



Data Privacy Act of 2012


2019 1st PAGBA Seminar & Meeting
February 13-16, 2019
Crowne Plaza Hotel, Quezon City



2019 1st PAGBA Seminar & Meeting
February 13-16, 2019
Crowne Plaza Hotel, Quezon City

RIGHT AT HOME

Is My Not-So-Smart House Watching Me?



All that data mining has given some Americans pause. Seventy percent of consumers worry that hackers might access their smart devices at home, and 58 percent fear a lack of privacy from manufacturers that have access to their data, conversations, voice patterns and search history, according to [iQor](#), a customer service outsourcing provider.

Juliette Borda

<https://www.nytimes.com/2018/04/27/realestate/is-my-not-so-smart-house-watching-me.html>

Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

Connected home devices have increasingly cropped up in domestic abuse cases over the past year, according to those working with victims of domestic violence. Those at help lines said more people were calling in the

One of the women, a doctor in Silicon Valley, said her husband, an engineer, “controls the thermostat. He controls the lights. He controls the music.” She said, “Abusive relationships are about power and control, and he uses technology.”

Hotline, said she started hearing stories about smart homes in abuse situations last winter. “Callers have said the abusers were monitoring and controlling them remotely through the smart home appliances and the smart home system,” she said.

<https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>

Right to Privacy

The right to privacy is the right of an individual to control the collection of, access to, and use of personal information about him or her that are under the control or custody of the government or the private

@bhopaliwrites
**IT'S NO SECRET. IT'S
JUST NONE OF YOUR
BUSINESS**



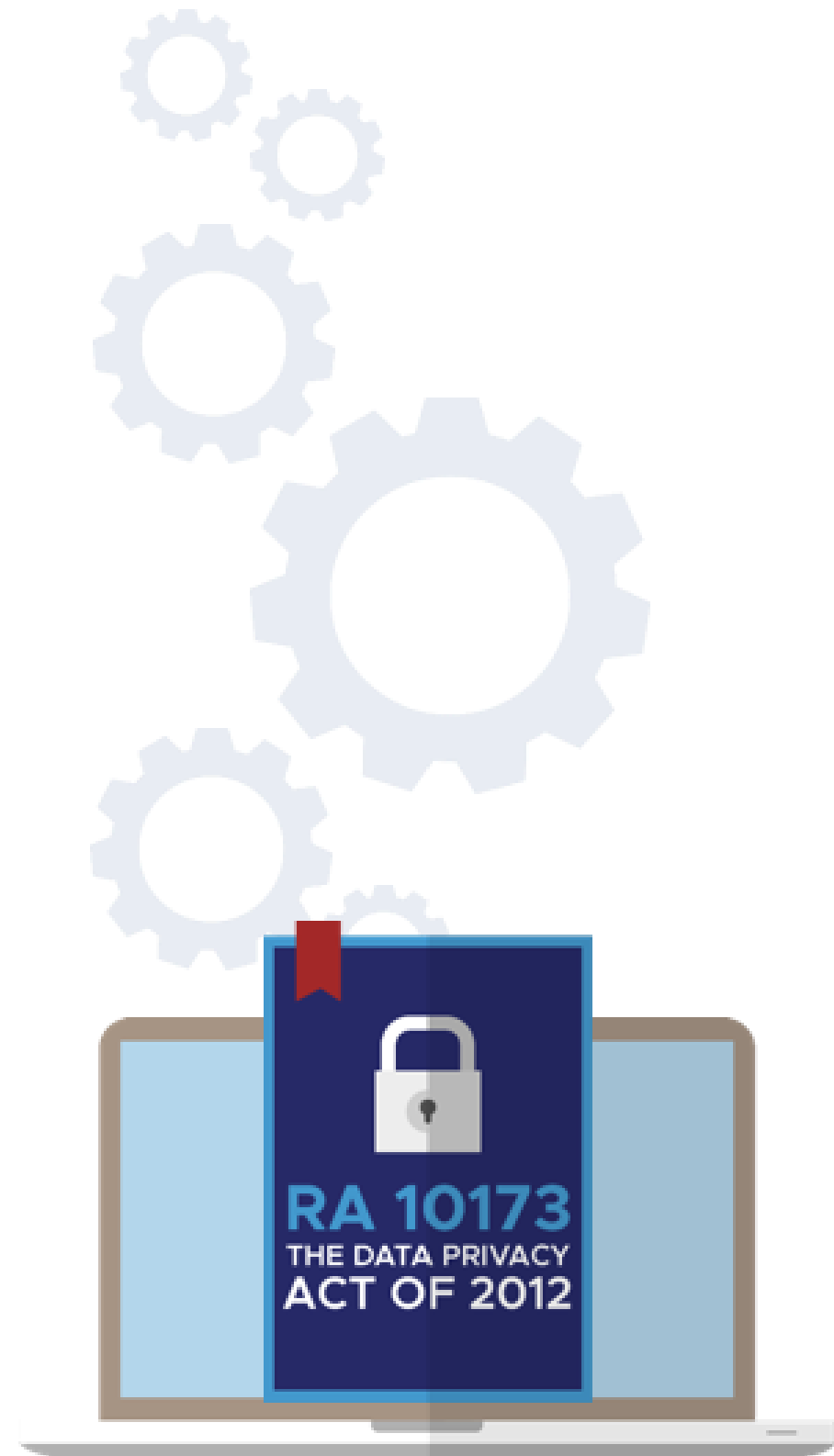
Image from:

https://www.instagram.com/p/BodXlYXBBW4/?utm_source=ig_share_sheet&igshid=brfth2a14m5p



INTRODUCTION: **RA 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.

