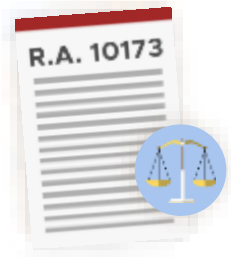
Compliance to the DPA

A Guide for PIPs

NATIONAL PRIVACY COMMISSION

DP FOR THE BPO INDUSTRY 5

Legal Basis



Section 14. Subcontract of Personal Information. – A personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

Implementing Rules and Regulations, RA 10173

Section 43. Subcontract of personal data.

Section 44. Agreements for outsourcing.

Section 45. Duty of personal information processor. The personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

DATA PRIVACY ACT OF 2012

How Can an Organization Comply?

STEP 1: **Appoint a** Data Protection Officer

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

STEP 2: **Conduct a Privacy Impact Assessment (PIA)**

A privacy Impact Assessment (PIA) is a process undertaken and used by a company or agency to evaluate and manage the impact of it's program process and/or measure on data privacy.

STEP 3: **Create Privacy Management Framework**

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

STEP 4: **Implement Privacy and Data Protection Measures**

The measures laid out in your privacy and data protection policies should not remain theoretical. They must continously be assessed, reviewed, and revised as necessary, while training must be regularly conducted.

STEP 5: **Exercise Breach Reporting Procedures**

Upon the discovery of a personal data breach, or reasonable suspicion thereof, it is important to conduct an initial assessment of the breach, to mitigate it's impact, and to notify both the affected data subjects and the National Privacy Commision (NPC) within 72 hours of discovery.

STEP 6: **Register your company with the National Privacy Commission (NPC)**

Registration with the NPC is up-to-date and contains all necessary compliance documentation. Registration includes all automated processing operations that would have legal effect on the data subject. Provide annual report which summarize documented security incidents and personal data breaches.

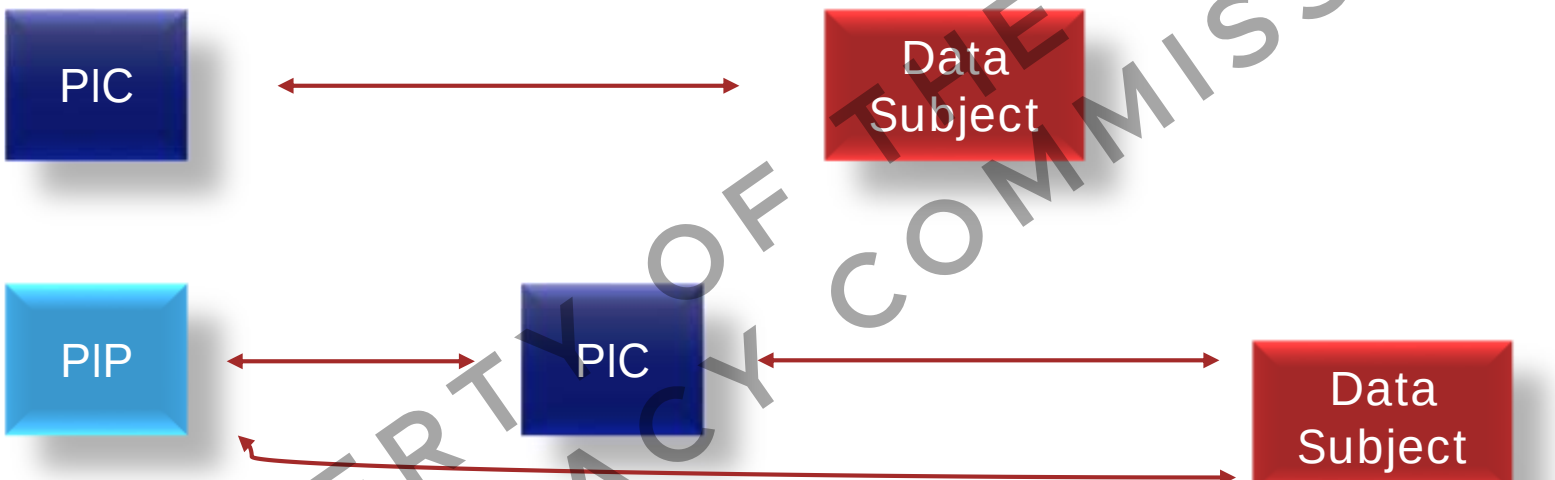
info@privacy.gov.ph

privacy.gov.ph

NATIONAL PRIVACY COMMISSION

DP 5

PICs vs PIPs



Sabre Breach May Have Exposed Payment Data at 36,000 Hotels

By Jeff Goldman, Posted May 4, 2017

The company recently identified unauthorized access to payment information processed through its SynXis Central Reservation system.

