

# Frameworks to Facilitate Cross-border Data Flows- The Case of Harmonization and Interoperability in Asia

Raymund Enriquez Liboro  
Privacy Commissioner  
September 12, 2019



**National Privacy Commission - APEC Business Advisory Council Philippines**

# **NPC Roadmap** to Data Privacy Resilience

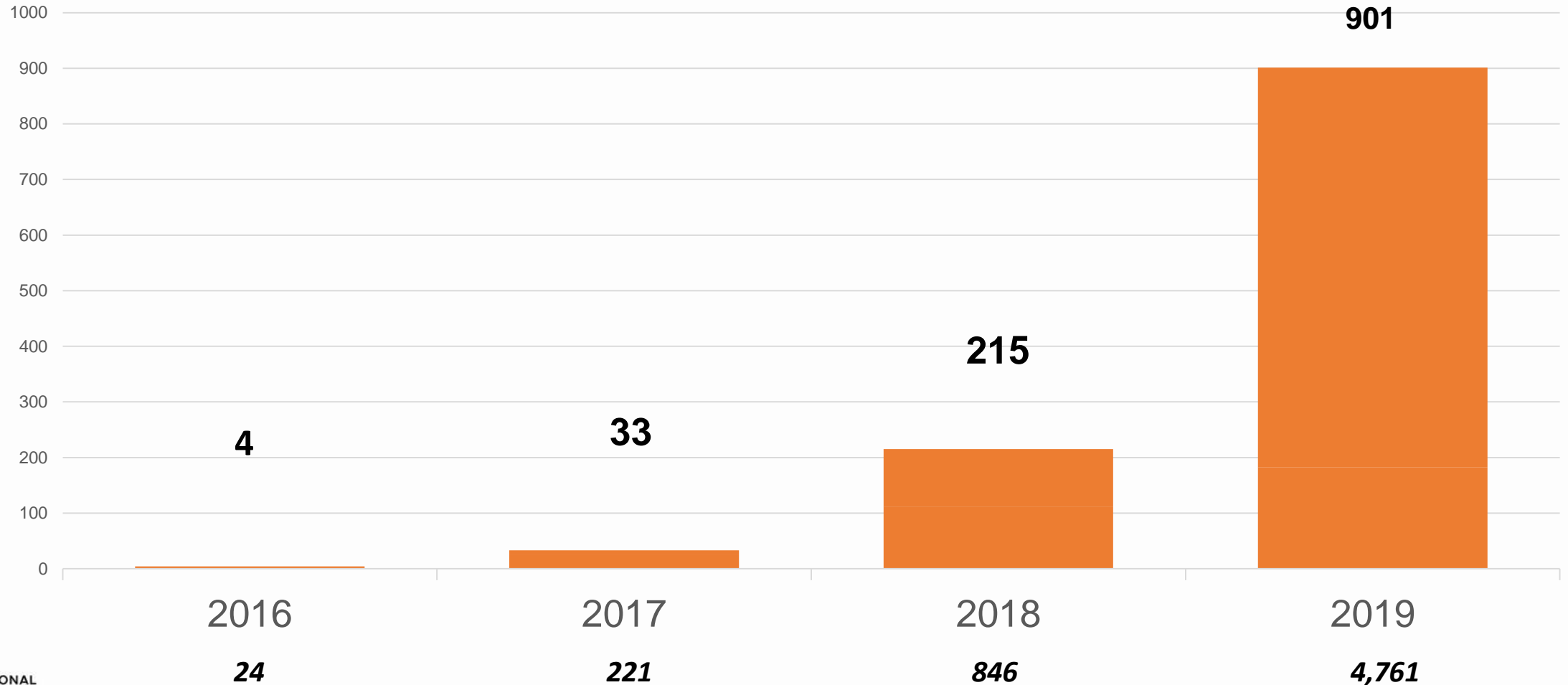




