NATIONAL PRIVACY COMMISSION

mcpi
MICROFINANCE COUNCIL OF THE PHILIPPINES, INC.

Understanding Data Privacy for Financial Institutions

Microfinance Council of the Philippines, Inc.

July 27, 2018

Dr. Rolando R. Lansigan, CEH, CHFI, SySA+

Introduction

- Microfinancial institutions and service providers to the financial industry process a huge amount of personal data on a daily basis. Much of the data processed is highly confidential and sensitive, like health records and other financial information of the clients.

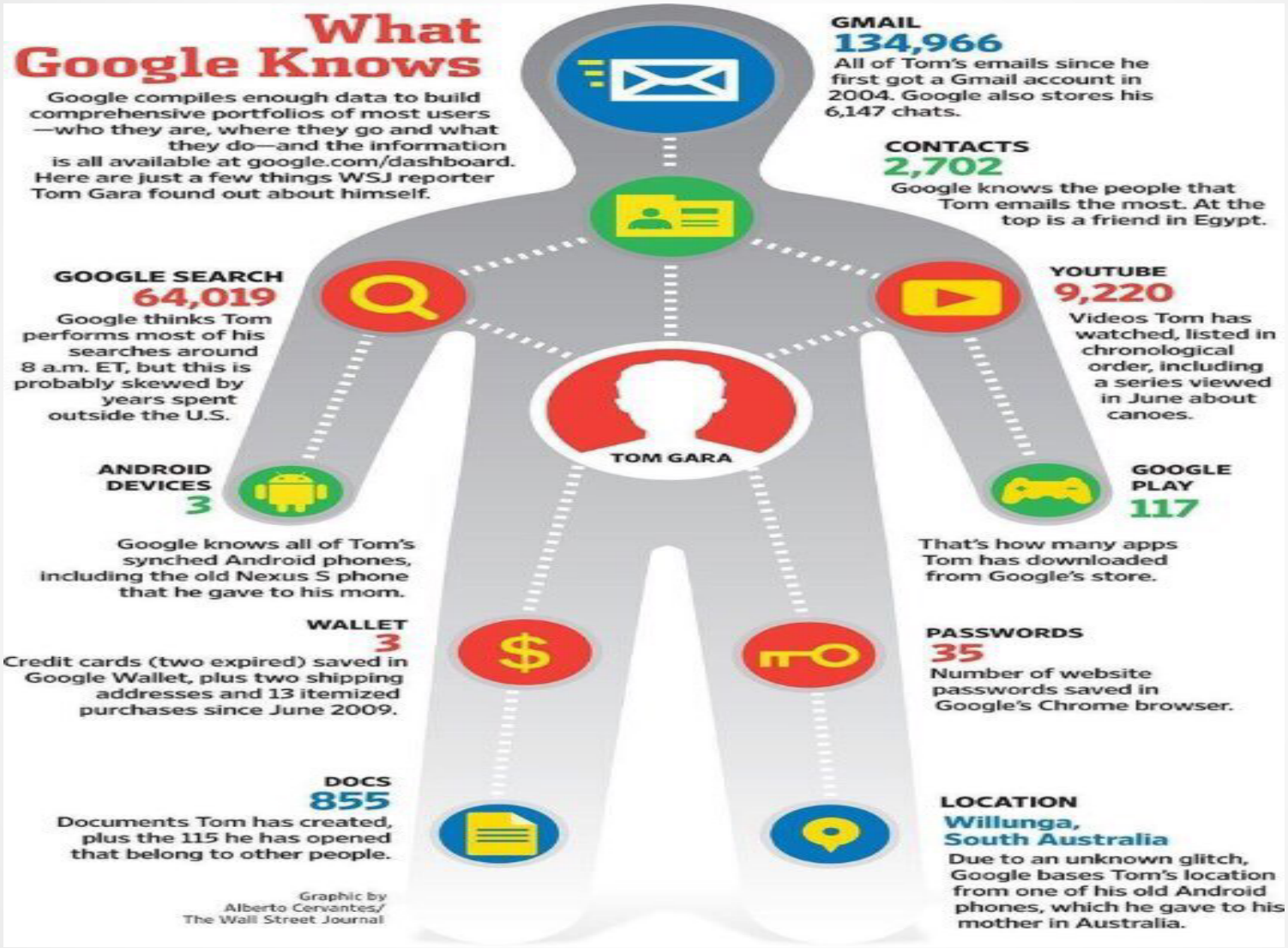
- This means there are high risks and a likelihood of being the target of cybercriminals, hackers and other potential breach.

