NATIONAL PRIVACY COMMISSION

Philippine Data Privacy Act of 2012

RA - 10173

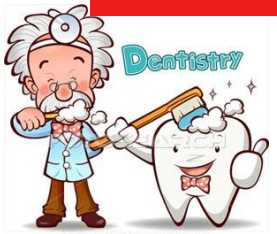
Do not COLLECT if you cannot PROTECT


© Hazel Thompson

Who stores data about you?

facebook

YouTube



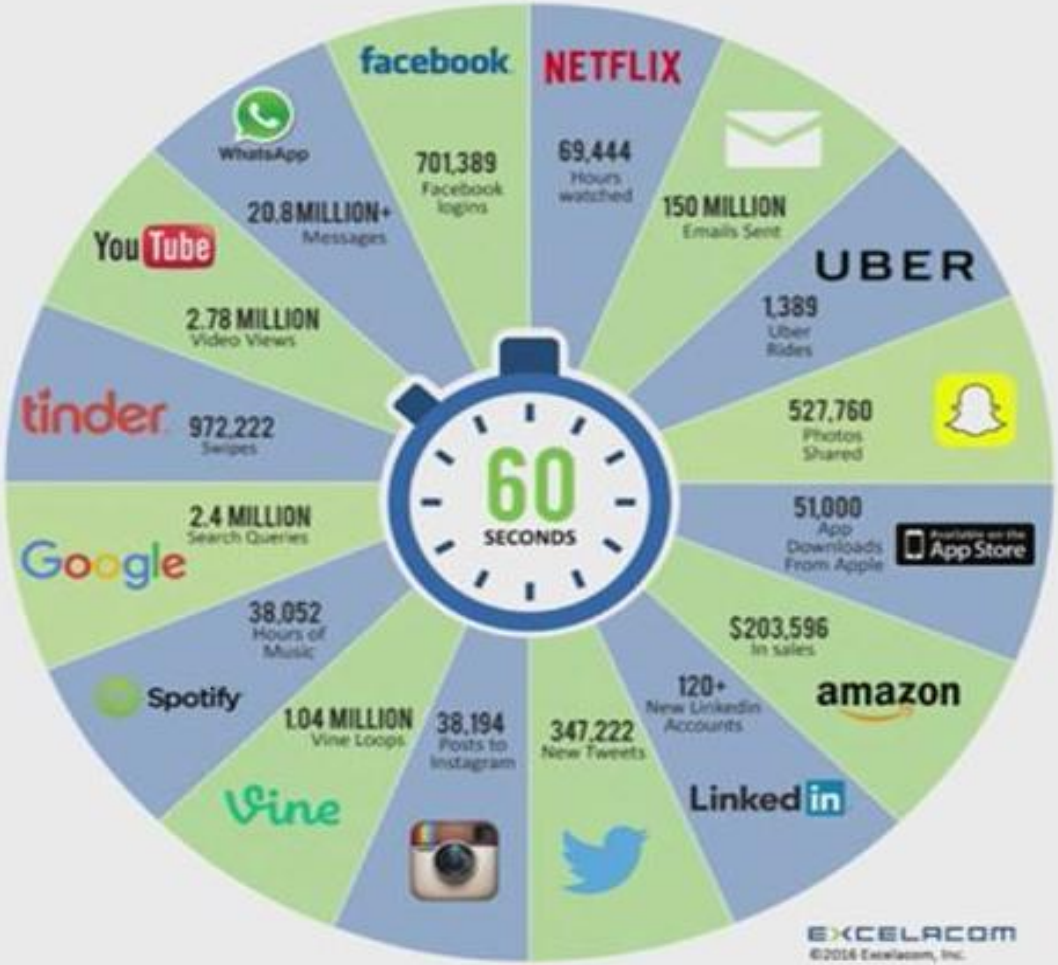
Google

powered by ebay.co.uk

HSBC

The world's local bank

SM



SPEED OF INFORMATION

Which is more valuable?