# DATA SUBJECTS' PRIVACY RIGHTS PROTECTION PROGRAM

- ENFORCEMENT AND COMPLAINTS HANDLING PROGRAM

## Complaints Handled

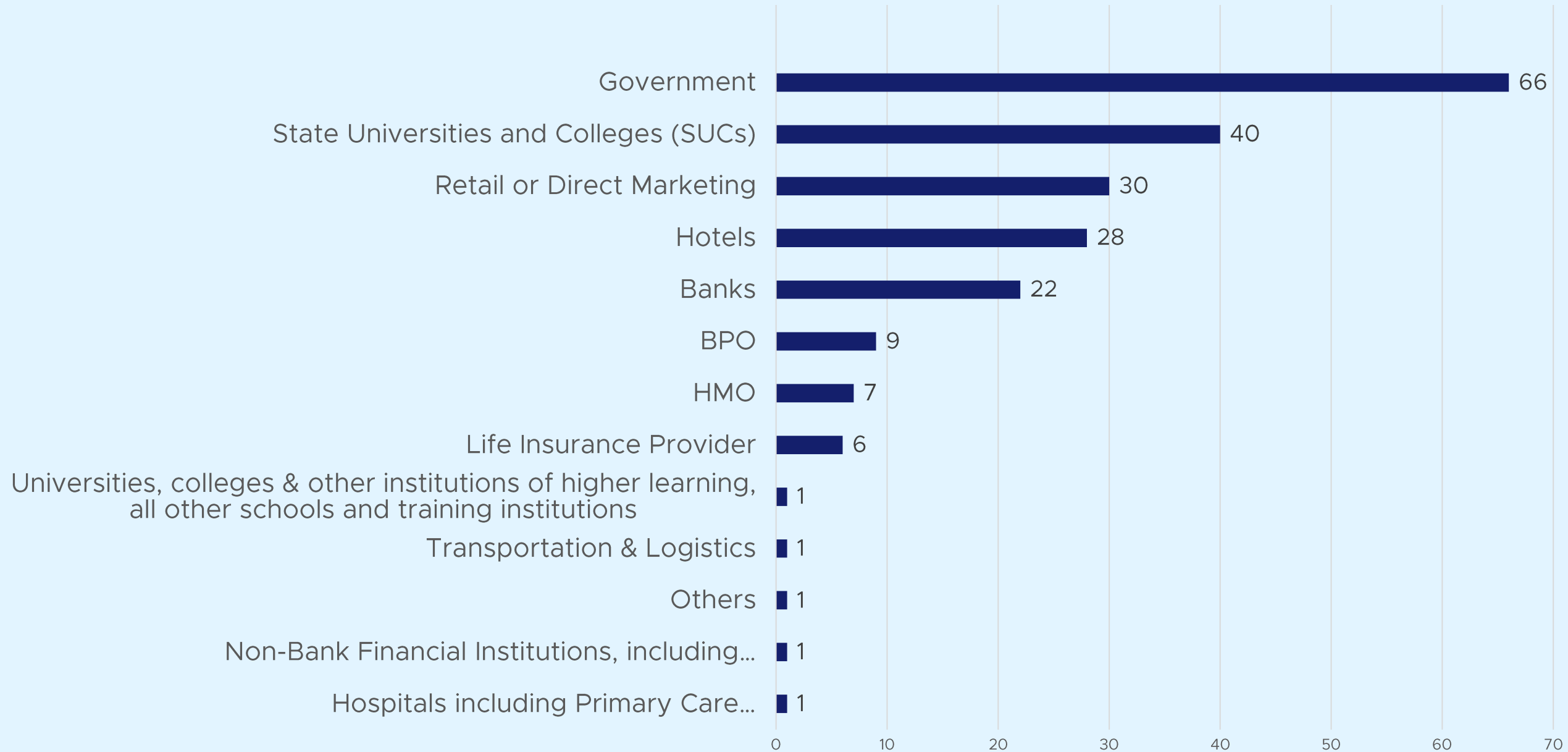


December  
2018  
To  
August 2019

213

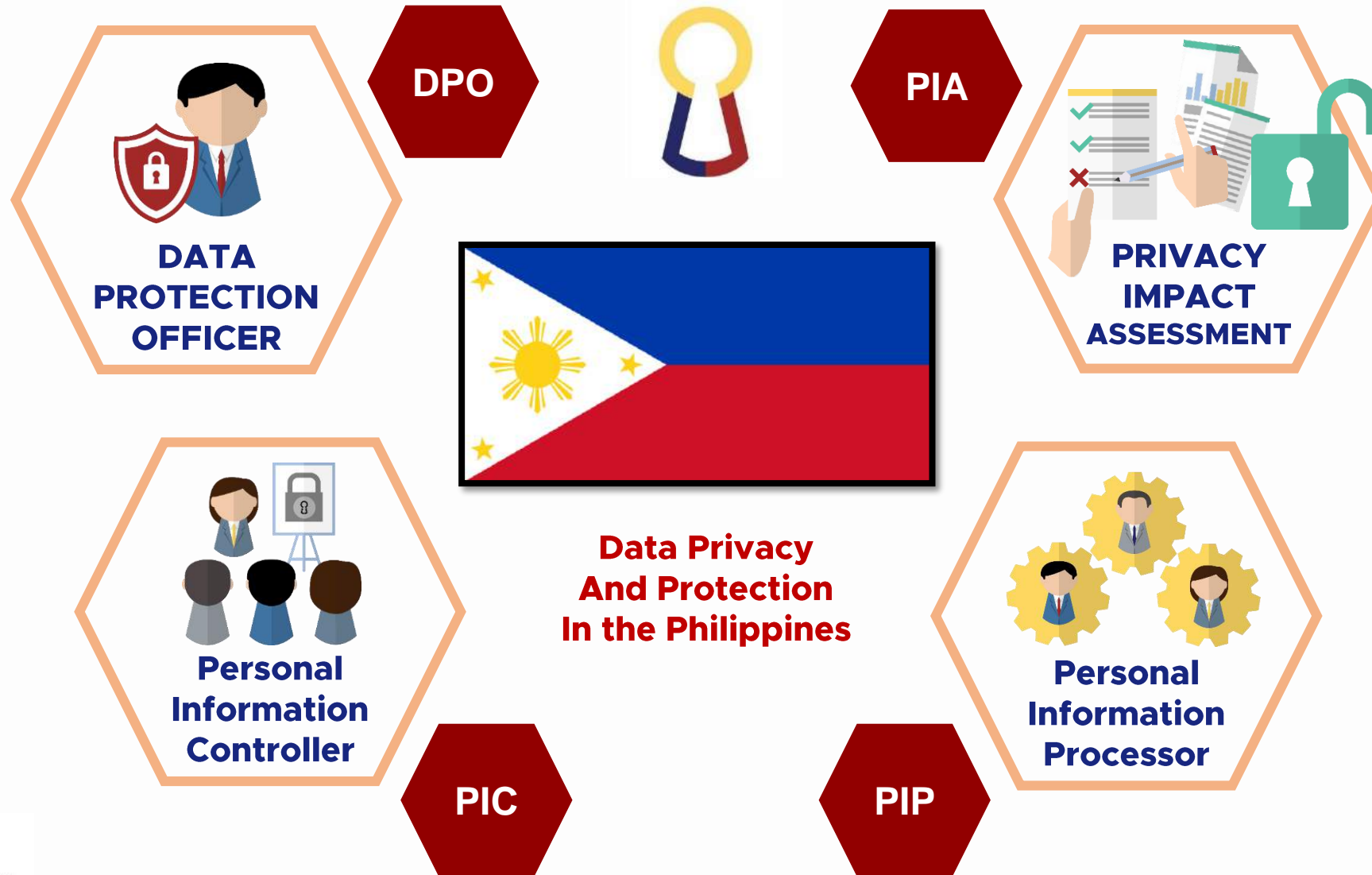
PRIVACY SWEEPS  
CONDUCTED

# Privacy Sweeps Conducted, by Sector

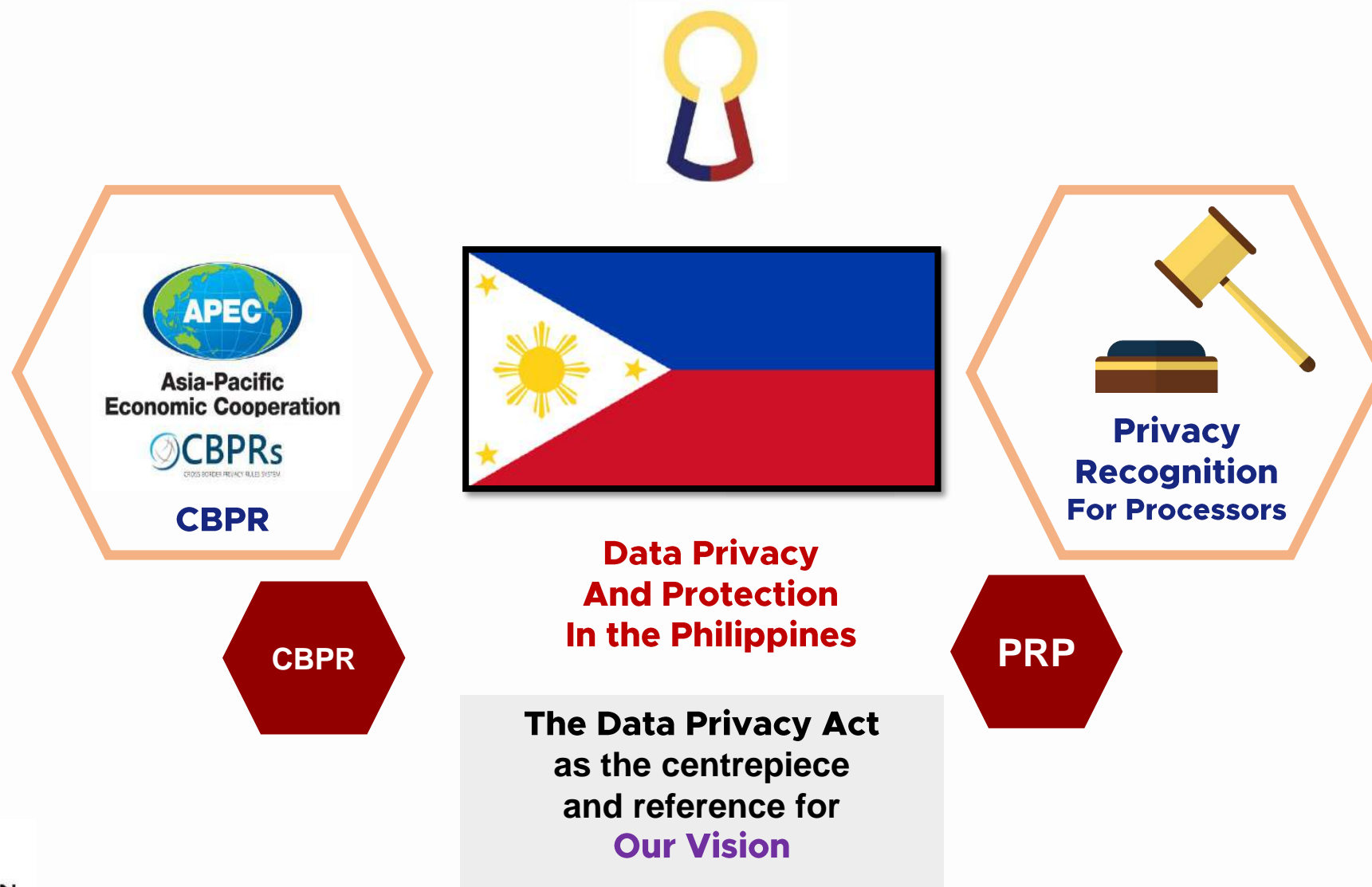




# Privacy in the Philippines



# Privacy in the Philippines





# R.A. 10173, the “Data Privacy Act”

---