- And in this case, the high probability of being checked and investigated by the concerned government agencies. That may eventually be charged of criminal liability under existing laws and some reputational concerns.

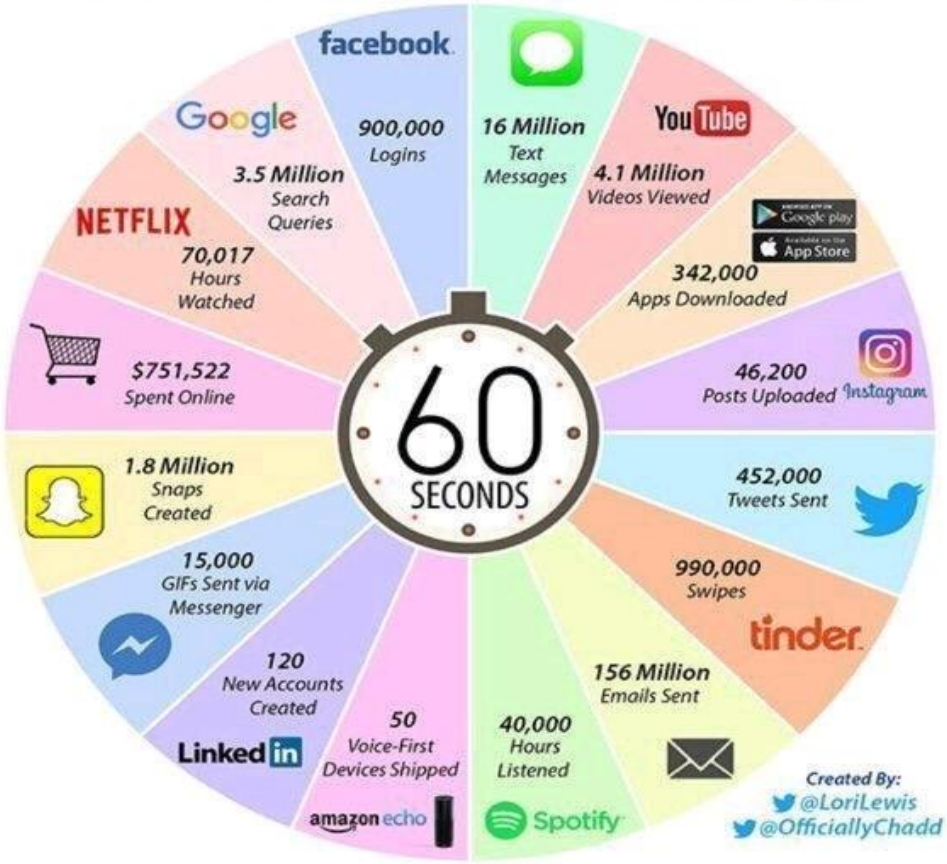
Do not COLLECT if you cannot PROTECT

ВОТРА

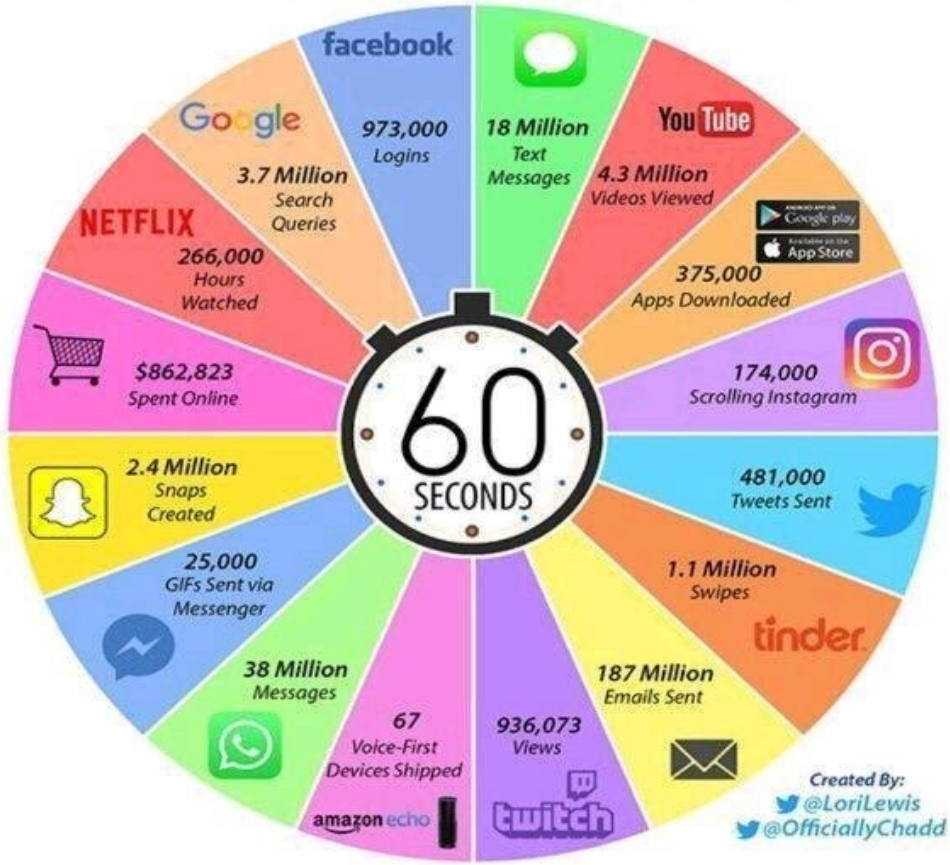
Who stores data about you?


What Google Knows
Google compiles enough data to build comprehensive portfolios of most users —who they are, where they go and what they do—and the information is all available at google.com/dashboard. Here are just a few things WSJ reporter Tom Gara found out about himself.
GMAIL
134,966
All of Tom's emails since he first got a Gmail account in 2004. Google also stores his 6,147 chats.
CONTACTS
2,702
Google knows the people that Tom emails the most. At the top is a friend in Egypt.
GOOGLE SEARCH
64,019
Google thinks Tom performs most of his searches around 8 a.m. ET, but this is probably skewed by years spent outside the U.S.
YOUTUBE
9,220
Videos Tom has watched, listed in chronological order, including a series viewed in June about canoes.
TOM GARA
ANDROID DEVICES
3
Google knows all of Tom's synched Android phones, including the old Nexus S phone that he gave to his mom.
GOOGLE PLAY
117
That's how many apps Tom has downloaded from Google's store.
WALLET
3
Credit cards (two expired) saved in Google Wallet, plus two shipping addresses and 13 itemized purchases since June 2009.
PASSWORDS
35
Number of website passwords saved in Google's Chrome browser.
DOCS
855
Documents Tom has created, plus the 115 he has opened that belong to other people.
LOCATION
Willunga, South Australia
Due to an unknown glitch, Google bases Tom's location from one of his old Android phones, which he gave to his mother in Australia.
Graphic by Alberto Cervantes/ The Wall Street Journal

2017 This Is What Happens In An Internet Minute



2018 This Is What Happens In An Internet Minute



Which is more valuable?

DATA

MONEY

What is the Data Privacy Act of 2012?

- SECTION 1. Short Title. – This Act shall be known as the "Data Privacy Act of 2012".