Data

Money

“Data is more valuable than Money. If someone takes your money, that's all they have. If you let someone take your data, they may eventually take your money too!“

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

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 erasure or blocking - IRR, Section 34.e
- Right to file a complaint - IRR, Section 34.a.2
- Right to damages - IRR, Section 34.f
- Transmissibility of Rights - IRR, Section 35

CLASSIFICATION OF PERSONAL DATA

Personal Information:

Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Sensitive Personal Information.

Refers to personal information about an individual's:

race, ethnic origin, marital status, age, color, religious, philosophical or political affiliations, health, education, genetics, sexual life, any proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings;

Also includes information issued by government agencies peculiar to an individual which includes, but not limited to:

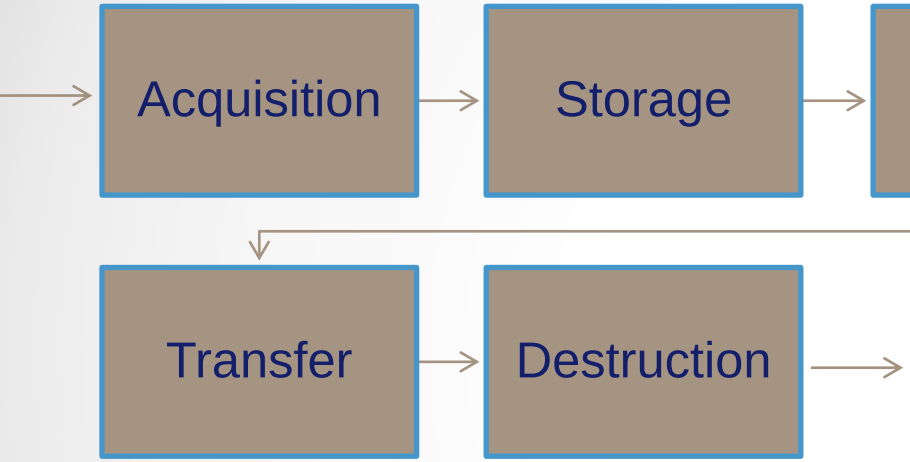
social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;

and specifically established by an executive order or an act of Congress to be kept classified.

Personal Information	**Sensitive Personal Information** (List based on IRR)	Privileged Information (List based on Rules of Court)
Name	Race	Data received within the context of a protected relationship – husband and wife
Address	Ethnic origin	
Place of work	Marital status	
Telephone number	Age	
Gender	Color	Data received within the context of a protected relationship – attorney and client
Location of an individual at a particular time	Religious affiliation	
IP address	Philosophical affiliation	
Birth date	Political affiliation	
Birth place	Health	Data received within the context of a protected relationship – priest and penitent
Country of citizenship	Education	
Citizenship status	Genetics	
Payroll & benefits information	Sexual life	
Contact information	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

	Sensitive Personal Information (List based on IRR)	
	Social security number	
	Licenses or its denials, suspension or revocation	
	Tax returns	
	Other personal info 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	
	Leave of absence reason	
	Licenses or its denials, suspension or revocation	