## ❖ Law of General Application

- Applies to both Public and Private Sector
- Applies, in general, to the different sectors
- Includes provisions for **extraterritorial application**

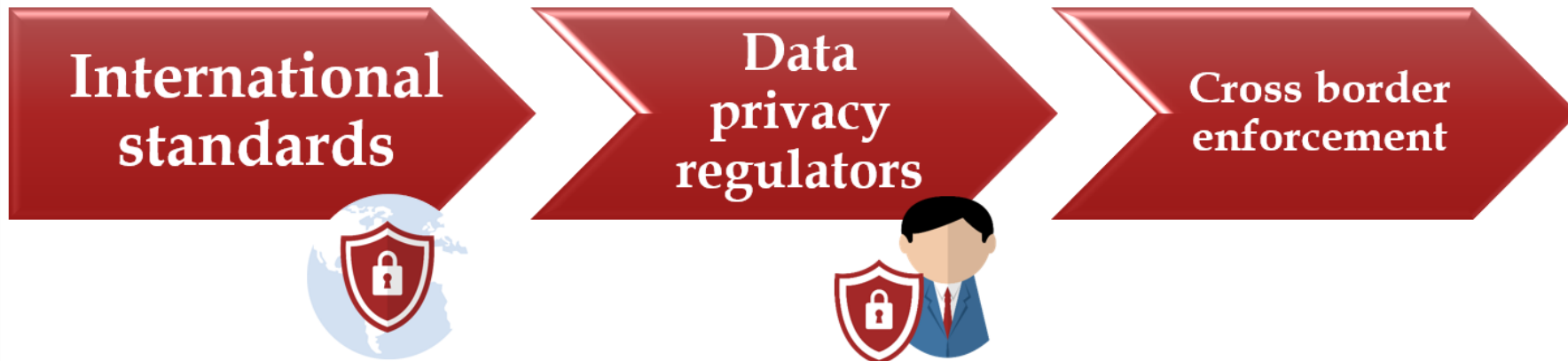


❖ Creates the **National Privacy Commission**, an independent body for the administration and implementation of the law

