjects.**



PROPERTY OF THE NATIONAL PRIVACY COMMISSION

HOW DO WE NOTIFY NPC?

Notification to the Commission may be done through e-mail at complaints@privacy.gov.ph or through **delivering a hard copy to the NPC office.**

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

Upon receipt of the notification, the Commission shall send a confirmation message/e-mail to the Personal Information Controller.

HOW TO NOTIFY DATA SUBJECTS

Notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

May be supplemented with additional information at a later stage on the basis of further investigation.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

HOW TO NOTIFY DATA SUBJECTS

Notification to affected data subjects may be done **electronically** or ***in* written form**, but must be done individually.

The notification must not involve a further, unnecessary disclosure of personal data.

If individual notice takes disproportional effort, NPC authorization is required for alternative means.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

CONTENTS OF NOTICE

- Nature of the Breach

- Personal Data Possibly Involved

- Remedial Measures to Address Breach

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

NATURE OF THE BREACH

- Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach
- Chronology of the events leading up to the loss of control over the personal data
- Approximate number of data subjects or records involved

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

NATURE OF THE BREACH

- Description or nature of the personal data breach
- Description of the likely consequences of the personal data breach
- Name and contact details of the data protection or compliance officer or any other accountable persons.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

PERSONAL DATA POSSIBLY INVOLVED

- Description of sensitive personal information involved
- Description of other information involved that may be used to enable identity fraud

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REMEDIAL MEASURES

- Description of the measures taken or proposed to be taken to address the breach

- Actions being taken to secure or recover the personal data that were compromised

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REMEDIAL MEASURES

- Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

REMEDIAL MEASURES

- Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification
- The measures being taken to prevent a recurrence of the incident.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

FULL REPORT!

The full report of the personal data breach must be submitted within **five (5) days**, unless the Personal Information Controller is granted additional time by the Commission to comply.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

ADVISORY 2018-02 TEMPLATE OF MANDATORY NOTIFICATION FOR PERSONAL DATA BREACH FOR NPC

ANNEX C

Mandatory Notification: Personal Data Breach for the National Privacy Commission

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<PRIVACY COMMISSIONER>
National Privacy Commission
Pasay City, Metro Manila
Philippines

Subject: <DATA BREACH> dated <DATE> of <DATABASE>
<NPC REGISTRATION NO.>

Gentlemen:

I write in behalf of <ENTITY>, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of <ENTITY>, and the responsible persons thereof, are as follows:

Head of the Organization	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Data Protection Officer	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
Process Owner	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- *Describe the nature of the personal data breach.*
  - *Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.*

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17

ADVISORY 2018-02 TEMPLATE OF MANDATORY NOTIFICATION FOR PERSONAL DATA BREACH FOR NPC

- *Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.*
- *Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.*
- *Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.*
- *Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.*
- *Describe the likely consequences of the personal data breach.* ***Consider effect on company or agency, data subjects and public.***

Personal Data Possibly Involved.

- *List all sensitive personal information involved, and the form in which they are stored or contained.*
- *Also list all other information involved that may be used to enable identity fraud.*

Measures taken to Address the Breach.

- Describe in full the measures that were taken or proposed to be taken to address the breach.
- Describe how effective these measures are.
- Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.
- Indicate actions of the organization to minimize/mitigate the effect on the affected individual. Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
- Indicate of the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.
- Describe the steps the organization has taken to prevent a recurrence of the incident.

Should you require further information on this matter, contact us using the information above. Any information that later becomes available shall be reported within five (5) days, or as further required by the Commission.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17

ADVISORY 2018-02 TEMPLATE OF MANDATORY NOTIFICATION FOR PERSONAL DATA BREACH FOR NPC

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

ANNEX D

Mandatory Personal Data Breach Notification to Data Subjects

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<DATA SUBJECT>
<ADDRESS>

Subject: <DATA BREACH> dated <DATE>
<NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>

Nature of the Breach

- *Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.*
- *Describe the likely consequences of the personal data breach.*

Measures taken to Address the Breach.

- **Provide information on** *measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.*
- *Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.*
- *Describe steps the organization has taken prevent a recurrence of the incident.*

Measures taken to reduce the harm or negative consequences of the breach.

- **Describe** *actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.*

Assistance to be provided to the affected data subjects.