- Republic Act 10173, the Data Privacy Act of 2012

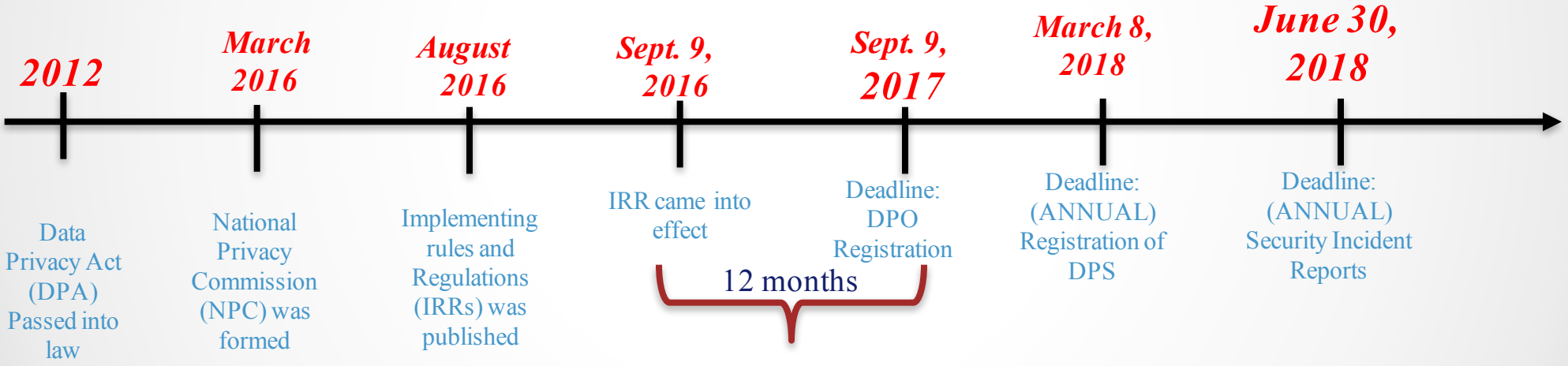
AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

- The National Privacy Commission (NPC) is a body that is mandated to administer and implement this law. The functions of the NPC include:
  - rule-making,
  - advisory,
  - public education,
  - compliance and monitoring,
  - investigations and complaints,
  - and enforcement.

Privacy Commissioner and Chairman
Honorable Raymund E. Liboro
Deputy Privacy Commissioners
Atty. Leandro Angelo Y. Aguirre
Atty. Ivy D. Patdu

- Office of the Commissioner
  - Office of the Executive Director
    - Public Information and Assistance Division
    - Data Security and Compliance Office
      - Compliance and Monitoring Division
      - Data Security and Technology Standards Division
    - Legal and Enforcement Office
      - Legal Division
      - Complaints and Investigation Division
      - Enforcement Division
    - Finance and Administrative Office
      - Financial Planning and Management Division
      - Administrative Services Division
      - Human Resource Development Division
    - Privacy Policy Office
      - Policy Development Division
      - Policy Review Division