# Extraterritorial Application

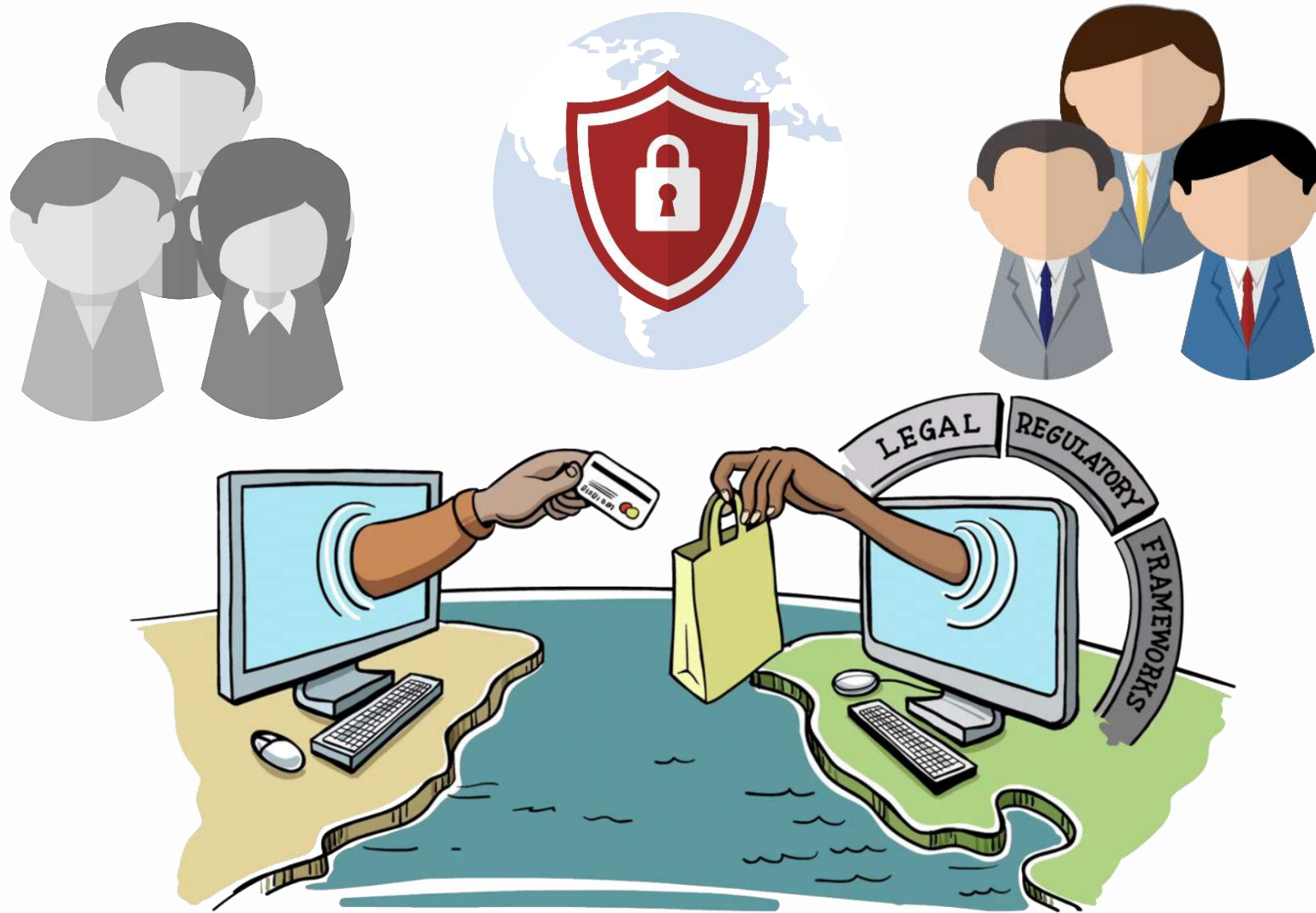
---

- Ensure compliance of the country with international standards for data protection
- Ensure coordination with data privacy regulators in other countries and private accountability agents
- Negotiate with other data privacy authorities for cross-border application and implementation of respective privacy laws
- Assist Philippine companies doing business abroad

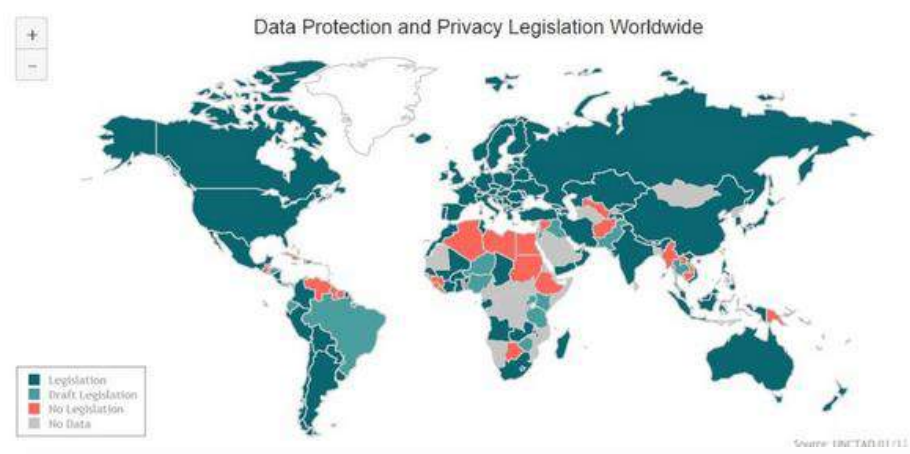


# The Digital World and flow of Information

---



# Where your Privacy Is (and Isn't) Protected




Countries that have enacted data privacy laws has risen from 120 to 132, a **10% increase**



# Data Privacy – Support for Multi-jurisdictions

|  |  |
|--|--|
|    | <b>Singapore</b><br>Up to S\$1 million.<br>\$10k per DNC breach<br>Legal Proceedings                         |
|    | <b>Malaysia</b><br>RM 500,000<br>Up to 3 years jail  |
|   | <b>European Union</b><br>Up to 4% of global annual turnover for companies<br>Euro 10m-20m                    |
|  | <b>Taiwan</b><br>Up to 5 years jail in addition to or instead of fines of up to NT\$500k-1m (sensitive data) |

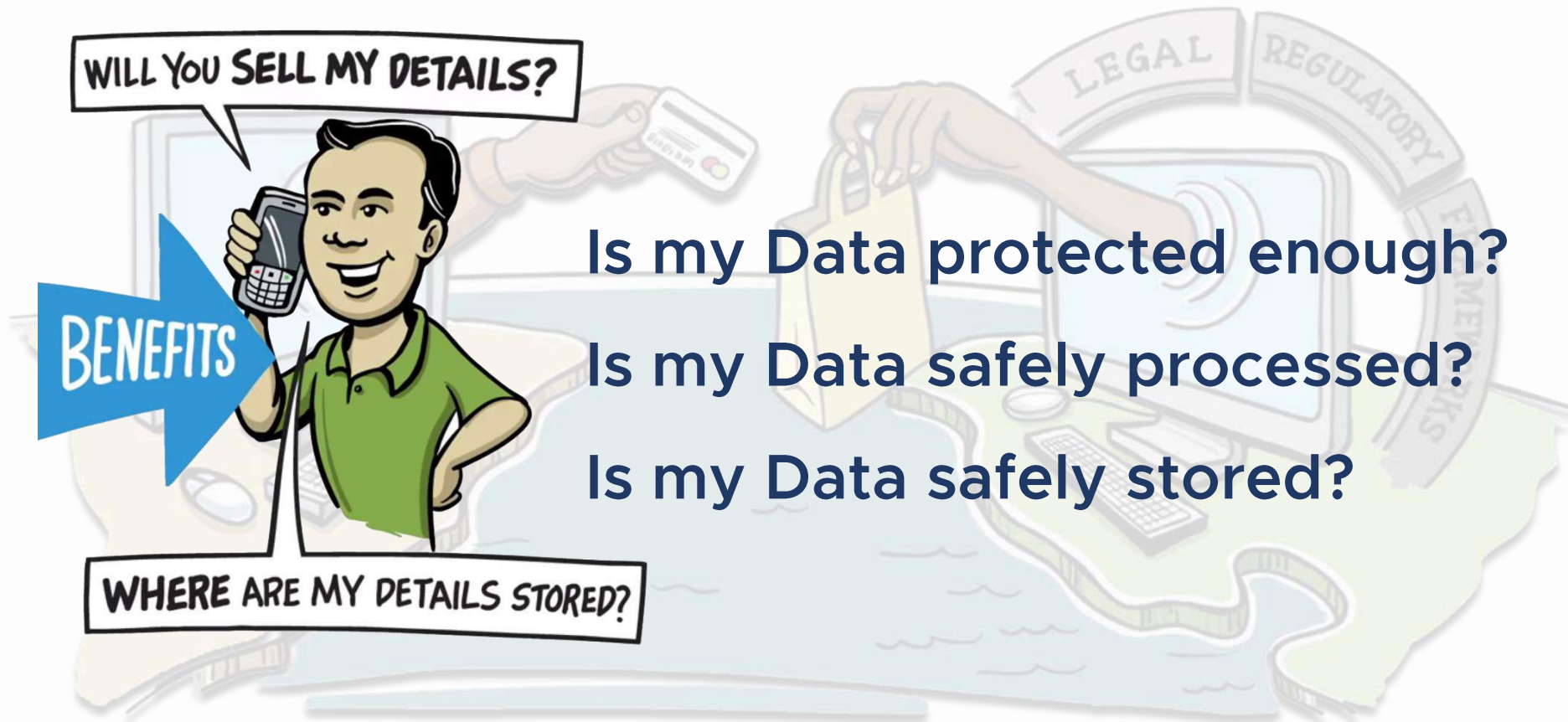
|   |  |
|---|--|
|    | <b>Australia</b><br>Up to A\$1.7 million for each breach   |
|    | <b>Hong Kong</b><br>Fines – HK\$500k-1m<br>And 3 to 5 years jail   |
|   | <b>Philippines</b><br>1-3 years jail – unauthorized disclosure (up to Php 1m fine)<br>3-6 years jail – sensitive data breach (up to Php 4m fine) |
|  | <b>India</b><br>Fine up to INR 500,000 or up to 3 years jail or both   |