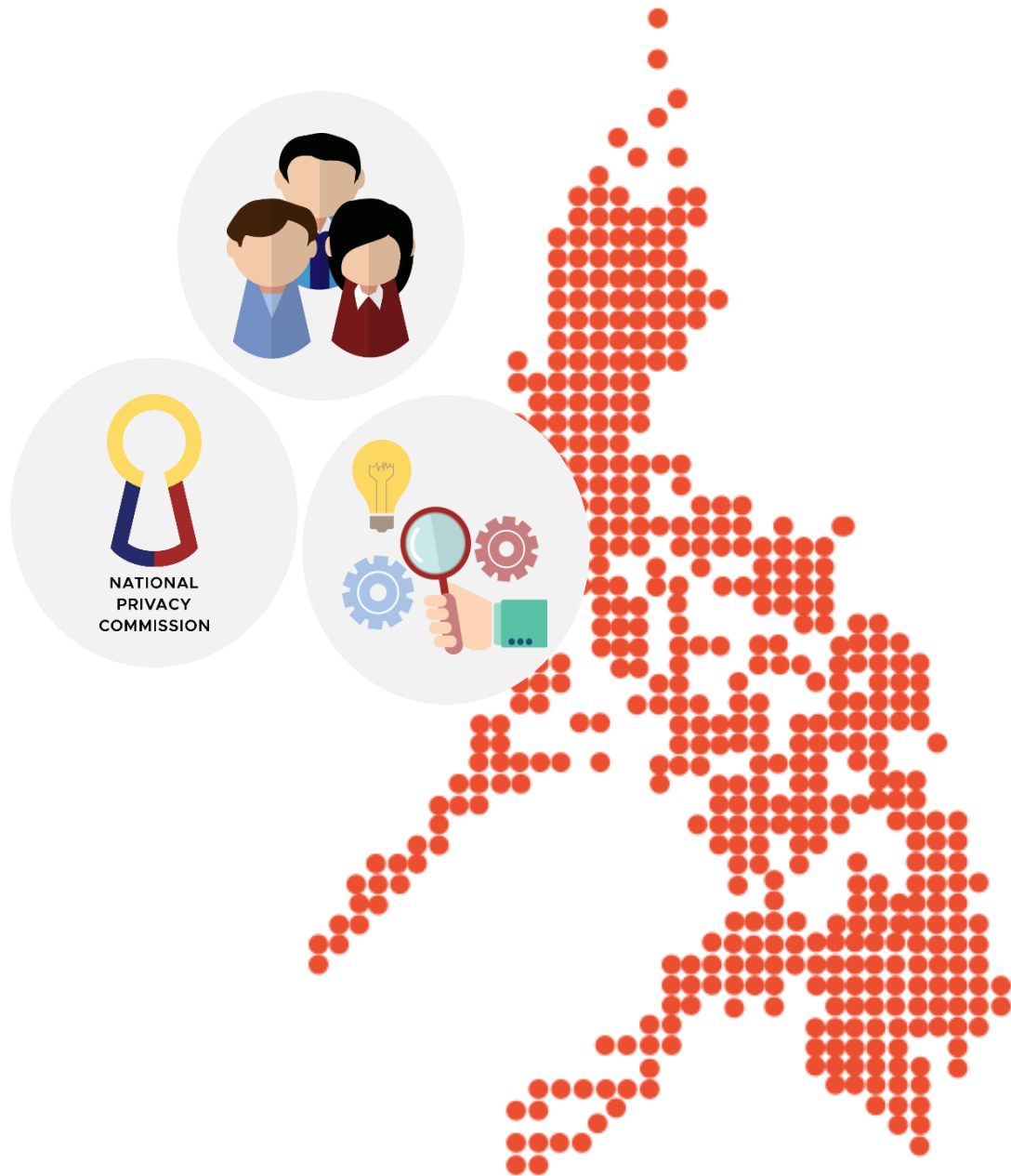


POLICY



It is the policy of the State to protect the fundamental human right of privacy while ensuring free flow of information to promote innovation and growth.

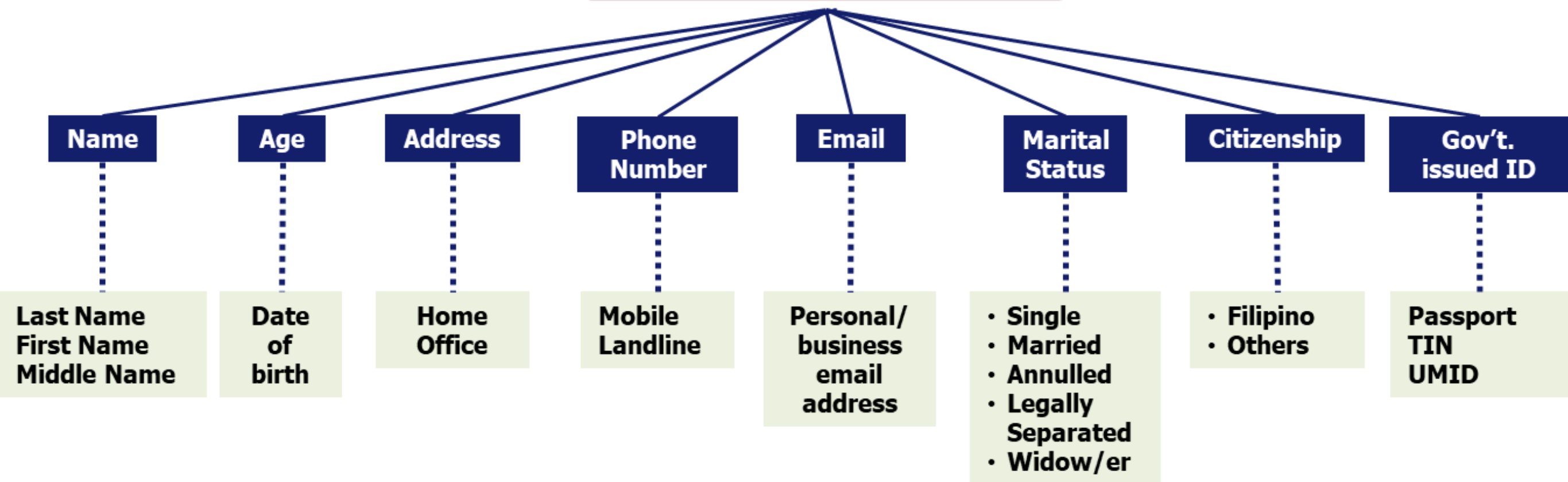
SCOPE



- government and the private sector
- processing of all types of personal information in the Philippines
- extraterritorial application in certain instances



KEY CONCEPTS



Personal Information



Name



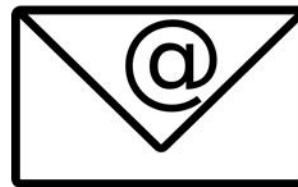
Address



**Landline
Number**



**Mobile
Number**



Email Address

- 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**.

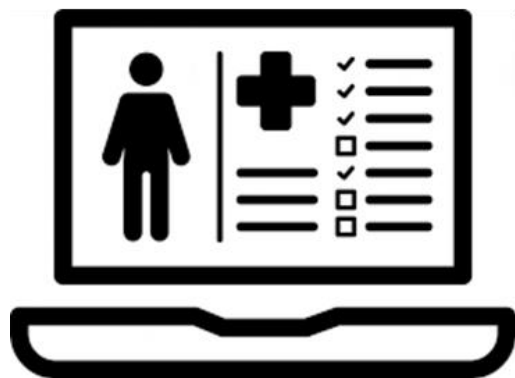
Sensitive Personal Information

race, ethnic origin, marital status, age, color and religious, philosophical, political affiliations