- **Include information on** *any assistance to be given to affected individuals.*

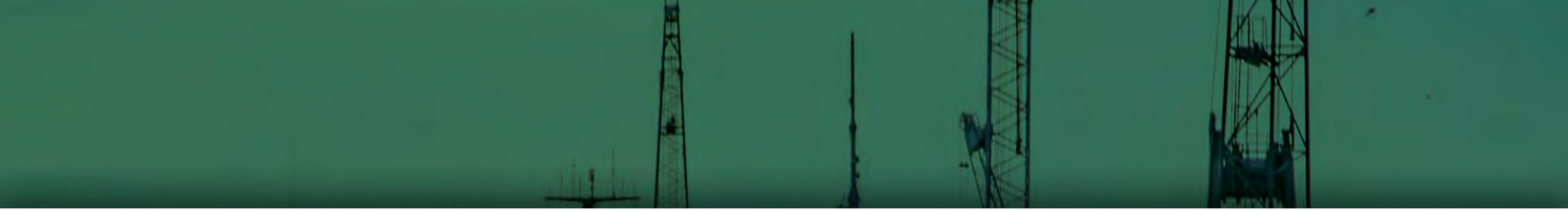
Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer <DATA PROTECTION OFFICER>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFORMATION>

We undertake to provide more information to you as soon as they become available.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>



DP 17

FOR MARITIME SECTOR

CONCEALMENT OR FAILURE TO DISCLOSE DATA BREACH

Sec. 30, R.A. 10173

Sec. 57, IRR, R.A. 10173

Sec. 20, NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

CONCEALMENT OF BREACH

An intention to conceal is presumed if the Commission does not receive notification from the personal information controller within five (5) days from knowledge of or upon a reasonable belief that a security breach occurred.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

PUNISHABLE ACT

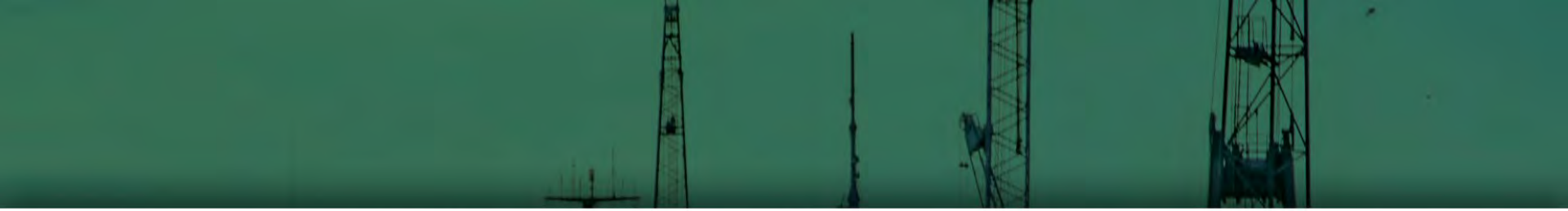
Concealment Is a crime!

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

Imprisonment from 1 year and 6 months to 5 years plus fine from ₱500,000 to ₱1,000,000

Imposed on persons who:

- After having knowledge of a security breach and of the obligation to notify the National Privacy Commission
- Either intentionally or by omission conceals the fact of such breach



DP 17

FOR MARITIME SECTOR

ANNUAL REPORT

Sec. 22, NPC Circular 16-03

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

SUBMISSION

Any or all reports shall be made available when requested by the Commission.

A summary of all reports shall be submitted to the Commission annually.*

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

***Deadline is on June 30, 2018**

DP 17

CONTENTS

In the event of a security incident amounting to a data breach, the report must include:

- The facts surrounding the incident
- The effects of the incident
- Remedial action taken by the PIC

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

CONTENTS

All security incidents and personal data breaches shall be documented.

Aggregated data for security incidents not involving a personal data breach suffices.

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

CONTENTS

The report must contain general information:

- The number of incidents and breaches encountered
- The classification of data breaches according to their impact on the availability, integrity, or confidentiality of personal data

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

ANNEX A

Annual Security Incident Reports for PICs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____ **City/Municipality:** _____ **Province:** _____

PIC (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION CONTROLLER

A. Personal Data Breach, Mandatory Notification	<#>
B. Personal Data Breach, not covered by mandatory notification requirements	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occured

Types	*Number*	Types	*Number*
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

Personal Data Breaches

	Confidentiality	Integrity	Availability
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO .: _____

DATE : _____

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

ANNEX B

Annual Security Incident Reports for PIPs

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____ City/Municipality: _____ Province: _____

PIP (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION PROCESSOR

This form applies to personal data processing performed on behalf of PICs

A. Personal Data Breaches, reported to PICs	<#>
B. Personal Data Breaches, not reported to PICs	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occured

Types	*Number*	Types	*Number*
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO.: _____

DATE : _____

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

IN CONCLUSION

DP 17 FOR MARITIME SECTOR

- Notifications are mandatory only for a specific form of confidentiality breach.
- There are two kinds of notifications:
  - Notification to the data subject
  - Notification to the NPC
- These notifications must be made within 72 hours of knowledge of a mandatory data breach has occurred.
- Failure to comply with the notification requirement can lead to criminal penalties.
- Deadline of the annual breach report is on June 30, 2018

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

DP 17

FOR MARITIME SECTOR

Thank you!

PROPERTY OF THE NATIONAL PRIVACY COMMISSION