DATA

PRIVACY AND PROTECTION

Second Activity

July 24, 2025

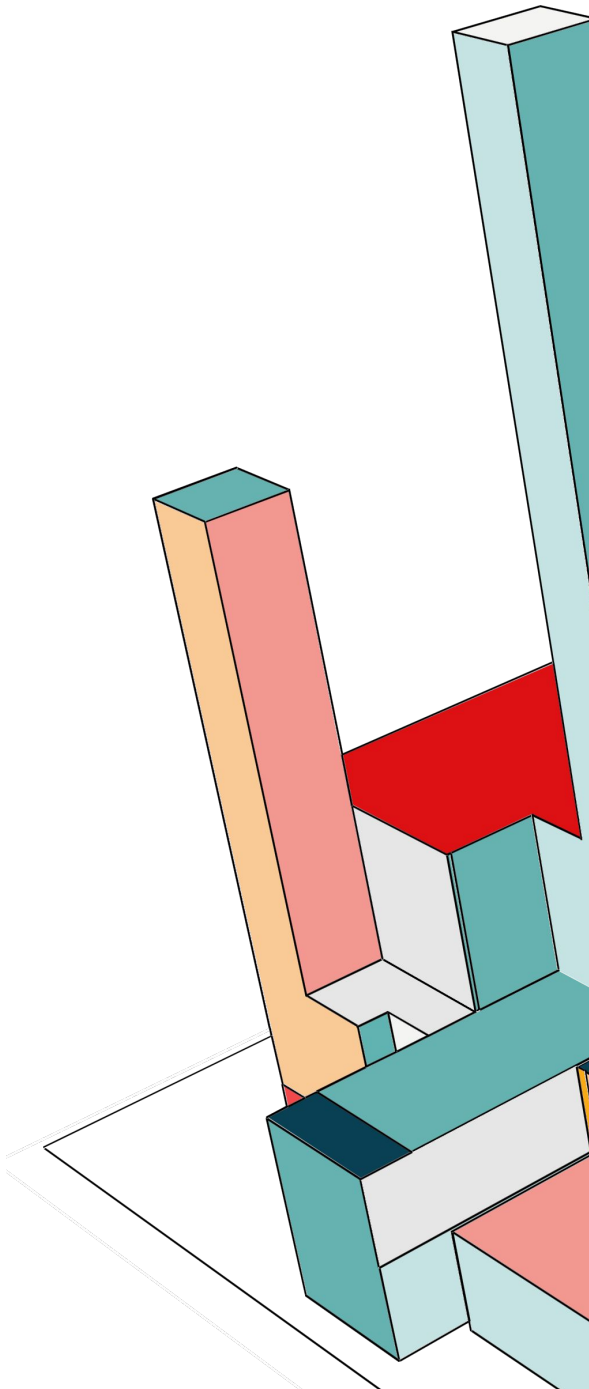
DEFINE THE FOLLOWING:

- ## Data Privacy

  Data privacy refers to the right of individuals to control how their personal information is collected, used, and shared. It focuses on ensuring that personal data is handled responsibly and only for the purposes agreed upon by the data subject.

- ## Data Protection

  Data protection involves the measures and strategies put in place to safeguard data from unauthorized access, breaches, loss, or corruption. This includes technical and organizational actions such as encryption, firewalls, access controls, and compliance with legal standards.



GENERAL DATA PROTECTION REGULATION (GDPR)

- Definition

The GDPR is a legal framework established by the European Union that sets guidelines for the collection and processing of personal information from individuals who live in the EU.

- Area and Scope

> Applies to all organizations processing the personal data of individuals residing in the EU, regardless of the organization's location.