Personal Data Lifecycle

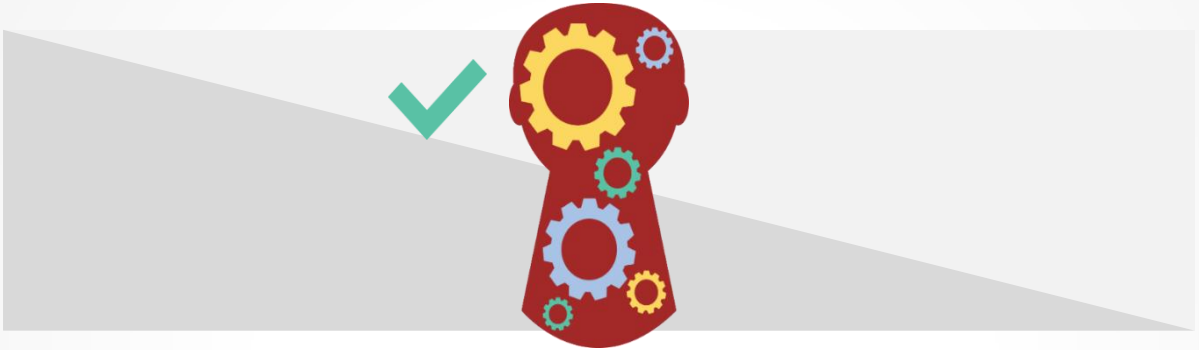


- Key considerations when listing your personal data:
  - What personal data do you collect?
  - In what form and through which channels?
  - For what purpose you collect personal data
  - How is it used?
  - Who is this data shared with internally and externally?
  - Who is authorized to access this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

Retention/Disposal should be based on:

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

TRANSPARENCY – “the CONSENT Regime”