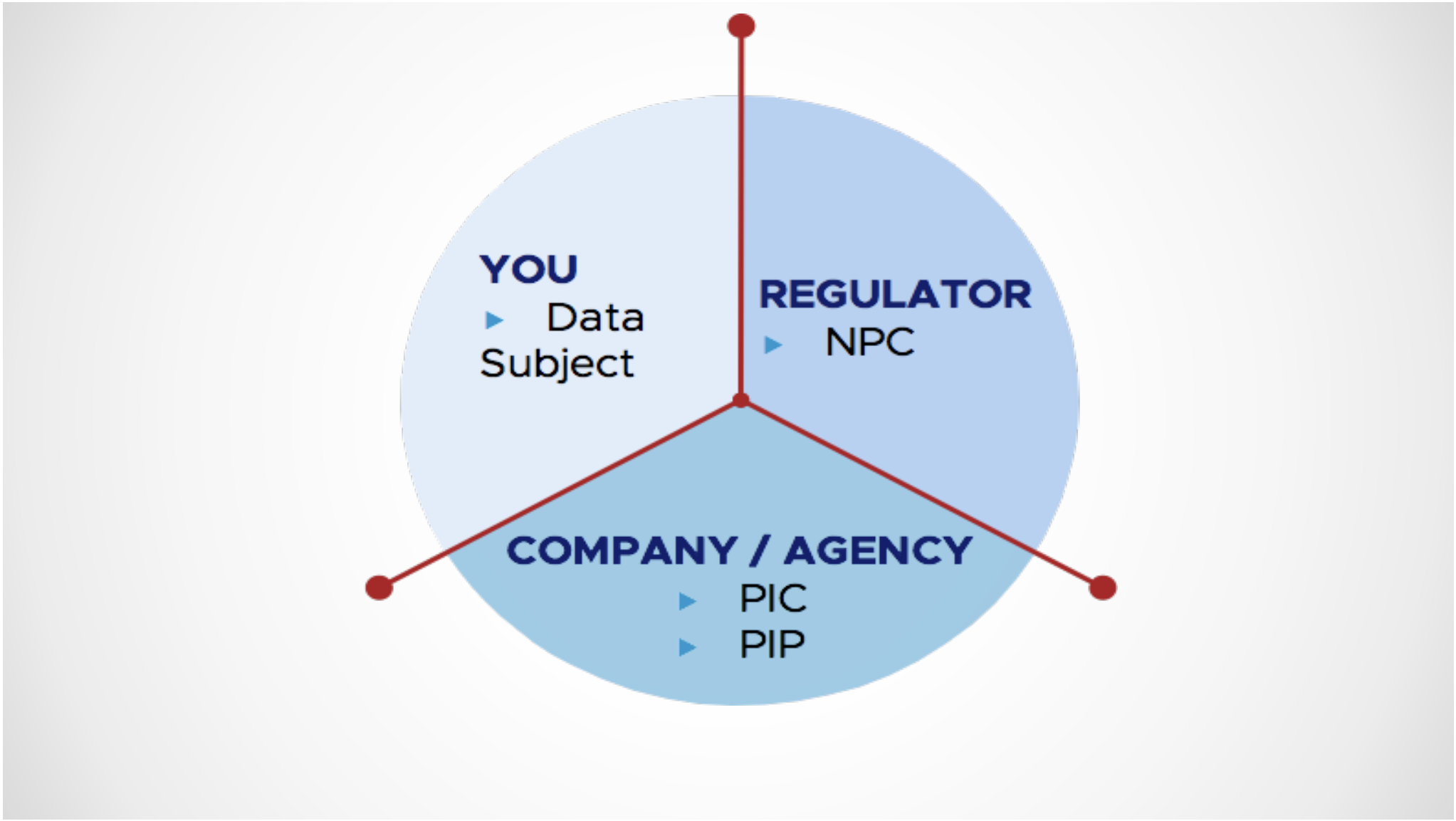
Timeline of DPA Law and other issuances passed to Organization's Compliance



Registration Requirements: All personal data processing systems (DPS) operating in the Philippines that involve Personal Data concerning at least 1,000 individuals/personal records must be registered with NPC

KEY ROLES IN THE DATA PRIVACY ACT

- **Data Subjects**
  - Refers to an individual whose, sensitive personal, or privileged information is processed personal
- **Personal Information Controller (PIC)**
  - Controls the processing of personal data, or instructs another to process personal data on its behalf.
- **Personal Information Processor (PIP)**
  - Organization or individual whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject
- **Data Protection Officer (DPO)**
  - Responsible for the overall management of compliance to DPA
- **National Privacy Commission**
  - Independent body mandated to administer and implement the DPA of 2012, and to monitor and ensure compliance of the country with international standards set for personal data protection