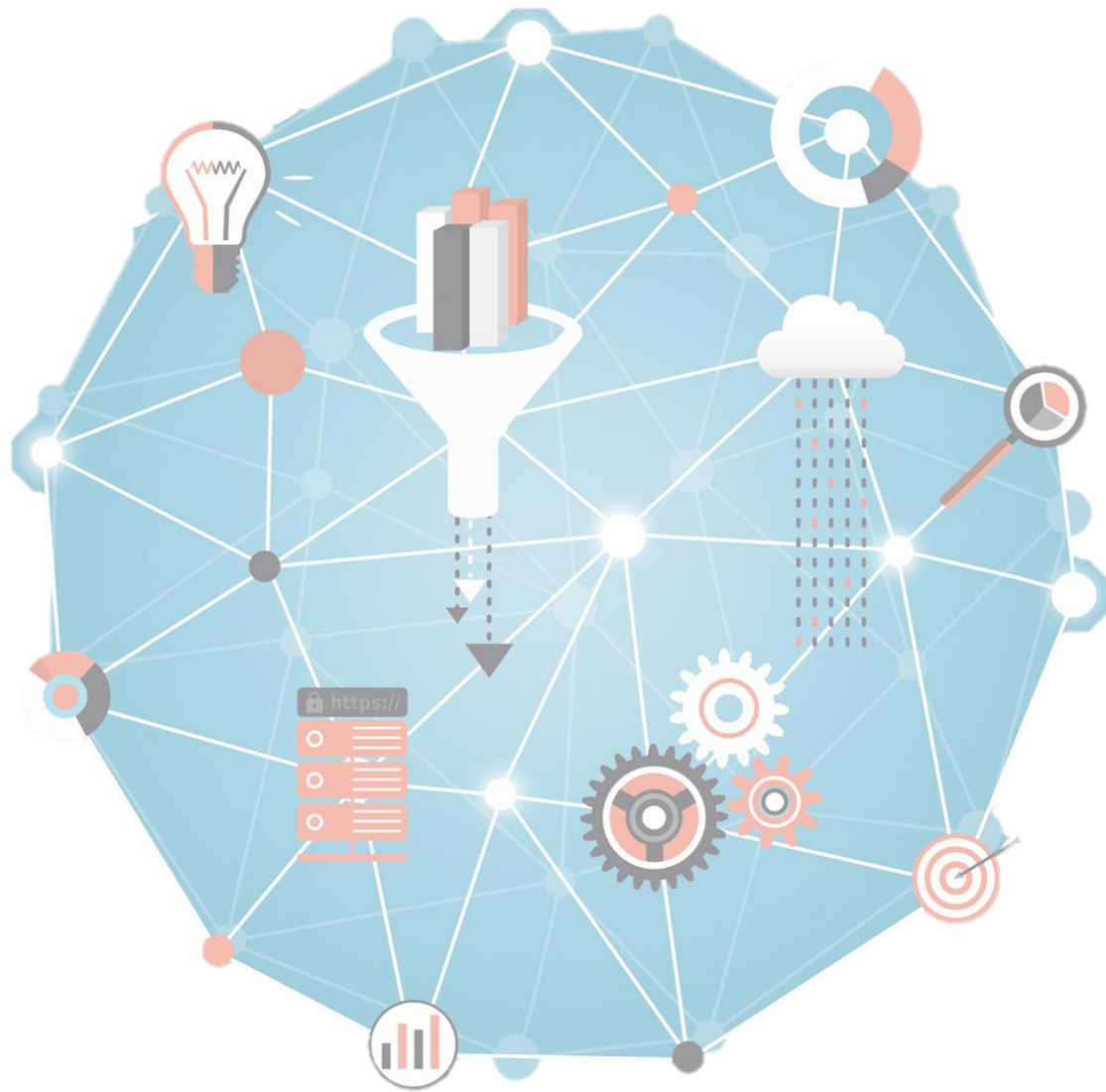
Marital Status

- ☐ Single
- ☐ Married
- ☐ Divorced
- ☐ Widowed



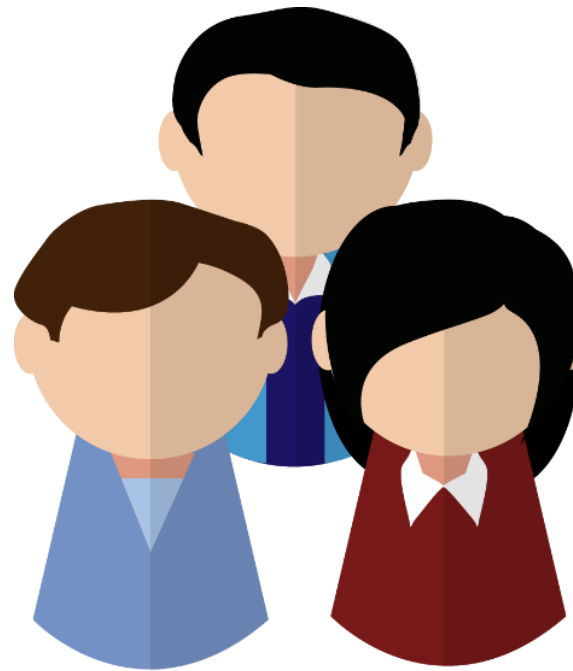
- health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed
- issued by government agencies peculiar to an individual (TIN, SSS Number, etc.)
- specifically established by law to be kept classified (Top Secret, Secret, Confidential, Restricted)

PROCESSING



- Collection
- Recording
- Organization
- Storage
- Updating or modification
- Retrieval
- Consultation
- Use
- Consolidation
- Blocking
- Erasure
- Destruction

DATA SUBJECT



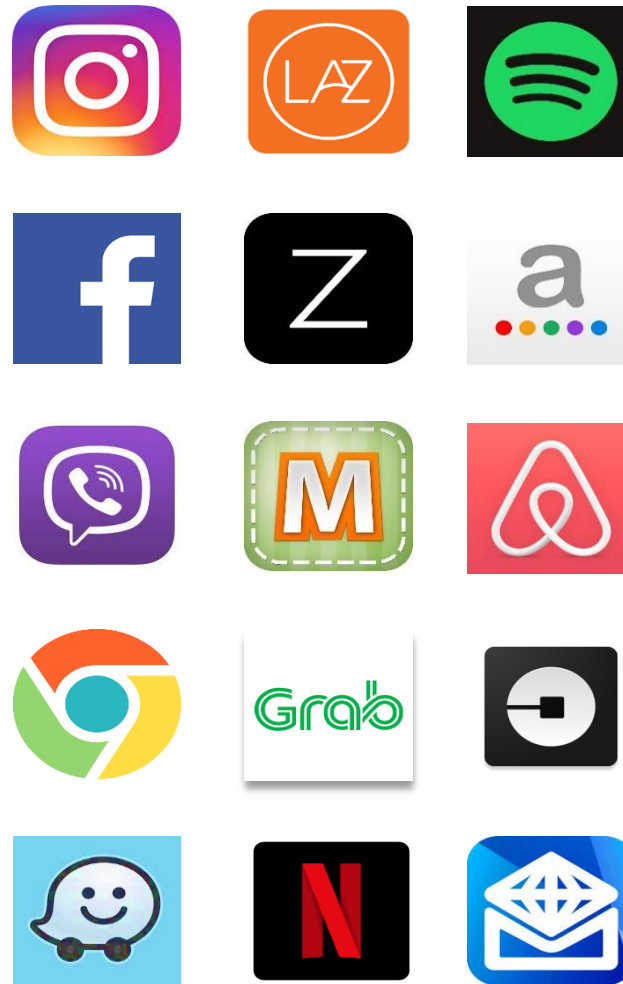
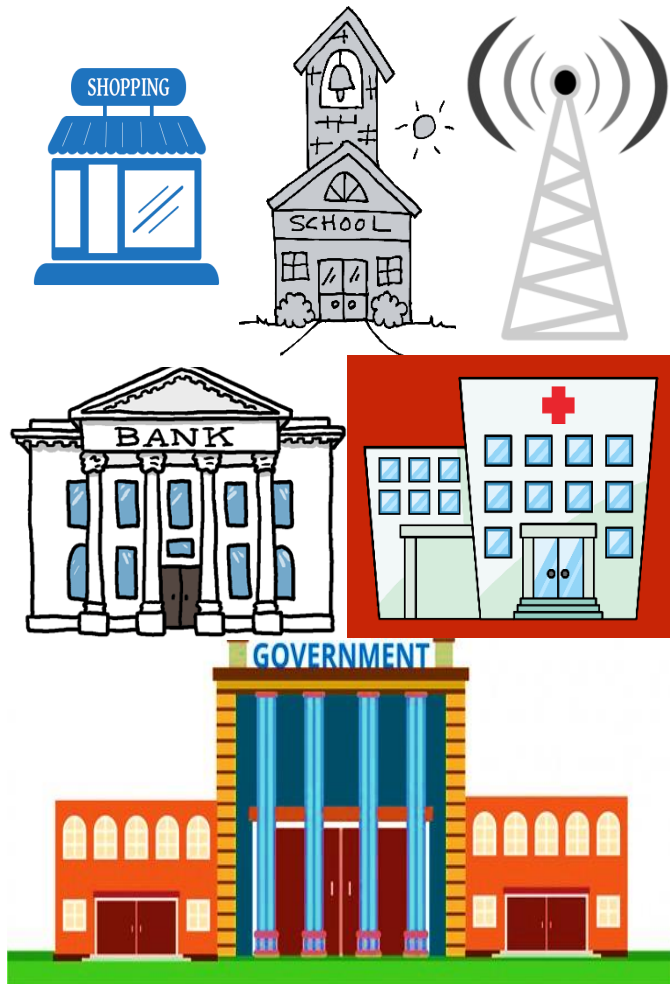
An individual whose **personal, sensitive personal or privileged information is processed.**

PERSONAL INFORMATION CONTROLLER



One who controls the collection, processing, use, sharing, disposal, and destruction of personal data, or instructs another to process personal data on its behalf.