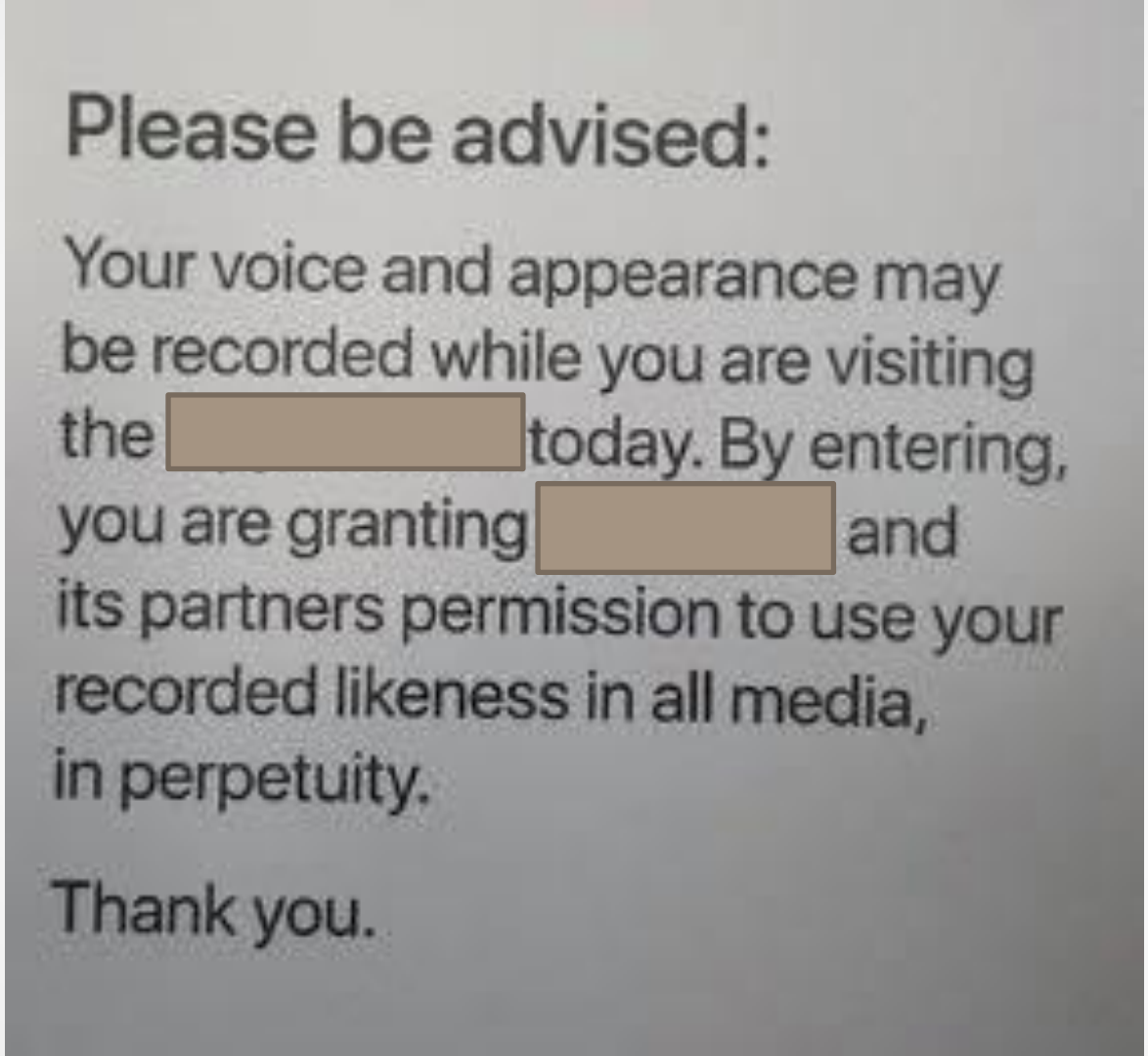
Principle of Transparency

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

Principle of 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.


Please be advised:
Your voice and appearance may be recorded while you are visiting the today. By entering, you are granting and its partners permission to use your recorded likeness in all media, in perpetuity.
Thank you.

PROPORTIONALITY

Principle of 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”

NATIONAL PRIVACY COMMISSION

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**

NATIONAL PRIVACY COMMISSION

Demonstrate Your Compliance: Implement your **privacy and data protection (PDP)** measures.

Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures (BRP)**.

NATIONAL PRIVACY COMMISSION

The Data Privacy Principles

- Personal data shall be:
  1. processed fairly and lawfully
  2. processed only for specified, lawful and compatible purposes
  3. adequate, relevant and not excessive
  4. accurate and up to date
  5. kept for no longer than necessary
  6. processed in accordance with the rights of data subjects
  7. kept secure
  8. shared to other PICs only if there is a DSA.

1 Technical

2 Organisational – other measures

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

Other Security Measures

- Shredding all confidential waste.
- Using strong passwords.
- Installing a firewall and virus checker on your computers.
- Encrypting any personal information held electronically.
- Disabling any ‘auto-complete’ settings.
- Holding telephone calls in private areas.
- Checking the security of storage systems.
- Keeping devices under lock and key when not in use.
- Not leaving papers and devices lying around.

12 offline measures to keep your physical data secure

- Lock rooms containing confidential information when not in use.
- Make sure employees don’t write their passwords down.
- Use swipe cards or keypads to access the office.
- Use CCTV cameras to monitor your office space.
- Shield keyboards when inputting passwords.
- Shred confidential waste.
- Use forensic property marking equipment and spray systems to mark assets.
- Use anti-climb paint on exterior walls and drains.
- Install an alarm system.
- Place bars on ground floor windows.
- Hide valuable equipment from view when not in the office.
- Assign a limited number of trustworthy employees as key safe holders.

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.

What support is needed from the rest of the org'n?

From Process Owners

- Process owners to own/maintain their respective Privacy Impact Assessments
- Process owners to consult on strategic projects involving the use of personal data ("Privacy by Design")
- Breach Drill to be conducted regularly test each Privacy Impact at least once a year

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From HR

- Roll-out training on privacy and data protection
- Issue security clearances to staff processing personal data (such clearance to be made contingent on passing the privacy training). DPOs must have access to all security clearances issued.
- Implement the recommended organizational controls

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Legal

- Legal to ensure that all PIP/service provider contracts, job orders, etc. are compliant. For example, all PIPs must also have their own DPO
- Legal to ensure that all external sharing of data meets the required guidelines of the NPC

Note: In order to avoid "privilege" issues, it's not advisable to have legal counsel be the DPO.

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Other Support Teams

- IT to implement the recommended technical controls
- Security to implement the recommended physical controls
- Internal audit to test internally for compliance

NATIONAL PRIVACY COMMISSION

What support is needed from the rest of the org'n?

From Top Management

- Budget support for security controls (technical, organizational, physical), for compliance tools and technology, for informational and training activities, for consultants, external auditors, advisors
- Incorporating compliance into the performance bonus parameters of those concerned, especially for those handling personal data
- Drive the message throughout the organization
- Drive the urgency (e.g. like the SARS epidemic, when everyone started installing hand sanitizers)

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! Any questions?

Gerard Paul B. Sentillas, R.N., O.H.N.
DOLE Accredited OSH Practitioner
0922- 8811-631