YOU
Data Subject
REGULATOR
NPC
COMPANY / AGENCY
PIC
PIP

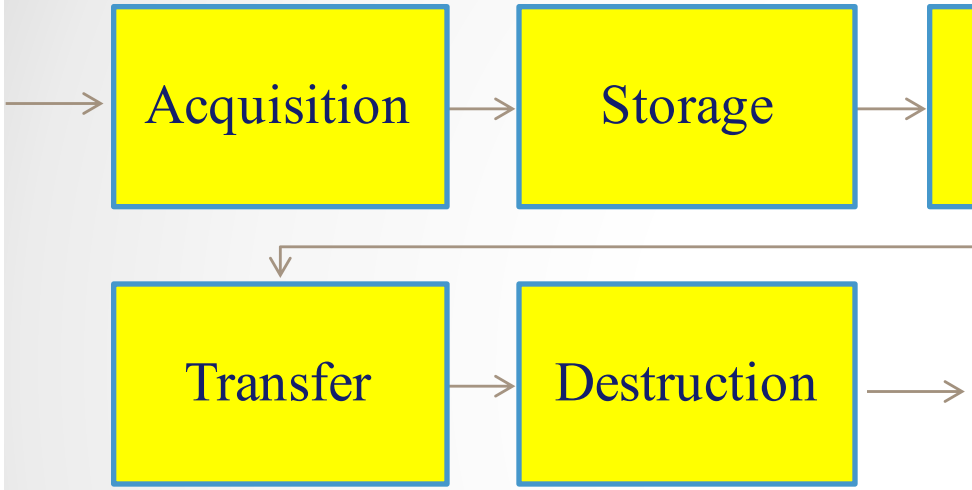
CLASSIFICATON OF PERSONALLY IDENTIFIABLE INFORMATION

PERSONAL INFORMATION	SENSITIVE PERSONAL INFORMATION (List based on IRR)	PRIVILEGED INFORMATION (List based on Rules of Court
Name	Race, Color and Ethnic origin	Data received within the context of a protected relationship – husband and wife
Address	Marital status	
Place of work	Age	
Telephone Number	Health	Data received within the context of a protected relationship – attorney and client
Gender	Philosophical affiliation	
Location of an individual at a particular time	Religious and Philosophical affiliation	Data received within the context of a protected relationship – priest and penitent
IP Address	Education	
Birthdate and Birthplace	Genetics and sexual life	
Country of citizenship	Proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings	Data received within the context of a protected relationship – doctor and patient
Payroll and benefits information		
Contact information		

CLASSIFICATON OF PERSONALLY IDENTIFIABLE INFORMATION

	SENSITIVE PERSONAL INFORMATION (List based on IRR)	
	Social Security Number	
	License or its denials, suspension or revocation	
	Tax returns	
	Other personal information issued by government agencies	
	Bank and credit/debit card numbers	
	Websites visited	
	Materials downloaded	
	Any other information reflecting preferences and behaviors of an individual	
	Grievance information	
	Discipline information	

Personal Data Lifecycle



Retention/Disposal should be based on:

1. **Law**
2. **Industry Best Practice**
3. **Business Needs**

- **Key considerations when listing your personal data:**
  - *What personal data do you collect?*
  - *In what form and through which channels?*
  - *For what purpose you collect personal data*
  - *How is it used?*
  - *Who is this data shared with internally and externally?*
  - *Who is authorized to access this data?*
  - *Where do you keep your data?*
  - *How long do you keep your data?*
  - *How do you dispose this data?*

EXAMPLES OF POTENTIAL BREACHES AND SECURITY INCIDENTS INVOLVING PERSONAL INFORMATION

- **Potential Breach**

1. Bank – consent form
2. Hospital and School Records – Storage and Disposal Policy
3. Student transferred by her Parents - Consent
4. Clinical record of a student to disclose with her parents - Consent
5. List of top students/passers - Consent
6. Known Fastfood delivery – disclosing personal info of clients – Unauthorized Disclosure / Intentional Breach
7. Cedula in Malls – Disposal Policy/Improper Disposal
8. Security issues in buildings – logbook
9. Use of re-cycled papers – Disposal Policy / Access due to negligence
10. Hard drives sold online –Disposal Policy
11. Use of USB – Encryption issue
12. Lost a CD in transit – Encryption issue
13. Personal laptop stolen – Encryption issue