PERSONAL INFORMATION CONTROLLER



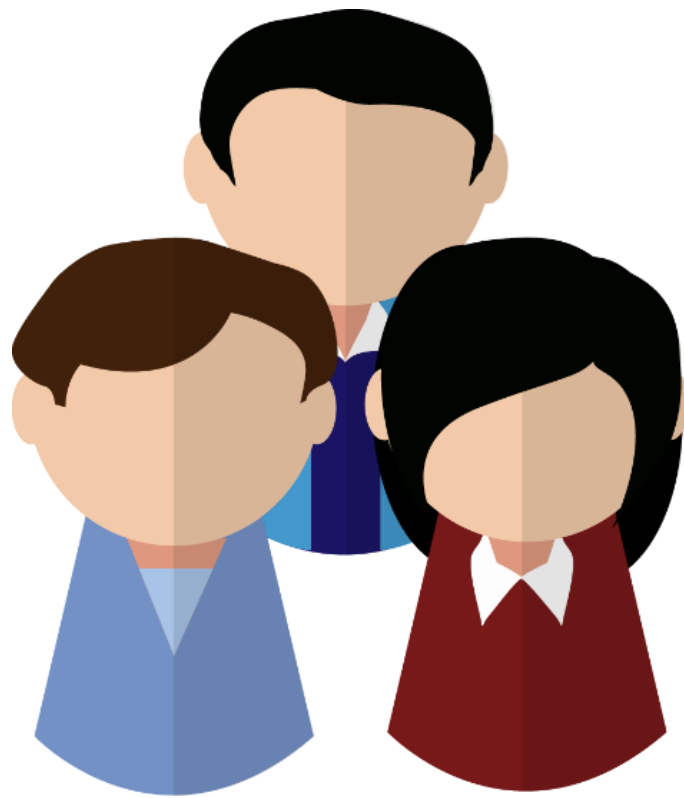
PERSONAL INFORMATION PROCESSOR



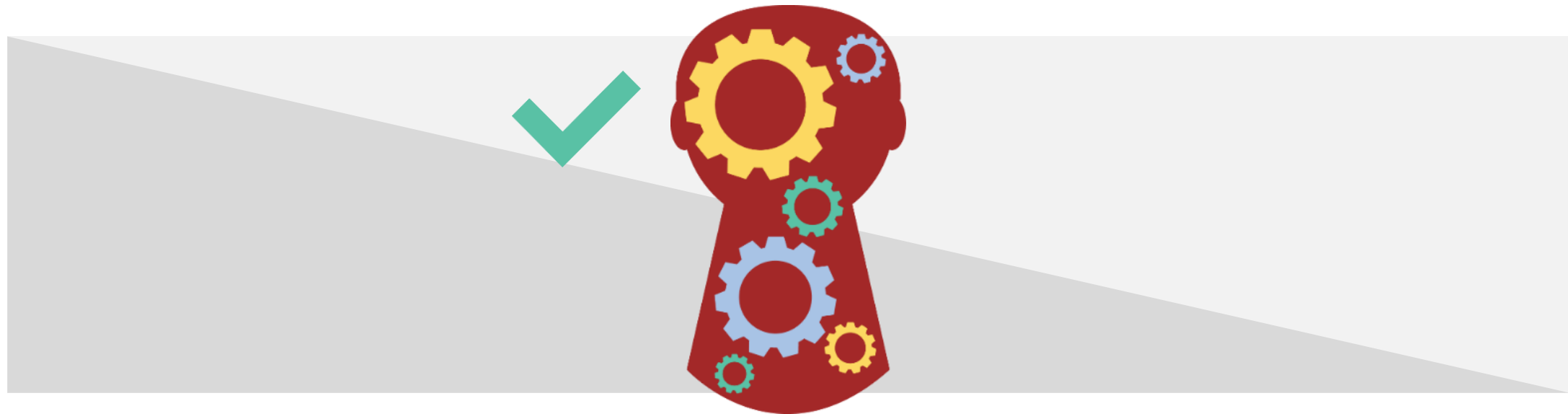
any natural or juridical person or any other body to whom a personal information controller may **outsource or instruct the processing of personal data** pertaining to a data subject

RIGHTS OF A DATA SUBJECT

1. Right to be Informed
2. Right to Access
3. Right to Object
4. Right to Rectification
5. Right to Erasure or Blocking
6. Right to Damages
7. Right to Data Portability
8. Right to File A Complaint



TRANSPARENCY



explicability
clarity
simplicity
unambiguity
perceptibility
manifestness
transparency
translucence
openness
conspicuousness
clearness
decipherability

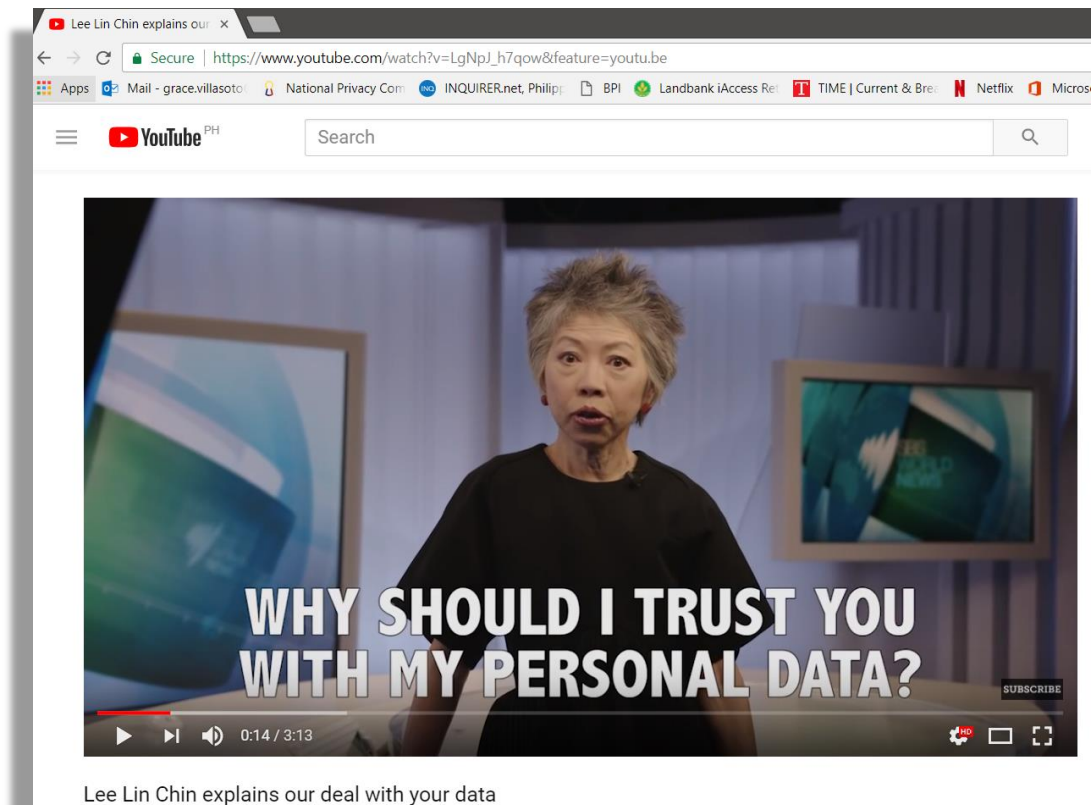
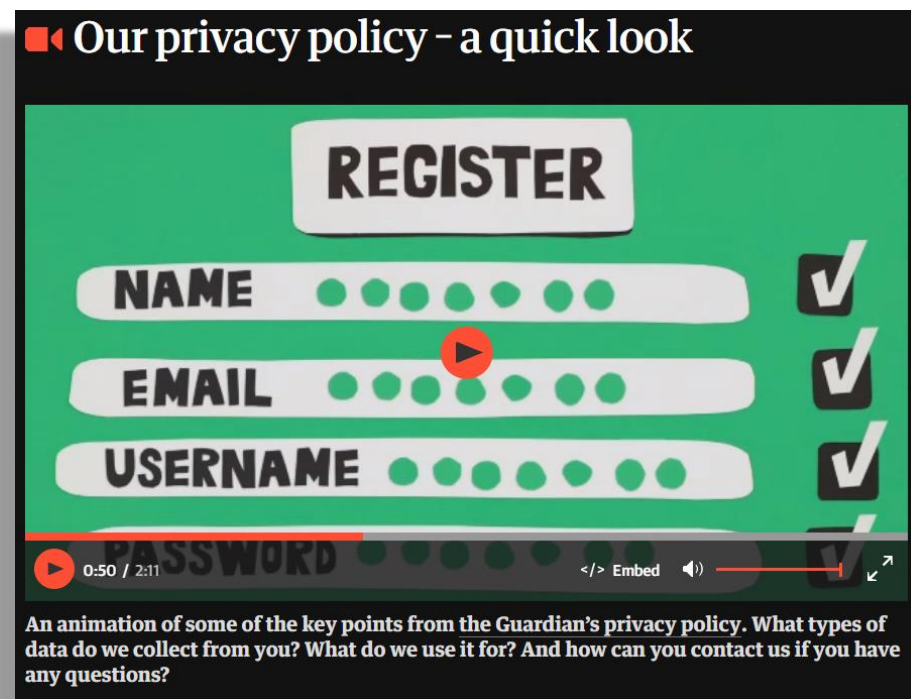
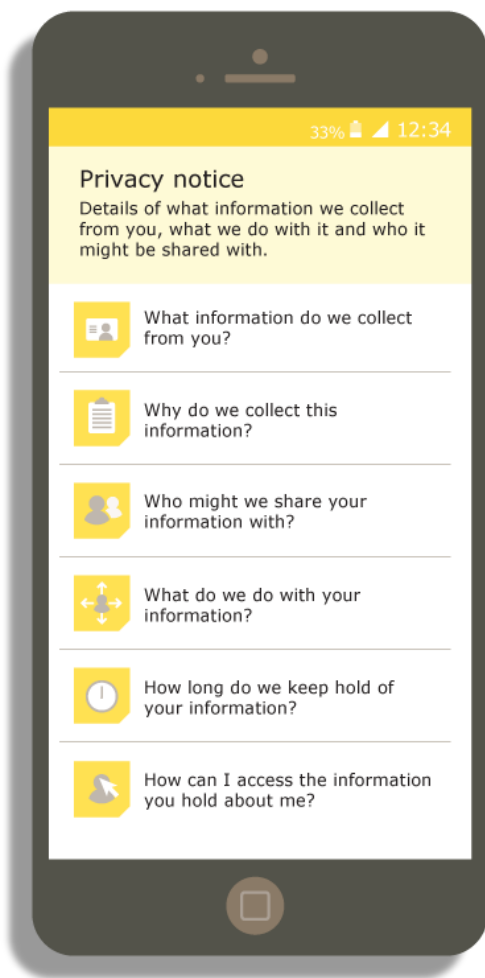
TRANSPARENCY