|   |
|---|
| <b>New Laws</b>   |
| <b>Indonesia</b><br> |
| <b>Thailand</b><br>  |



# Dangers in Cross Border Data Transfers

---



Is my Data protected enough?  
Is my Data safely processed?  
Is my Data safely stored?

**Benefits versus Dangers in  
Cross-Border Transfer of Data**



# “THE CBPR” A SYSTEM THAT CUTS ACROSS JURISDICTIONS

*Cross Border Privacy Rules System*

**Harmonization**  
and  
**interoperability**  
as the way  
forward  
towards  
**consistent**  
**privacy**  
**protections** for  
cross-border  
data flows

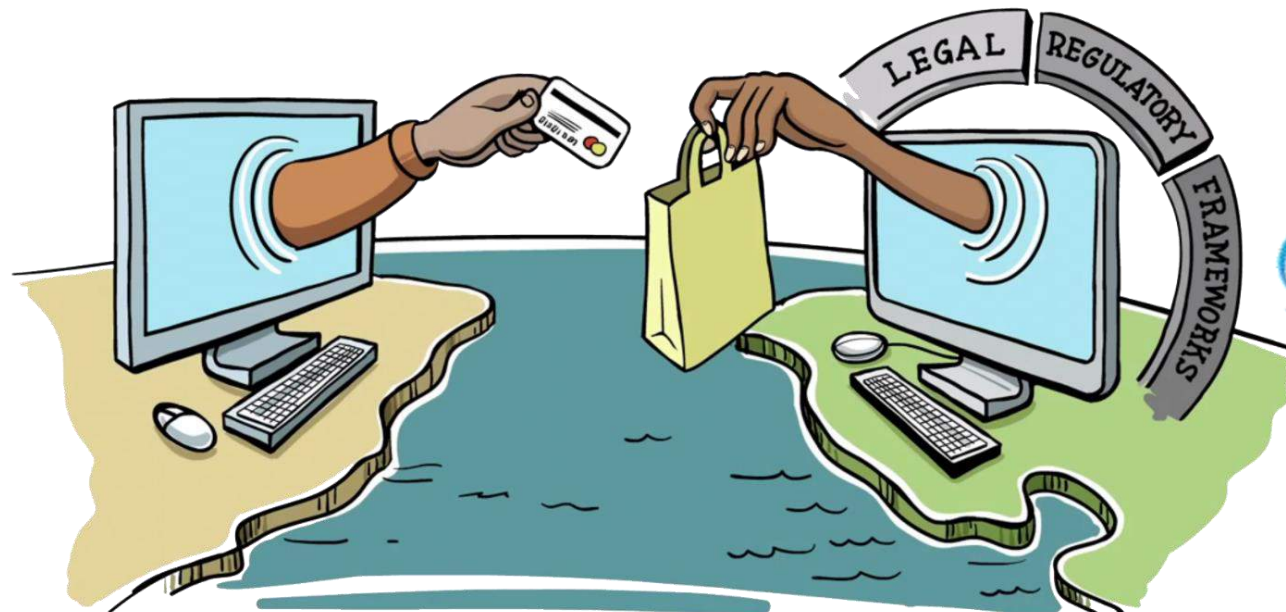
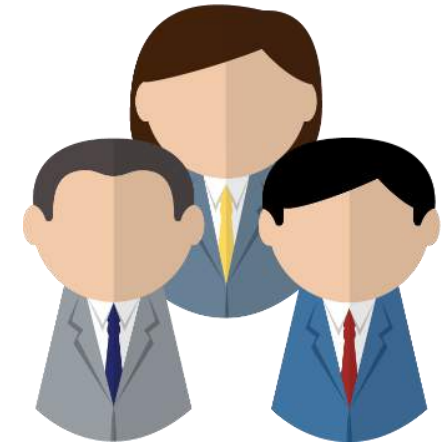
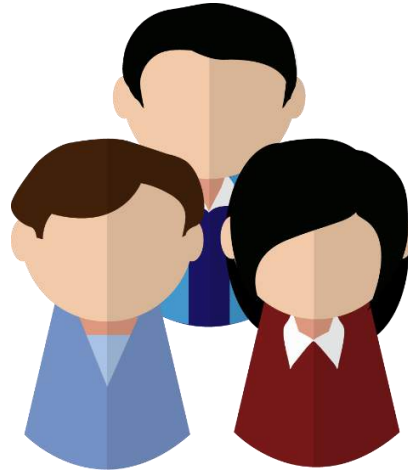