- **Access Control and Security Policy**

14. Personal Records stolen from home of an employee - Security
15. Viewing of Student Records in Public – Physical Security
16. Raffle stubs – Privacy Notice / Storage and Disposal Policy
17. Universities and Colleges websites with weak authentication
18. Photocopiers re-sold without wiping the hard drives
19. Password hacked/revealed -
20. Accidentally sent an email attachment – Unauthorized Disclosure

- **Other Violations / Data Privacy Act Principles**

21. No Data Sharing Agreement (DSA)
22. No Privacy Notice
23. No Sub-contracting Agreement
24. No Breach Drill
25. Profiling of customers of malls – Targeted Marketing
26. Unjustifiable collection of personal data of a school – Principle of Proportionality

In the event of a data breach, we will not ask you how many millions you've spent on your hardware and IT experts.

We will, instead, ask whether you've implemented **NPC's five data privacy guidelines**.

PRIVACY COMMISSIONER AND CHAIRMAN RAYMUND E. LIBORO

Potential Penalties listed in the Data Privacy Act

DPA Section	Punishable Act	For Personal Information	For Sensitive Personal Information	Fine (Pesos)
		JAIL TERM		
25	Unauthorized processing	1-3 years	3-6 years	500 k – 4 million
26	Access due to negligence	1-3 years	3-6 years	500 k – 4 million
27	Improper disposal	6 months – 2 years	3-6 years	100 k – 1 million
28	Unauthorized purposes	18 months – 5 years	2-7 years	500 k – 2 million
29	Intentional breach	1-3 years		500 k – 2 million
30	Concealment of breach	18 months – 5 years		500 k – 1 million
31	Malicious disclosure	18 month – 5 years		500 k – 1 million
32	Unauthorized disclosure	1-3 years	3-5 years	500 k – 2 million
33	Combination of acts	1-3 years		1 million – 5 million

Rights of the Data Subject

- Right to be informed - IRR, Section 34.a
- Right to object - IRR, Section 34.b
- Right to access - IRR, Section 34.c
- Right to data portability - IRR, Section 36
- Right to correct (rectification) - IRR, Section 34.d
- Right to file a complaint - IRR, Section 34.a.2
- Right to damages - IRR, Section 34.f
- **Right to erasure or blocking - IRR, Section 34.e**
- **Transmissibility of Rights - IRR, Section 35**

Data Privacy Principles

- Transparency – "the CONSENT regime"
  - A 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.
- 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
- 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.

Avoid this mentality:
"just in case we need it"
"this is what we always do"

THE FIVE PILLARS OF COMPLIANCE

- Commit to Comply: Appoint a Data Protection Officer (**DPO**)
- Know your Risk: Conduct a Privacy Impact Assessment (**PIA**)
- Be Accountable: Create your Privacy Management Program and Privacy Manual (**PMP**)
- Demonstrate your Compliance: Implement your Privacy and Data Protection Measure (**PDP**)
- Be Prepared for Breach: Regularly Exercise your Breach Reporting Procedure (**BRP**)

Other Requirements

- Annual Breach Drill
- ❑ **Notification to NPC within 72 hours**
- ❑ **(in the event of a personal data breach)**
- Annual Breach Report
- Security Clearance
- Privacy Notice
- Data Sharing Agreement (DSA), if applicable
- Sub-contracting Agreement / Outsourcing Agreement

Consent of Data Subject

- Express and Specific
- Time-bound
- Documented
- Specifies the purpose
- Confirms data sharing

Privacy notice

- Facts of personal data processing: including automated decision-making and profiling
- Description of personal data
- Purpose(s) of processing
- Basis of processing (when consent is not required)
- Scope of method of processing
- Recipients to whom personal data may be disclosed
- Methods for automated access
- Identity and contact details of data controller
- Retention period of personal data
- Rights of the data subject

1 Technical

2 Organisational – other measures

BEST PRACTICE

Technical

Encryption

To what standard? (cost Vs benefit)

All devices or just some?

Passwords

Enforced strength and updates?

Sharing data

Technical solutions – e.g. via email; portals

Backups

Secure: encrypted tapes | cloud-provider

Auditable process

Access control

Who decides permissions and privileges ('need to know')?