Data subject must be:

Aware of the **nature, purpose** and **extent** of processing of his/her personal data, including:

- ☐ *Risks and safeguards involved*
- ☐ *Identity of personal information controller*
- ☐ *Rights as data subject and how these rights can be exercised*

HOW TRANSPARENCY IS DEMONSTRATED



LEGITIMATE PURPOSE



legitimate purpose

lawful objective justifiable reasonable authorized sanctioned
genuine appropriate statutory proper accepted
fair

LEGITIMATE PURPOSE



The data subject agrees to the collection and processing of personal information

- ✓ **Freely given**
- ✓ **Specific**
- ✓ **Informed indication of will**

Evidenced by written, electronic or recorded means:

- ✓ signature
- ✓ opt-in box/clicking an icon
- ✓ sending a confirmation email
- ✓ oral confirmation

LEGITIMATE PURPOSE

Processing which may not need consent:



LEGITIMATE PURPOSE

What are the alternatives to consent?

For processing of personal information:

- ✓ Contract
- ✓ Compliance with a legal obligation
- ✓ Protect vital interests of the data subject, including life and health
- ✓ National emergency, requirements of public order and safety, or fulfill functions of a public authority
- ✓ Legitimate interests of the PIC or a third party to whom data is disclosed

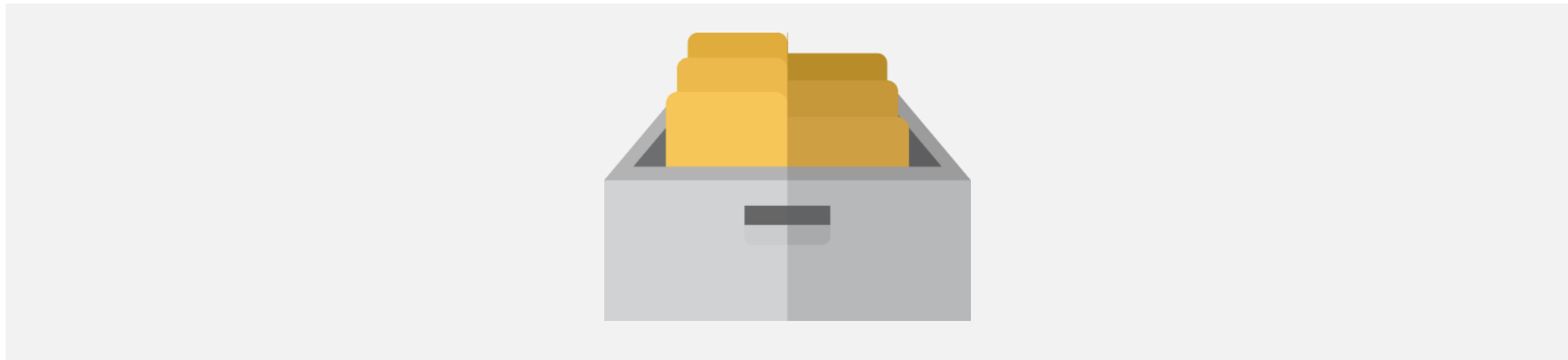
LEGITIMATE PURPOSE

What are the alternatives to consent?

For processing of sensitive personal information:

- ✓ Existing law and regulation
- ✓ Protection of life and health
- ✓ Public organizations
- ✓ Medical treatment
- ✓ Lawful rights and interests in court proceedings, establishment/exercise/defense of legal claims, or when provided to government

PROPORTIONALITY



proportionality

reciprocal
equitable
commensurate
even
comparative
just
equal
corresponding
correlative
comparable
rational