The travel technology company Sabre Corp. has acknowledged that its hotel reservation system was recently breached, according to investigative reporter Brian Krebs.

The breach affects a platform that Sabre says is used by more than 36,000 hotels worldwide.

In its most recent quarterly filing with the SEC, the company stated, "We are investigating an incident involving unauthorized access to payment information contained in a subset of hotel reservations processed through the Sabre Hospitality Solutions SynXis Central Reservation system."

PICs vs PIPs

	DPO	PIA	PMP	PDP	BRP	REG	
PIC	✓	✓	✓	✓	✓	✓	PH and others
PIP	✓	w/PIC	✓	✓	w/PIC	✓	PH and others

PICs vs PIPs

	DPO	PIA	PMP	PDP	BRP	REG	
PIC	✓	✓	✓	✓	✓	✓	PH and others
	?	?	✓	✓	?	✓	Non-PH only
PIP	✓	w/PIC	✓	✓	w/PIC	✓	PH and others

NATIONAL PRIVACY COMMISSION

DP FOR THE BPO INDUSTRY 5

PICs vs PIPs

	DPO	PIA	PMP	PDP	BRP	REG	
PIC	✓	✓	✓	✓	✓	✓	PH and others
	?	?	✓	✓	?	✓	Non-PH only
PIP	✓	w/PIC	✓	✓	w/PIC	✓	PH and others
	?	?	✓	✓	w/PIC	✓	Non-PH only

NATIONAL PRIVACY COMMISSION

DPO FOR THE BPO INDUSTRY

RULE #1

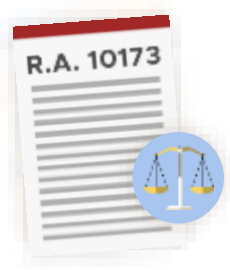
Commit to Comply: Appoint a **Data Protection Officer** (DPO).

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

NATIONAL PRIVACY COMMISSION

DP FOR THE BPO INDUSTRY 5

Legal Basis



Section 21 (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act.

PIP considerations:

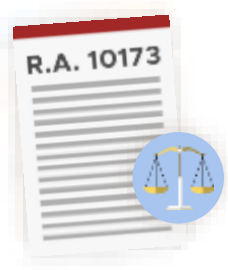
- Are you servicing a government agency, regulated industry, EU company?
- Would having a DPO give you competitive advantage?
- During an investigation or inquiry, if there is no DPO, the default DPO is the highest-ranking person in the organization.
- Separate internal DPO from external DPO.

RULE #2

Know Your Risks: Conduct a **Privacy Impact Assessment** (PIA).

A **Privacy Impact Assessment** (PIA) is a process undertaken and used by a government agency to evaluate and manage the impact of its program, process and/or measure on data privacy.

Legal Basis



Section 20 (c) “The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.”

PIP Considerations:

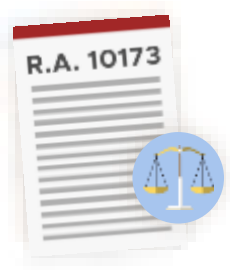
- Before you sign the contract, know your risks.
- **Conduct a PIA (good) or participate in the PIC’s** PIA process (better).
- Employees who are aware of the risks will be more vigilant.

RULE #3

Write Your Plan: 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 in mitigating the impact of a data breach.

Legal Basis



Section 12. The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists (a-f):

Section 13. The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases (a-f):

PIP Considerations:

- Transparency – **was the data you're** processing obtained properly by the PIC?
- Legitimate Purpose – does the PIC have a legal purpose for the processing?
- Proportionality – is the PIC collecting data **which doesn't seem to be needed for** processing?