 **CBPRs**  
CROSS BORDER PRIVACY RULES SYSTEM



# MAKING DATA PRIVACY REGULATIONS **INTEROPERABLE**

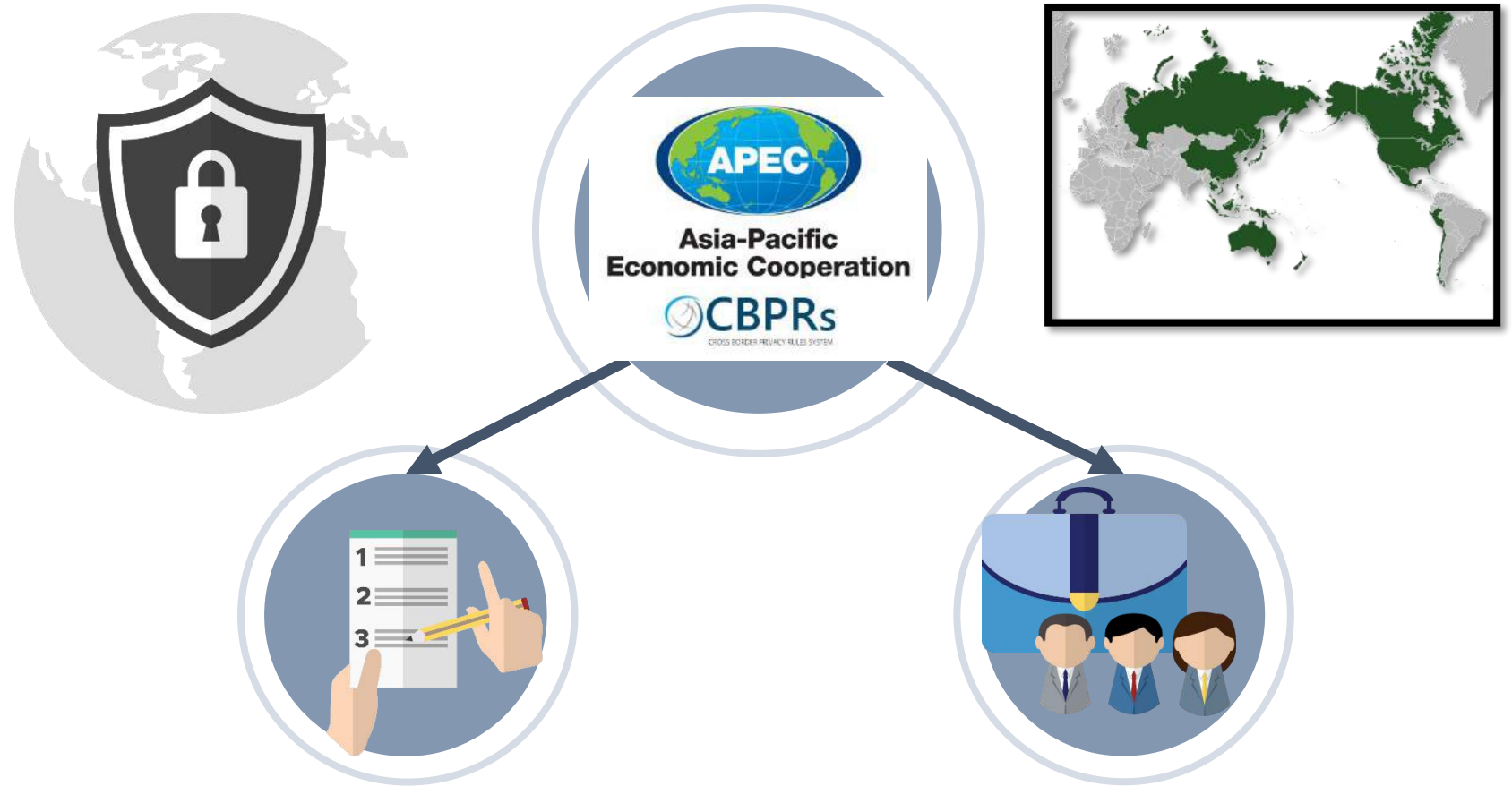
...work together  
**through frameworks  
or set of standards  
that would include  
privacy protections**  
that these privacy  
laws have already in  
common and can  
also include  
additional  
elements mutually  
agreed upon.



 **CBPRs**  
CROSS BORDER PRIVACY RULES SYSTEM

# The APEC CBPR System Explained

A **regional interoperability scheme**. The CBPR System is a **voluntary, accountability based system** that facilitates privacy-respecting data flows among APEC economies.





## What standards are the **CBPR** and **PRP** certifications based on?



- **Accountability**
- **Prevent Harm**
- **Notice**
- **Choice**
- **Collection Limitation**

- **Use of personal information**
- **Integrity of Personal Information**
- **Security Safeguards**
- **Access and Correction**



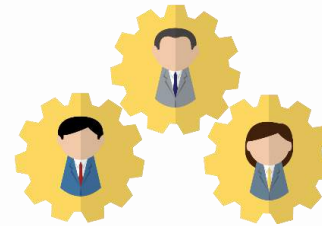
# Benefits of the **CBPR** and **PRP** certification to organizations



- Provide **assurance through third-party certification** that improves and validates your data protection standards.



- **Build trust and confidence** by demonstrating a high-standard commitment to data protection among your business counterparts and customers.



- **Reduce cost and time** with a single and consistent set of privacy standards that facilitates international data flows.
- Demonstrate **good faith compliance** to enforcement authorities



# The APEC CBPR System

**Promoting APEC-EU interoperability** has long been one of the goals of the Data Privacy Sub-group in the APEC.

This led to the development of a **common Referential** for the structure of the APEC and EU systems



## Countries part of the CBPR System



The **Philippines**, through the National Privacy Commission, is now working towards becoming the **9<sup>th</sup> Member Economy** participating in the APEC CBPR System