PROPORTIONALITY





THE FIVE PILLARS OF COMPLIANCE

1

**Appoint
Your
Data
Protection
Officer**



2

**Conduct
Your
Privacy
Impact
Assessment**



3

**Create
Your
Data
Privacy
Manual**



4

**Implement
Data
Privacy
and
Security
Measures**

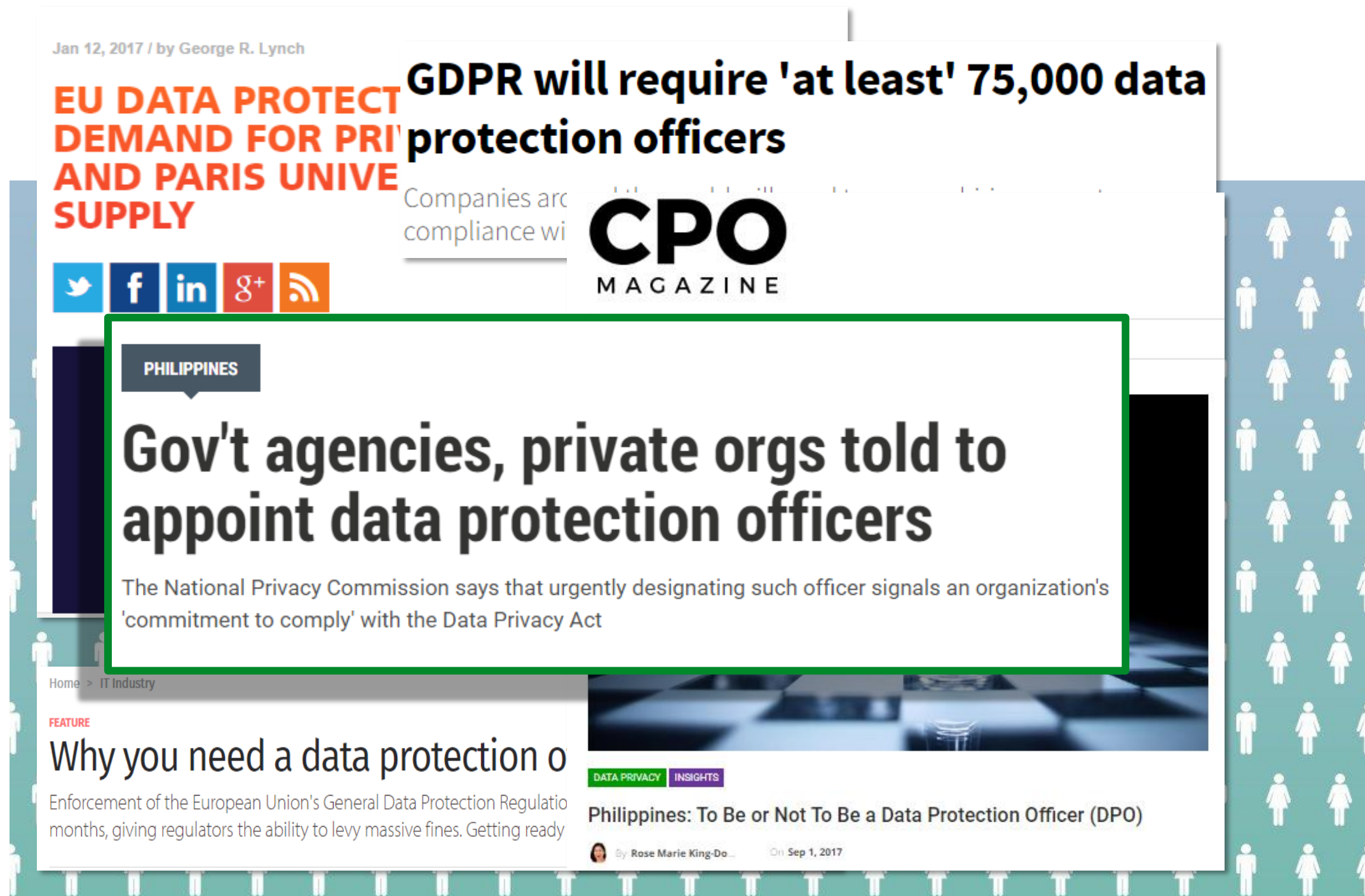


5

**Be
Ready
In Case of
Data
Breach**



PILLAR # 1



APPOINT A DATA PROTECTION OFFICER



Personal information controllers and personal information processors are required to appoint or designate a data protection officer (DPO) or compliance officer. DPOs will be accountable for ensuring compliance with applicable laws and regulations relating to data privacy.

What does a DPO do?



- a. Monitor compliance
- b. Ensure conduct of PIAs
- c. Ensure data subjects' rights are respected
- d. Ensure proper breach management
- e. Cultivate internal awareness on data privacy
- f. Advocate a privacy-by-design approach
- g. Serve as contact person for privacy matters
- h. Serve as conduit with the NPC
- i. Perform other duties as may be assigned

**See NPC Advisory No. 2017-01*

PILLAR # 2

CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)



A Privacy Impact Assessment (PIA) is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP.

PILLAR # 3




CREATE YOUR PRIVACY MANAGEMENT PROGRAM (PMP)

Your Privacy Management Program serves to align everyone in the organization in the same direction, to facilitate compliance with the Data Privacy Act and issuances of the NPC, and to help your organization mitigate the risks of a personal data breach.

PILLAR # 4

IMPLEMENT YOUR PRIVACY AND DATA PROTECTION (PDP) MEASURES



Measures laid out in your privacy and data protection policies should not remain theoretical.

They must continuously be assessed, reviewed and revised as necessary, while training must be regularly conducted.

PILLAR # 5

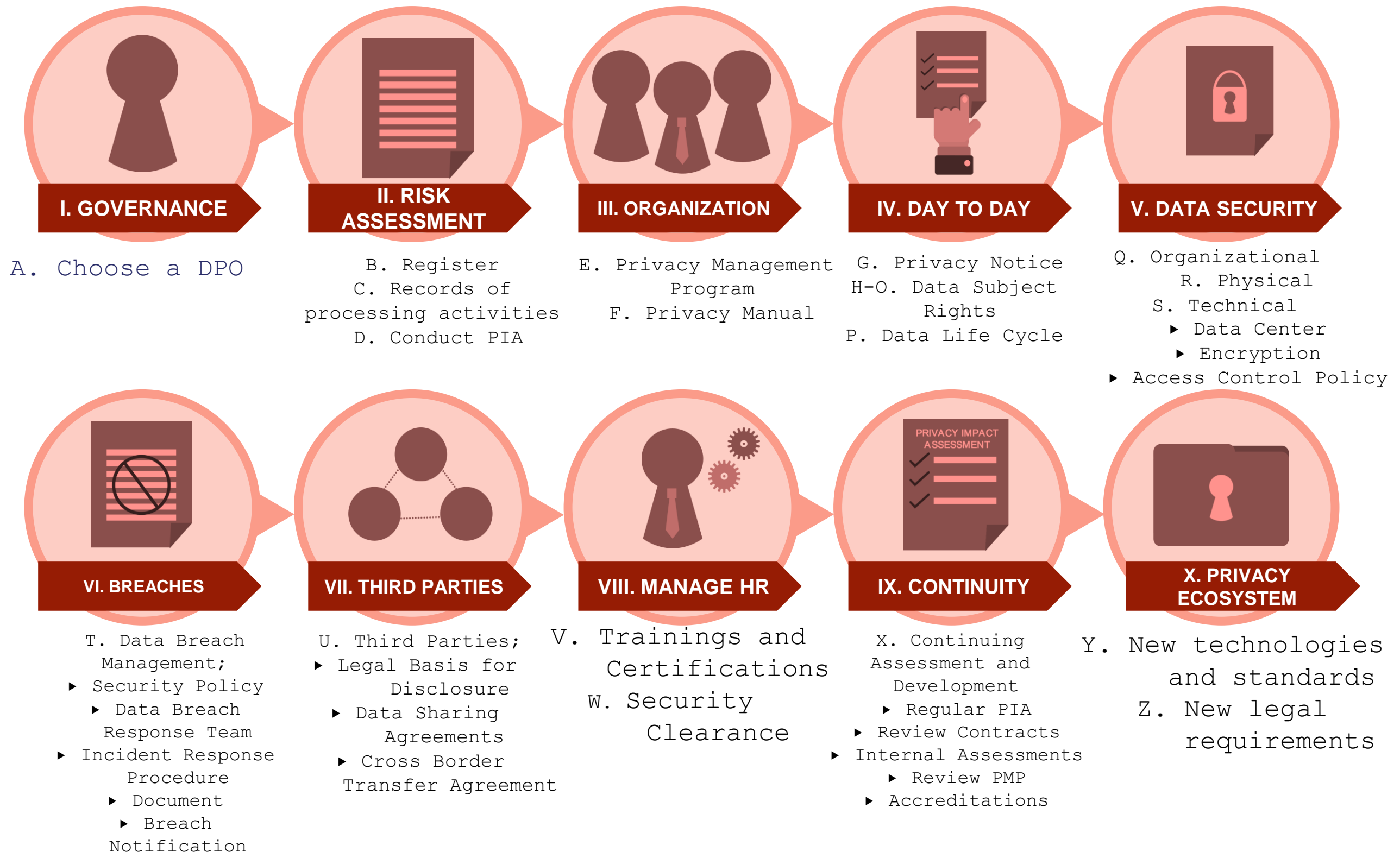
01100110101000
01010000101000
01100110101000
01010000101000
01100110101000
01010000101000
01010000101000



PRACTICE YOUR BREACH REPORTING PROCEDURES (BRP)

Upon **knowledge** of a personal data breach, it is important to conduct an initial assessment of the breach, to mitigate its impact, and to **notify both the National Privacy Commission and affected data subjects within 72 hours.**

NPC DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



UPDATES ON THE IMPLEMENTATION OF THE DPA

NPC Functions



RULE MAKING



ADVISORY



PUBLIC
EDUCATION



COMPLIANCE AND
MONITORING



COMPLAINTS
AND
INVESTIGATION



ENFORCEMENT

NPC Organizational Outcomes

- ✓ **Data Privacy Rights Promoted**
- ✓ **Data Subjects' Rights Protected**
- ✓ **Stakeholders' Capacity Developed**





DPO Assemblies



2019 1st PAGBA Seminar & Meeting
February 13-16, 2019
Crowne Plaza Hotel, Quezon City



1st National
**DATA
PRIVACY**
Conference



NPC marks PAW 2018 with call to uphold Filipino Data Privacy Rights

MANILA, PHILIPPINES -- The National Privacy Commission (NPC) marks the weeklong celebration of the Privacy

Awareness Week (PAW) from May 28 to 31 with the flagship **1st National Data Privacy Conference**, where around 2,000 Filipino privacy professionals and advocates came together for the biggest community gathering of its kind in the country, and probably, the world.