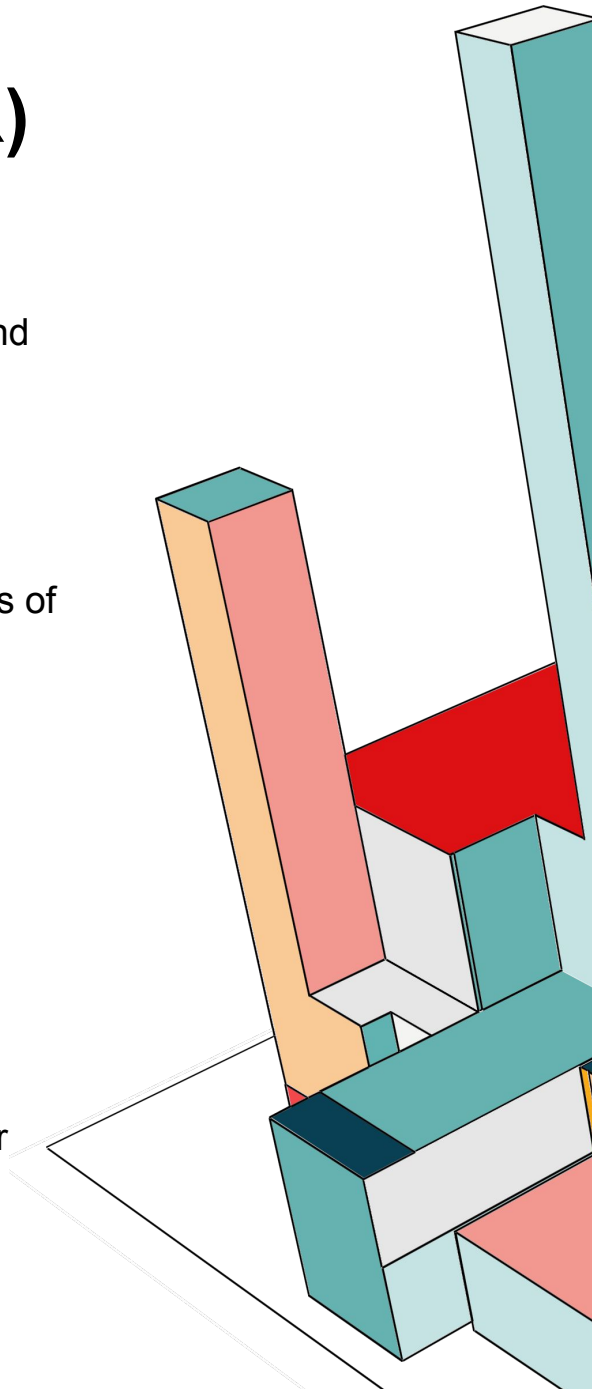
> Covers both data controllers and processors.

- Processes

> Requires lawful basis for data processing (e.g., consent, contract).

> Mandates data minimization and accuracy.

> Obligates organizations to maintain records and conduct Data Protection Impact Assessments (DPIAs) for high-risk processing.