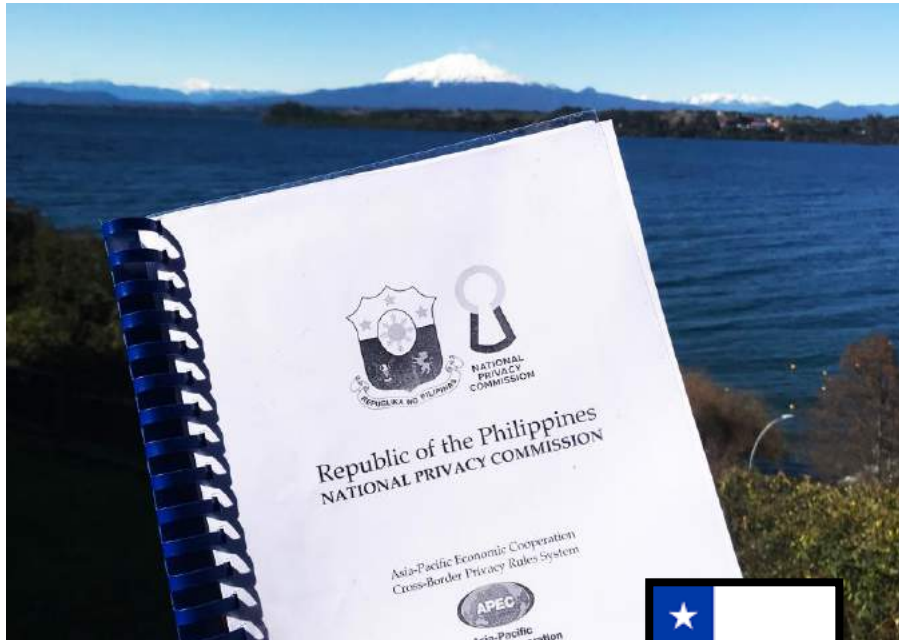




# Philippines and the intent to join the CBPR System



## Countries part of the CBPR System



Puerto Varas, Chile



The National Privacy Commission (NPC) has formally submitted the Philippines' letter of intent to join the CBPR System last 18 August 2019 in Puerto Varas, Chile.





Republic of the Philippines

**DEPARTMENT OF TRADE AND INDUSTRY**

*Trabaho, Negosyo, Konsumer*



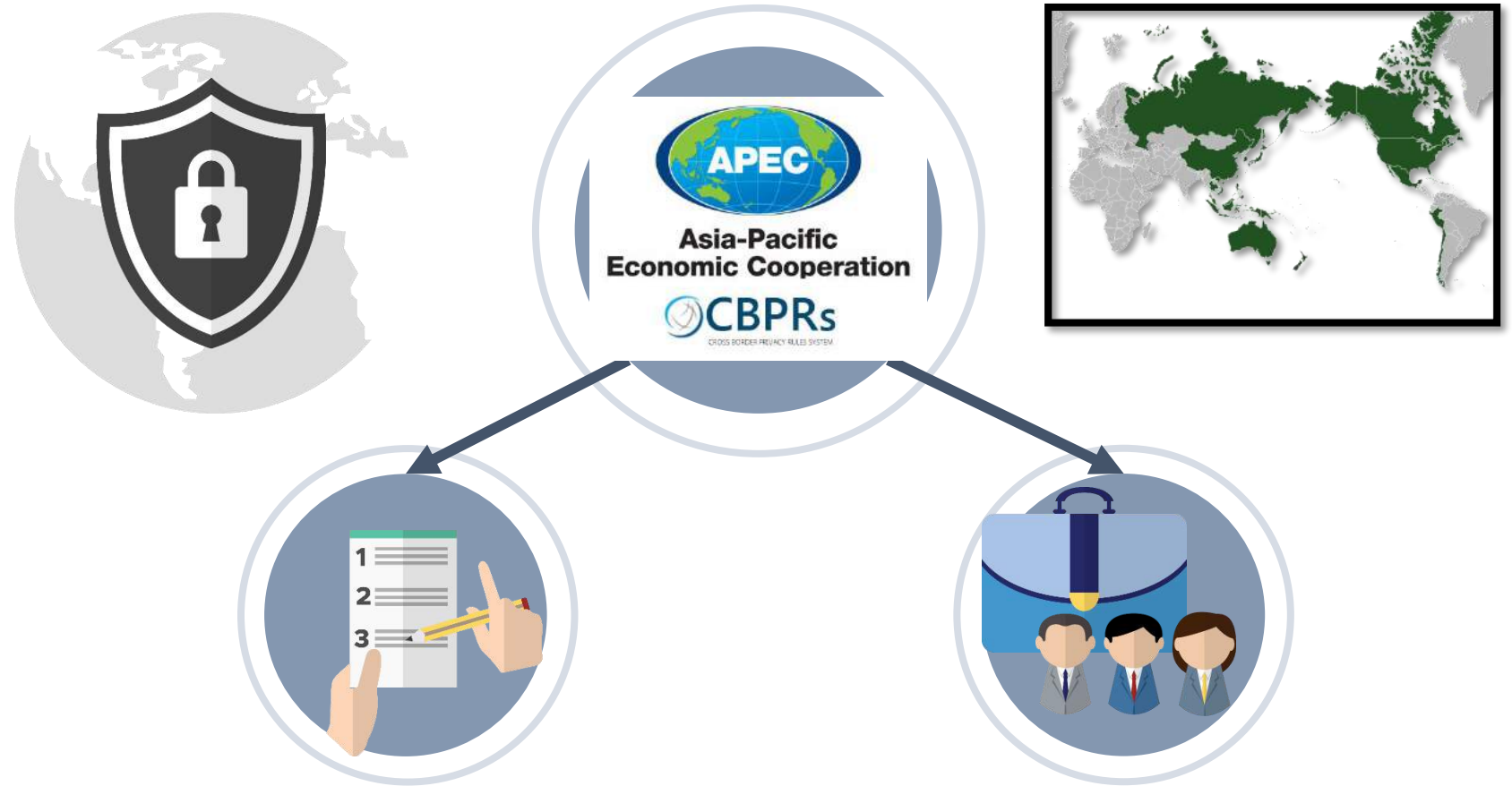






# The APEC CBPR System Explained

A **regional interoperability scheme**. The CBPR System is a **voluntary, accountability based system** that facilitates privacy-respecting data flows among APEC economies.



**Cross Border  
Privacy Enforcement  
Agreement**

**Use of  
Accountability  
Agents**







# Phl chairs ASEAN data privacy forum

The forum ensures that everyone has a seat on the table especially in tackling common issues on data protection and privacy



PRIVACY Commissioner Raymund Enriquez Liboro chairs the ASEAN Data Protection and Privacy Forum in Bangkok, Thailand.

The Philippines spearheaded the first Association of Southeast Asian Nations (ASEAN) Data Protection and Privacy Forum through the chairmanship of Privacy Commissioner Raymund Enriquez Liboro in its inaugural meeting

in Bangkok, Thailand.

The forum, which initiates the harmonization of regional data protection, privacy regulations and initiatives, was attended by all 10 ASEAN member countries, gathering all data privacy regulators and

privacy enforcement agencies and bodies.

It carries the intent to foster sharing of knowledge and best practices, discussion of governance and operational know-how, and development of a framework for enforcement cooperation

"Though ASEAN Member States are in varying stages of development when it comes to their respective data protection and privacy regimes, the Forum ensures that everyone has a seat on the table especially in tackling common issues on data protection and privacy," Liboro said in his welcome remarks.

Developments and updates on the proposals about Data Classification Framework and Cross Border Data Flow Mechanism for ASEAN were also tackled during the meeting with the increasing global concern over data privacy.