"Personal data breaches and violations to data subjects' rights are man-made. They can be prevented by building resilience and a culture of privacy and protection within the organization. You start by appointing an accountable officer within the organization, through proper privacy management policies, by training your staff, conducting risk assessments, implementing controls and preparing for breaches."



DICT Sec. Elmer A. Placido, Jr.



DSM USec. Lita C. Gutierrez



DPS USec. Ruth B. Castillo

In a show of support, representatives from high government expressed solidarity with the NPC in pursuing the cause of data protection and privacy rights.



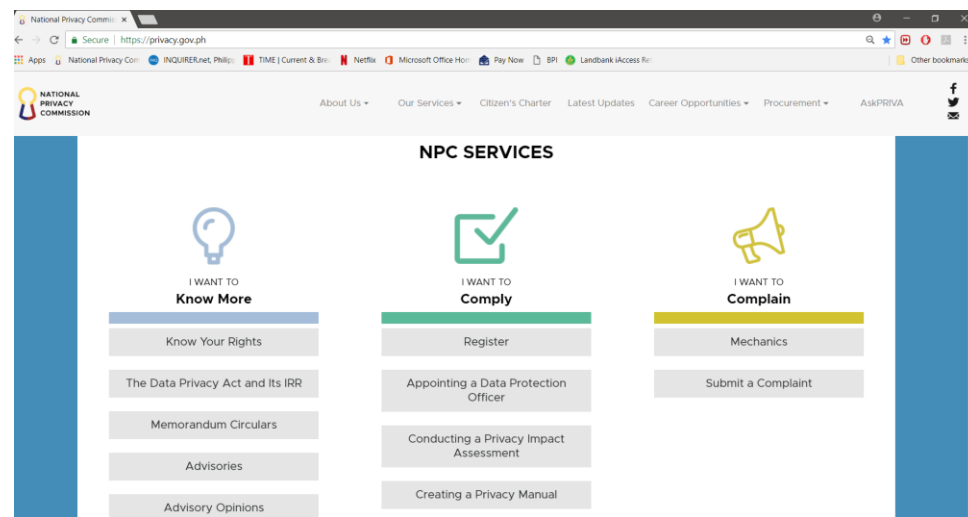
SAP Sec. Christopher Lawrence "Bong" T. Go

Privacy Awareness Week

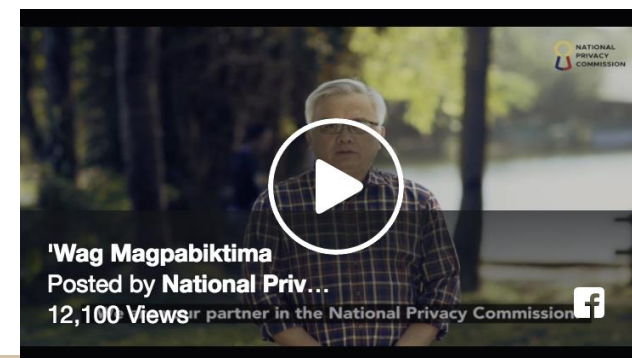


2019 1st PAGBA Seminar & Meeting
February 13-16, 2019
Crowne Plaza Hotel, Quezon City

Website & Print Knowledge Materials



Videos & Advocacy Campaigns



Data Privacy Advocacy Program



2019 1st PAGBA Seminar & Meeting
February 13-16, 2019
Crowne Plaza Hotel, Quezon City

The Commission continues to accept requests for opinions/clarifications on the interpretation of the provisions of the DPA and IRR, and have released numerous advisory opinions.

The Commission likewise provide comments and position papers on bills with the Senate and House of Representatives which has privacy implications.



PRIVACY NOTICE VS. CONSENT

- A privacy notice is a statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information.
- Being a mere notice, it is emphasized that the privacy policy or notice is not equivalent to consent. This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of data subjects.
- Mere posting of a PIC's privacy policy or notice and requiring the consumers to agree thereon via the online platform does not equate to obtaining the consent for purposes of processing his or her personal information as required by law. While consent may be obtained through electronic means, the fact that the data subject must agree to a privacy policy or notice fails to meet the requirement of a meaningful consent. A "bundled" consent, for instance, will generally not suffice as the data subject is not empowered to make a true choice. (ADVISORY OPINION NO. 2018-013)

CONSENT

- Consent may be evidenced by written, electronic, or recorded means. Any of the three (3) formats provided may be adopted by a personal information controller relative to the collection and processing of personal data. The NPC currently does not maintain any preference among the three. Nonetheless, it is worth emphasizing that, regardless of the format of the consent given by the data subject, it must be freely given, specific, and informed. (ADVISORY OPINION NO. 2017-007)
- The entity must never assume the data subject's consent for any activity involving his or her personal information, most especially, sensitive personal information, unless circumstances permit the processing of personal or sensitive personal information without consent, pursuant to the DPA and the IRR. (ADVISORY OPINION NO. 2017-42)
- If the PIC would require the consent of the customer for other purposes, the customer would have to provide his express consent thereto – saying on record that he agrees, ticking a box in an online form, or submitting a signed form. (ADVISORY OPINION NO. 2017-59)

CCTV

- A CCTV is a camera surveillance system that captures images of individuals or information relating to individuals.
- Need to inform/clearly notify the data subjects and the public in general, through a privacy notice or prominent signs that the establishment is being monitored by a CCTV camera.
- Viewing or disclosure of CCTV footages for identification of the person liable for the loss of personal property can be considered as processing necessary for the legitimate interests of the third party to whom the data is disclosed.
- Viewing and/or disclosure of footages should be limited to the following:
 1. Specific date of the incident;
 2. Particular time and duration of stay of the data subject in the establishment;
 3. If there are several CCTV cameras being operated, viewing only of the camera positioned at the precise location of the data subject during the incident; and
 4. Viewing only by the data subject, and other persons permitted by the data subject. (ADVISORY OPINION NO. 2018-080)

Scope - Special Cases

Processing by government/compliance with other laws

- A government agency having a constitutional or statutory mandate to collect and process personal data may do so even without the consent of the data subject. But this is with the concomitant responsibility of ensuring that organizational, physical and technical security measures are in place to protect the personal data it is processing. (ADVISORY OPINION NO. 2017-35)
- The exemptions from the coverage of the law are those information being collected pursuant to the laws enumerated; the exemption is not an exemption on the entity or agency but on the type of information processed. Also, this exemption is not a blanket exemption but only to the minimum extent necessary to achieve the specific purpose, function or activity. (ADVISORY OPINION NO. 2017-48)

Scope - Special Cases

Processing by government/compliance with other laws

Request for information

PNP - Considering that the personal data being requested is information of public concern, i.e. information of government employees, DSWD may accede to the PNPRO1's request and provide the following items only as these are the data which relates to the position or function of the employee:

- 1) Name of Agency Employees;
- 2) Office Address of Employees; and
- 3) Position/Designation in the Agency.

The other requested information – sex, age, and civil status – do not form part of information of public concern. These are likewise sensitive personal information the processing of which is prohibited except in certain instances provided under Section 13 of the DPA. (ADVISORY OPINION NO. 2017-56)

Scope - Special Cases

Processing by government/compliance with other laws

Request for information

BIR - The BIR is a public authority. Its powers and duties shall comprehend the assessment and collection of all national internal revenue taxes, fees, and charges, and the enforcement of all forfeitures, penalties, and fines connected therewith.