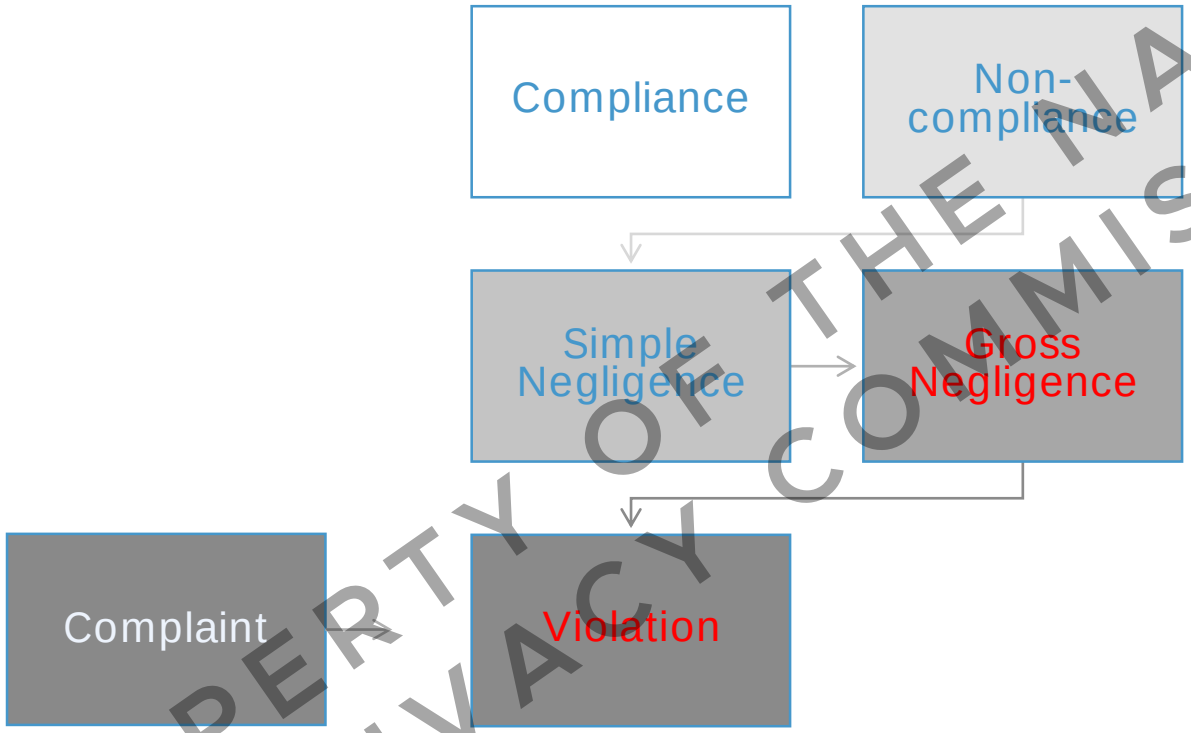
Are there exemptions?

- IRR, Section 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:
  - f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules

The information is exempt, but you are not...

- Consider an example where medical data is collected from a patient in a foreign country, then the data is sent to the Philippines to be converted to digital format.
- *Is consent required for digitizing the information? NO*
- HOWEVER,
  - if the data is improperly disclosed
  - if the data accuracy is altered
  - if the data availability is impacted
- *YOUR company can become the subject of a data privacy complaint.*

Compliance

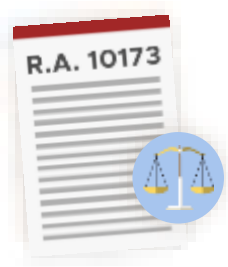


RULE #4

Be Accountable: Implement your **privacy and data protection** (PDP) measures.

The 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.

Legal Basis



Sections 16-18. (Rights of the data subject)
Section 20. (Security obligations)

PIP Considerations:

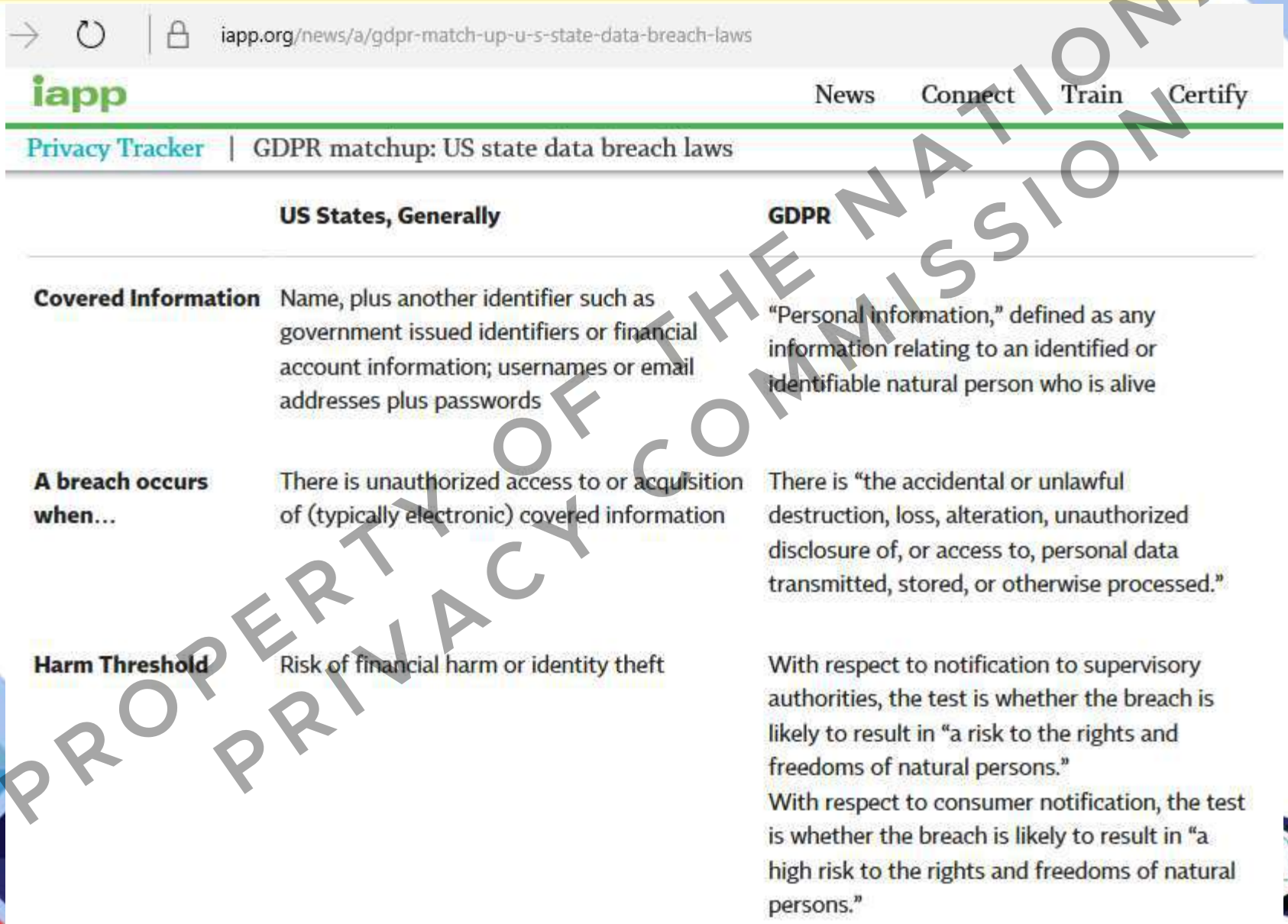
- Contract should specify service level agreements for handling requests for access, correction, rectification, removal, etc.
- Contract should specify data protection measures (organization, physical, technical) to protect against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.
- Conduct regular drills to test security and business continuity measures.

RULE #5

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

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

Legal Basis



iapp.org/news/a/gdpr-match-up-u-s-state-data-breach-laws

iapp News Connect Train Certify

Privacy Tracker | GDPR matchup: US state data breach laws

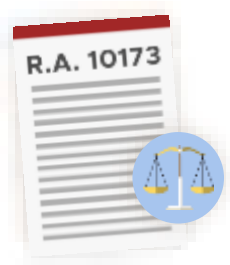
	US States, Generally	GDPR
Covered Information	Name, plus another identifier such as government issued identifiers or financial account information; usernames or email addresses plus passwords	"Personal information," defined as any information relating to an identified or identifiable natural person who is alive
A breach occurs when…	There is unauthorized access to or acquisition of (typically electronic) covered information	There is "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."
Harm Threshold	Risk of financial harm or identity theft	With respect to notification to supervisory authorities, the test is whether the breach is likely to result in "a risk to the rights and freedoms of natural persons." With respect to consumer notification, the test is whether the breach is likely to result in "a high risk to the rights and freedoms of natural persons."