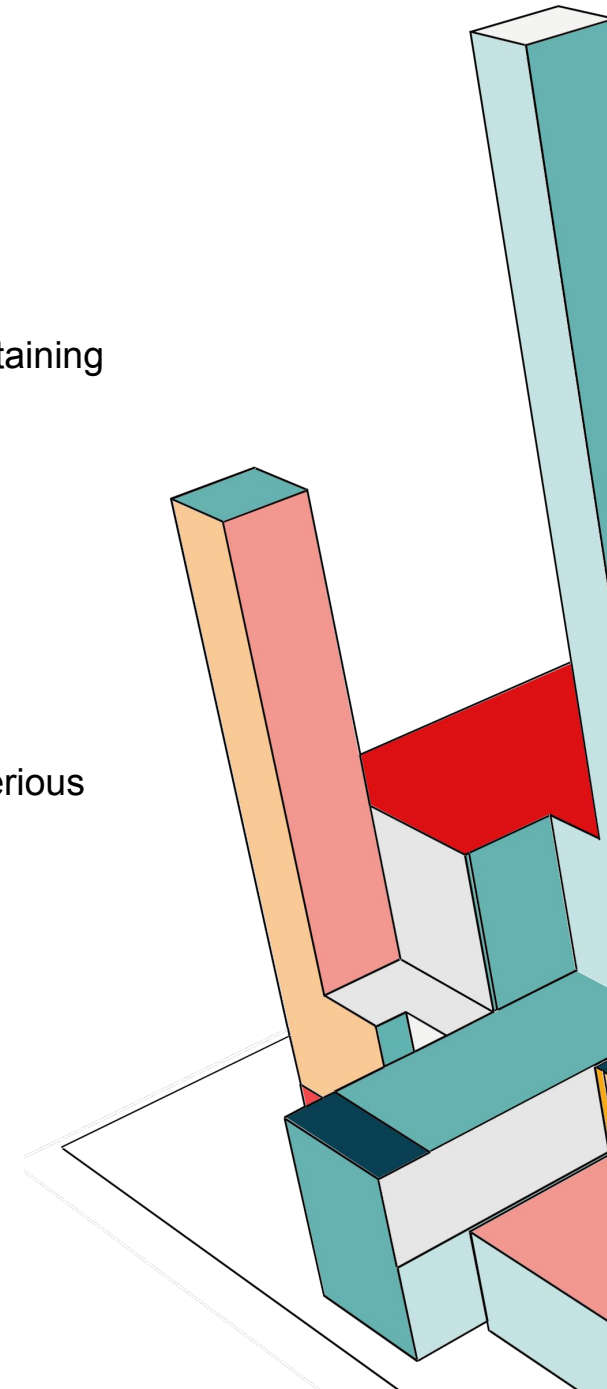
- Involve ICT Professionals

ICT professionals play a role in implementing secure data systems, managing data breach responses, maintaining GDPR-compliant data infrastructure, and ensuring data portability and erasure capabilities.

- Enforcement and Penalties

> Enforced by Data Protection Authorities (DPAs) in EU member states.

> Organizations may be fined up to €20 million or 4% of global annual turnover, whichever is higher, for serious breaches.



CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

- Definition

The CCPA is a state-level privacy law in California that gives consumers more control over the personal information businesses collect about them.

- Area and Scope

> Applies to for-profit businesses that do business in California and meet certain thresholds (e.g., $25 million+ annual revenue).

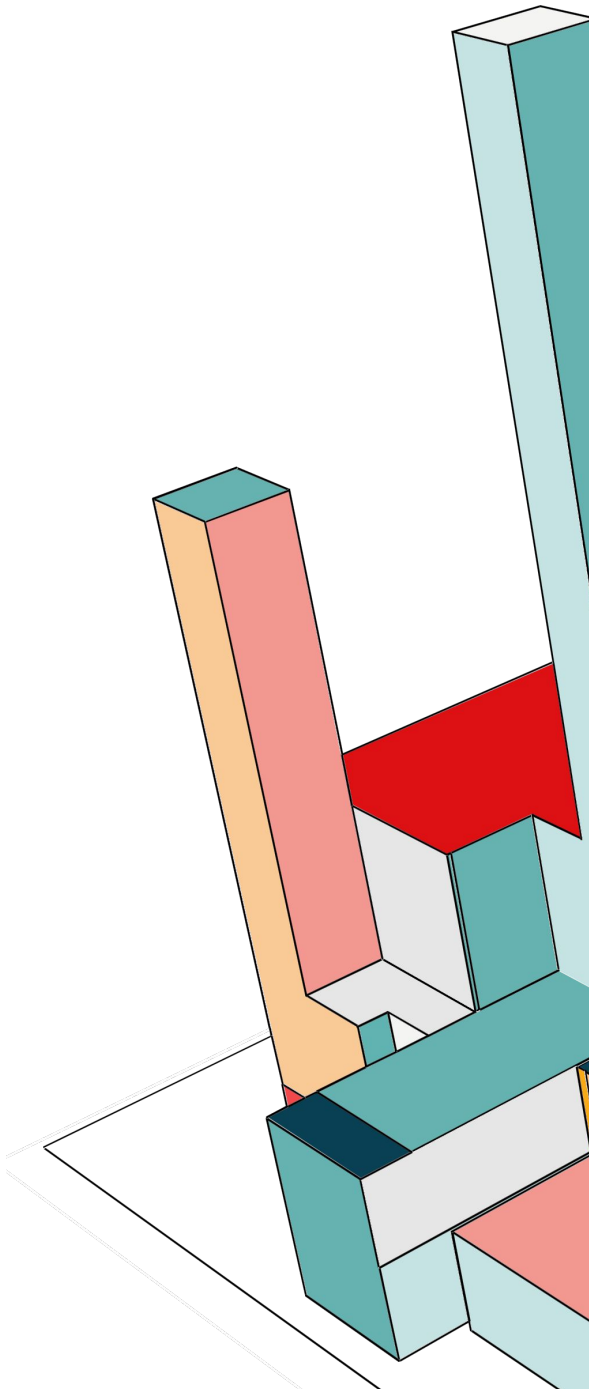
> Focuses on California residents' personal data.