ASEAN member states also use the forum to exchange views and information on data protection and privacy matters which include enforcement cooperation. Seeking to harmonize data protection and regulation, the Forum comes as at a juncture in ASEAN history when privacy and data protection is becoming an important concern.

"The ASEAN must harness technologies and digital innovation to its advantage through effective policies that will enable greater movement of data and ease of market access that will bridge the digital divide among the Member States and at the same time, provide guidance to its digital citizens in protecting their data," Liboro said.

By RAINIER ALLAN RONDA

Raymund Liboro, National Privacy Commission (NPC) commissioner, said that the NPC was an active participant in the first ASEAN Data Protection and Privacy Forum in Bangkok, Thailand, since the Philippines helmed the conference, and he chaired the summit's inaugural meeting.

The summit was an important inaugural conference that aims to harmonize regional data protection, privacy regulations and initiatives.

The forum had gathered all data privacy regulators and privacy enforcement agencies and bodies in the ASEAN.



## Phl leads ASEAN data protection efforts

"The ASEAN must harness technologies and digital innovation to its advantage through effective policies that will enable greater movement of data and ease of market access that will bridge the digital divide among the member states and at the same time, provide guidance to its digital citizens in protecting their data. We must ensure that everybody can benefit from the digital economy and that no one is left behind. That is the ASEAN Way," Liboro said in his welcome remarks.

With the increasing global concern over privacy, "responsible data stewardship and data management across the

region will protect and benefit all our citizens and certainly boost the region's competitiveness," Liboro added.

Representatives from all 10 ASEAN Member States (AMS) were present as key decisions on priority areas for cooperation and the scope of work of the regional summit were made. Developments and updates on the proposals about Data Classification Framework and Cross Border Data Flow Mechanism for ASEAN were also tackled during the meeting.

The forum will serve as the platform for the AMS to exchange views and information on data protection and privacy

matters, including enforcement cooperation. Seeking to harmonize data protection and regulation, the forum comes as at a juncture in ASEAN history when privacy and data protection is becoming an important concern.

To date, three ASEAN countries have data protection laws and established a data privacy authority regulator.

These are the Philippines, Singapore, and Malaysia. Just recently, Thailand passed its own data protection law, while other states in the region such as Indonesia are in various stages of developing their own data protection and data privacy laws.





# 2022

## Road to a Data Privacy Nation



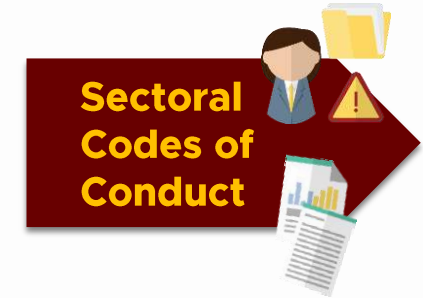
- (1) Appoint a DPO
- (2) Know your Risks: Conduct a Privacy Impact Assessment
- (3) Create a Privacy Management Program and Privacy Manual
- (4) Demonstrate accountability and compliance
- (5) Breach Management



- Data Protection Officer Training and Certification Program
- Philippine **Privacy Trust Mark**



- Cross-border Privacy regulations
- General Data Protection Regulation adequacy
- Bilateral Agreements



- Sectoral Codes of conduct







# Thank you for listening!

[facebook.com/privacy.gov.ph](https://facebook.com/privacy.gov.ph)  
[twitter.com/privacyPH](https://twitter.com/privacyPH)  
[info@privacy.gov.ph](mailto:info@privacy.gov.ph)



# **APEC PRIVACY RECONIGATION FOR PROCESSORS SYSTEM**

## **Self-Assessment Form**

## 1. General Information

|                                  |  |
|----------------------------------|--|
| Name of Organisation             |  |
| Name of point of contact for PRP |  |
| Title                            |  |
| Email Address                    |  |
| Contact Number                   |  |
| Company Registration Number      |  |

## 2. APEC PRP System

List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you.

| Name of subsidiary and/or affiliate | Location of subsidiary and/or affiliate | Relationship of subsidiary and/or affiliate to you |
|-------------------------------------|---|--|
|                                     |   |  |
|                                     |   |  |
|                                     |   |  |
|                                     |   |  |

For what offering(s) or type(s) of processing service(s) are you applying for recognition?

## SECURITY SAFEGUARDS (QUESTION 1 – 8)

| S/N | Questions  | Assessment Requirements (AR)  | AR Met?   | Applicant's response / supporting documents and details |
|-----|--|---|---|---|
| 1   | Has your organization implemented an information security policy that covers personal information processed on behalf of a controller? | Where the Applicant answers <b>YES</b> , the Accountability Agent must verify the existence of this written policy.<br><br>Where the Applicant answers <b>NO</b> , the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.  | <input type="checkbox"/> Yes<br><input type="checkbox"/> No |   |
| 2   | Describe the physical, technical and administrative safeguards that implement your organization's information security policy.         | Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: <ul style="list-style-type: none"> <li>• Authentication and access control (e.g. password protections)</li> <li>• Encryption</li> <li>• Boundary protection (e.g. firewalls, intrusion detection)</li> <li>• Audit logging</li> <li>• Monitoring (e.g. external and internal audits, vulnerability scans)</li> <li>• Other (specify)</li> </ul> The Applicant must periodically review and reassess these measures to evaluate their relevance and effectiveness.<br><br>Where the Applicant indicates that it has <b>NO</b> physical, technical and administrative safeguards, or inadequate | <input type="checkbox"/> Yes<br><input type="checkbox"/> No |   |

|   |   |   |   |  |
|---|---|---|---|--|
|   |   | safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.  |   |  |
| 3 | Describe how your organization makes employees aware of the importance of maintaining the security of personal information. | The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: <ul style="list-style-type: none"> <li>• Training program for employees</li> <li>• Regular staff meetings or other communications</li> <li>• Security policy signed by employees</li> <li>• Other (specify)</li> </ul> Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such | <input type="checkbox"/> Yes<br><input type="checkbox"/> No |  |

|   |   |  |   |                  |
|---|---|--|---|------------------|
| 5 | Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above?   | The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.  | <input type="checkbox"/> Yes<br><input type="checkbox"/> No | Please describe. |
| 6 | Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information?                               | The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.  | <input type="checkbox"/> Yes<br><input type="checkbox"/> No |                  |
| 7 | Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the | Where the Applicant answers <b>YES</b> , the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information.<br><br>Where the Applicant answers <b>NO</b> , the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle. | <input type="checkbox"/> Yes<br><input type="checkbox"/> No |                  |