Notification Requirements (Regulatory)	**Timing:** Varies by state ranging from 2 to 90 days, with 30-45 being more common when specific timing required; otherwise, "without unreasonable delay." **Content:** (1) Description of incident in general terms, (2) types of covered information affected by breach, (3) remedial or protective steps taken, (4) contact information for the organization. **Method:** Varies by state; postal delivery usually accepted, although some states prefer email or online submission and fax numbers available for others.	**Timing:** "Without undue delay" and "where feasible, not later than 72 hours after having become aware [of the breach]." **Content:** (1) Nature of the breach including approximate number of data subjects and records concerned, (2) contact information for controller's DPO, (3) description of the likely consequences of the breach, and (4) measures taken to remediate or mitigate potential negative effects. **Method:** Not specified.
Notification Requirements (Consumer)	**Timing:** Varies; for states with deadlines, typically between 30-45 days unless special classes of covered information are at risk, such as health information; other states "without unreasonable delay." **Content:** Typically the same as for regulatory notification, but including advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. Note Massachusetts prohibits sharing facts or circumstances that lead to breach.	**Timing:** "Without undue delay." **Content:** A description "in clear and plain language" of the nature of the breach and items (2)-(4) of the regulatory notification. **Method:** Not specified.

Legal Basis

Breach Definition	A notifiable breach occurs when sensitive personal information or any other information, whether recorded in a material form or not, that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.	Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.
Breach Notification	The National Privacy Commission and affected data subjects shall be notified by the personal information controller within 72 hours upon knowledge of or when there is a reasonable belief by that an unauthorized acquisition of sensitive personal information is likely to give rise to a real risk of serious harm to any affected data subject. A real risk of serious harm includes whether any information may, under the circumstances, be used to enable identity fraud.	The GDPR requires assessment of data incidents and prompt notification of the breach to data subjects when there is a high risk to the rights and freedoms of natural persons and, with respect to supervisory authorities, notification when the breach is likely to result in a risk to the rights and freedoms of natural persons.

Legal Basis



IRR Section 38 (a) The Commission and affected data subjects shall be notified by the PIC within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

PIP Considerations:

- Contract should specify service level agreements and protocols for breach management.
- Employees should know what constitutes a breach, and be vigilant in reporting at the earliest sign of a possible breach.
- Breach team should be formed, educated on what steps to perform, and conduct regular drills to ensure reporting obligations can be met.

LAST: Registration

NOTE on Registration (from Circular 17-01):
PIC or PIP shall provide the following registration information to the NPC by Sept. 9, 2017:

name and contact details of the PIC or PIP, head of agency or organization, and DPO

LAST: Registration

PIC or PIP shall provide the following registration information to the NPC by March 8, 2018:

A. purpose or mandate of the government agency or private entity;

B. identification of all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;

C. attestation regarding certifications attained by the PIC or PIP, including its relevant personnel, that are related to personal data processing;

D. brief description of data processing system or systems:

   a. name of the system;

   b. purpose or purposes of the processing;

   c. whether processing is being done as a PIC, PIP, or both;

   d. whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;

   e. description of the category or categories of data subjects, and their personal data or categories thereof;

   f. recipients or categories of recipients to whom the personal data might be disclosed; and

   g. whether personal data is transferred outside of the Philippines;

E. notification regarding any automated decision-making operation.

"In the digital age, privacy issues can impact millions of people around the world. It's imperative that regulators work together across borders to ensure that the privacy rights of individuals are respected no matter where they live," said Commissioner Daniel Therrien of the Office of the Privacy Commissioner of Canada.

"My office was pleased to work with the FTC and the Office of the Canadian Privacy Commissioner on this investigation through the APEC cross-border enforcement framework," said Australian Privacy Commissioner Timothy Pilgrim. "Cross-border cooperation and enforcement is the future for privacy regulation in the global consumer age, and this cooperative approach provides an excellent model for enforcement of consumer privacy rights."

To facilitate cooperation with its Canadian and Australian partners, the FTC relied on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

Let's work together!

ET tech | From the newsroom of the Economic Times | Startups | Technology | Corporate | Mobile | Internet | People | Principal Partner TATA COMMUNICATIONS

E-commerce • Digital Payments • Interviews • Funding • Smartphones • Govt policy • Long Reads • Social Media • Search

Technology News / Latest Technology News / Technology

Personal data may only be transferred to third countries where the EU has considered the laws to provide adequate protection or where protected by binding corporate rules, approved model clauses, binding agreements combined with an approved code of conduct or approved certification.

According to Nasscom, the apex body of India's IT sector, getting India declared as a data-secured country will increase revenues from the EU to the extent of $7 billion (Rs 38,350 crore) annually by way of increased offshoring and cost savings to companies leveraging India in their business model.

various apps.

India from the 'biggest ransomware' attack

NATIONAL PRIVACY COMMISSION

DP FOR THE BPO INDUSTRY 5

privacy.gov.ph

NATIONAL PRIVACY COMMISSION

privacyPH

Personal Data Processing. More safe in the

Philippines.