It is incumbent upon the BIR to demonstrate that the information being requested from the PMA is necessary in order to fulfill its function of determining the liability of any person for any internal revenue tax, or in collecting any such liability, or in evaluating tax compliance.

Prior to disclosing the requested information, it is advisable for the PMA to ask and clarify from the BIR the relation of the PMA Certification indicating the status of the membership of a person vis-à-vis the BIR audit or investigation of the tax liabilities, if any, of the said person following the general data privacy principles of legitimate purpose and proportionality. (ADVISORY OPINION NO. 2018-034)

Data Sharing

- A data sharing agreement can only be executed between or among PICs, as opposed to outsourcing, which is entered into by a PIC and a PIP. (ADVISORY OPINION NO. 2017-014)
- The data sharing of government agencies should always have a basis in law in order to fulfill the performance of a public function and provision of a public service. (ADVISORY OPINION NO. 2017-28)
- Data sharing between private sector entities is generally presumed to be in pursuit of some commercial objective or purpose, as is the compliance by such entities with the DSA requirement prior to any data sharing arrangement. (ADVISORY OPINION NO. 2017-018)

Publicly available information

- The provisions of the DPA are still applicable even for those personal data which are available in the public domain.
- There is no express mention that personal data which is available publicly is outside of its scope. Thus, “it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation.”
- Even if the data subject has provided his or her personal data in a publicly accessible platform, this does not mean he or she has given blanket consent for the use of his/her personal data for whatever purposes. (ADVISORY OPINION NO. 2017-30)

Processing of Personal Information for Character Reference

- The name and contact information of the character reference are considered personal information, and the processing of such is permitted if not otherwise prohibited by law, and when at least one of the conditions set by the Section 12 of the DPA is met.
- Among the criteria provided in the law for the processing of personal information is when “the processing is necessary for the purposes of the **legitimate interests** pursued by 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.”
- Taking into account that the sole purpose in requesting the names and contact numbers of the character references is to ask for additional information about the applicant or borrower, such as new address and/or new contact number of the applicant or borrower, in the event that the latter defaults in his/her loan obligation and can no longer be reached at the contact information he/she provided, the same may be considered as a legitimate interest of the company for verification and fraud prevention. (ADVISORY OPINION NO. 2017-41)

OFFENSES AND PENALTIES

OFFENSES AND PENALTIES

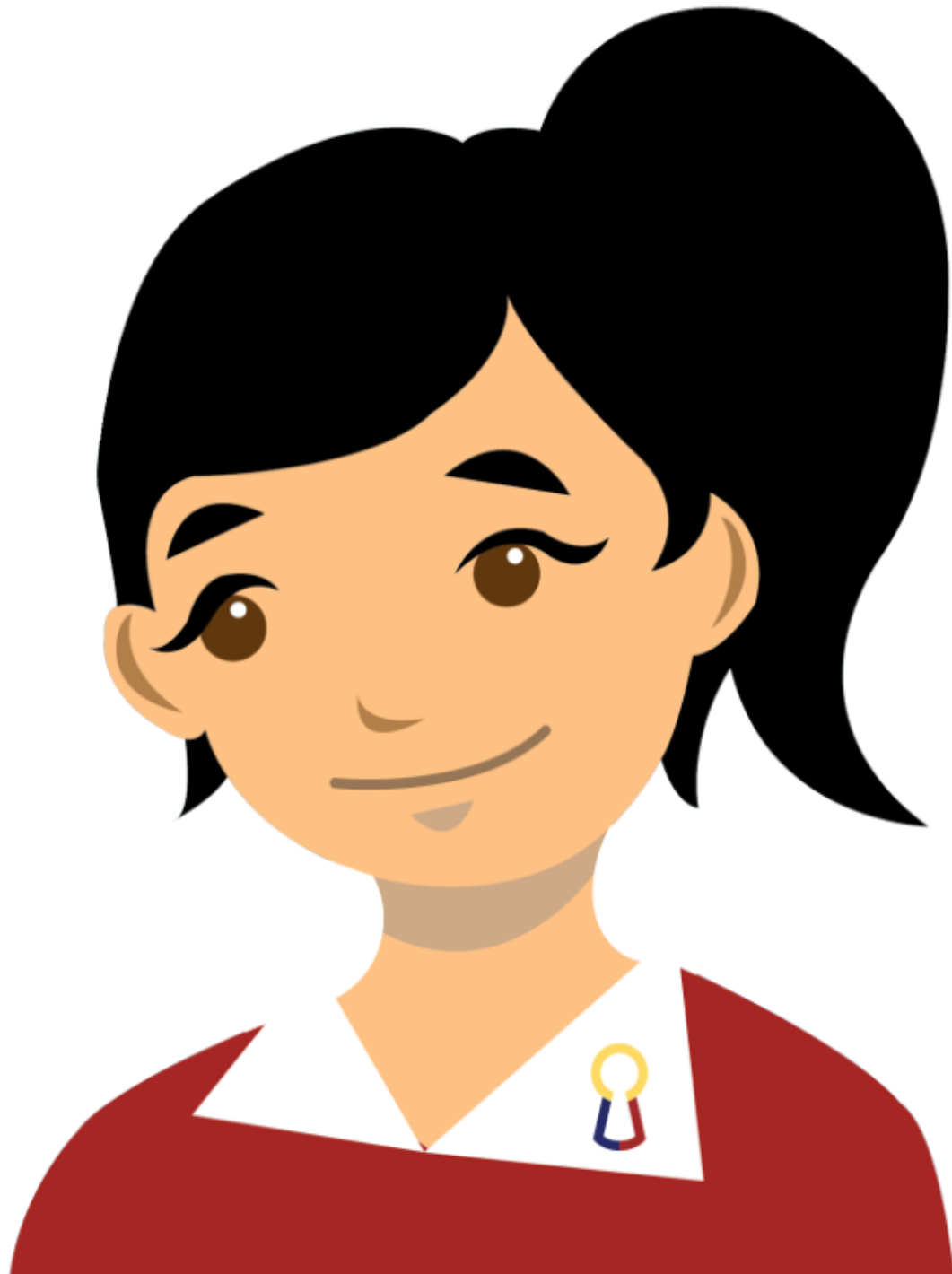
Punishable Act	Imprisonment		Fine	
	PI	SPI	PI	SPI
Unauthorized processing (without consent of the data subject or without being authorized by law)	1y-3y	3y-6y	500k-2m	500k-4m
Access due to negligence (provided access to without being authorized by law)	1y-3y	3y-6y	500k-2m	500k-4m
Improper disposal (knowingly or negligently dispose, discard, or abandon the personal information in an area accessible to the public or otherwise placed the personal information for trash collection)	6m-2y	3y-6y	100k-500k	100k-1m
Unauthorized purposes	18m-5y	2y-7y	500k-1m	500k-2m

OFFENSES AND PENALTIES

Punishable Act	Imprisonment		Fine	
	PI	SPI	PI	SPI
Intentional breach (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)	1y-3y		500k-2m	
Concealing breach (intentionally or by omission conceals the fact of breach)	18m-5y		500k-1m	
Malicious disclosure (with malice/in bad faith, discloses unwarranted or false information)	18m-5y		500k-1m	
Unauthorized disclosure (discloses to a third party personal information not covered by the immediately preceding section without consent)	1y-3y	3y-5y	500k-1m	500k-2m
Combination of acts	3y-6y		1m-5m	

Extent of Liability

- If the offender is a juridical person, the penalty shall be imposed upon the **responsible officers** who:
 - ✓ participated in; or
 - ✓ allowed the commission of the crime by their gross negligence.
- Maximum penalty shall be imposed when the personal information of at least 100 persons is harmed, affected or involved as the result of the abovementioned actions.
- When the **offender is a public officer** in the exercise of his or her duties, an accessory penalty consisting in the **disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.**



Complaints : 517-7806
Compliance/
registration : 517-7810
0910-1029114
0965-2863419
Public assistance : 0945-1534299
0939-9638715

Email us at info@privacy.gov.ph

privacy.gov.ph
facebook.com/privacy.gov.ph
twitter.com/privacyph

AskPriva