Remote access

How delivered securely?

Permit Bring Your Own Device?

System testing & maintenance

Who has access, to what (System Administrators)

Live or dummy data?

Firewalls / Anti-virus / Spam filters

Organisational – physical security

Secure Office Storage

For removable devices **and** hardcopy information

- Identifying marks?
- Kensington locks?
- Locked print?
- Offsite?

Building access control

Secure premises – CCTV | locked windows | perimeter

Locked CCTV room | server room

ID badges, supervised visitors | contractors

Remote working

Secure both hardcopies and devices when in transit.

Kept out of sight: in transit | at home.

Lockable pedestals | Kensington locks?

Secure disposal

Shredding of hardcopies

Beyond use | Reuse | Resale

Organisational – other measures

Policy, procedures, guidance & training

Eliminate ambiguities

Clearly communicated, readily accessible and understood

Human Resources

Explicit roles and responsibilities in Job Descriptions and Terms of Reference

Terms and Conditions: confidentiality clauses

Clear expectations | reporting lines

Disciplinary process

Training records

Procurement (and contracts)

i.e. outsourced services like IT and software

Due diligence

Compliant contract Terms and Conditions:

- Act on your instructions
- Equivalent security

Auditing and monitoring

Recommended Security Measures

1. Shredding all confidential waste.
2. Using strong passwords.
3. Installing a firewall and virus checker on your computers.
4. Encrypting any personal information held electronically.
5. Disabling any 'auto-complete' settings.
6. Holding telephone calls in private areas.
7. Checking the security of storage systems.
8. Keeping devices under lock and key when not in use.
9. Not leaving papers and devices lying around.
10. Lock rooms containing confidential information when not in use.
11. Make sure employees don't write their passwords down.
12. Use swipe cards or keypads to access the office.
13. Use CCTV cameras to monitor your office space.
14. Shield keyboards when inputting passwords.
15. Install an alarm system.
16. Hide valuable equipment from view when not in the office.
17. Assign a limited number of trustworthy employees as key

RECOMMENDATION:

Holding Data and Keeping it Up-to-Date

- **Carry out an information audit at least annually.**
  - Write a letter at the start of each school year asking parents and students to check that their details are correct. This also helps prevent emergency risks, e.g. if an old address or phone number is on record.
  - Check that 'live' files are accurate and up to date.
  - Any time you become aware that information needs amending, do so immediately
  - Any personal data that is out of date or no longer needed should be 'destroyed'. This may involve shredding documents or deleting computer files securely so that they cannot be retrieved.
  - Schools must follow the disposal of records schedule. This schedule states how long certain types of personal data can be held for until it must be destroyed. Some stipulations are legal obligations while others are best practice.

You are violating the Data Privacy Act if you keep any data for longer than it is needed.

TOP FIVE KEY AREAS OF DATA PRIVACY ACT ON FINANCIAL INSTITUTIONS

- Client Consent
- Rights of the Data Subjects
- Breach Management
- Vendor Management
- Profiling
- Anonymization and Pseudonymisation

Recommendation in Preparation for Compliance to the Data Privacy Act of 2012

- Awareness
- Information you hold
- Communicating privacy information
- Individuals' rights
- Subject access requests
- Lawful basis for processing personal data
- Consent
- Data breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officer
- International

In Closing: How the NPC can help

Help in delivering the message to top management

-Generic guidance and frameworks (www.privacy.gov.ph)

-Updates on new standards and/or circulars (www.privacy.gov.ph)

When requested, advice on specific matters **(info@privacy.gov.ph)**

-Give advice on How to Comply (compliancesupport@privacy.gov.ph)

NATIONAL PRIVACY COMMISSION

"Compliance to Data Privacy Act is not a one-shot initiative. It is a discipline and culture that must be embedded on a continuous basis within the organization."

CULTURE OF PRIVACY in the PHILIPPINES

NATIONAL PRIVACY COMMISSION

Thank you!!!

For inquiries, email us at

info@privacy.gov.ph

rolando.lansigan@privacy.gov.ph