- Processes

> Grants rights to access, delete, and opt out of the sale of personal data.

> Requires transparency in data collection and usage.

> Businesses must update privacy policies and provide clear consumer rights notices.



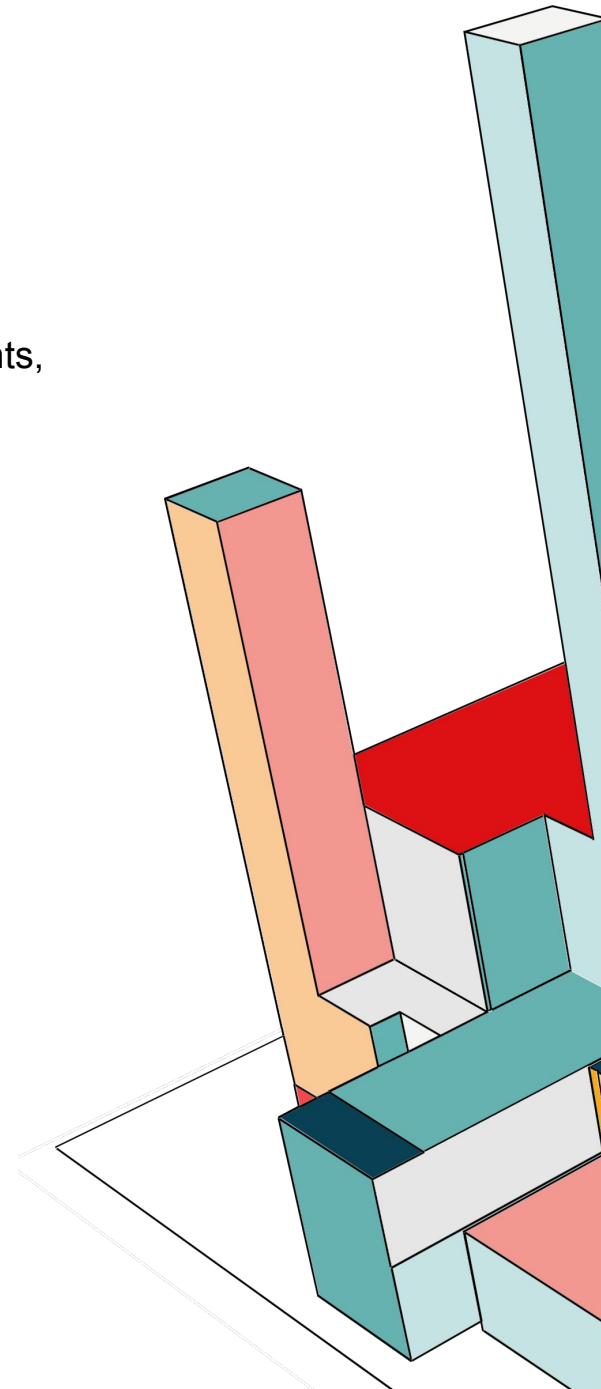
- Involve ICT Professionals

ICT teams are responsible for designing and maintaining systems that allow consumers to exercise their rights, securing data infrastructures, and logging data access requests.

- Enforcement and Penalties

> Enforced by the California Attorney General and the California Privacy Protection Agency (CPPA).

> Penalties can reach up to $7,500 per intentional violation and $2,500 for unintentional violations.



PERSONAL DATA PROTECTION ACT (PDPA)

- Definition

The PDPA is a data protection law that governs the collection, use, and disclosure of personal data by organizations in a manner that recognizes both the individual's right to protect their personal data and the organization’s need to collect, use, or disclose it for legitimate purposes.

- Area and Scope

> Applies to all private organizations that collect personal data.

> Covers electronic and non-electronic data.

> Does not typically apply to public agencies or data processed outside commercial activities.

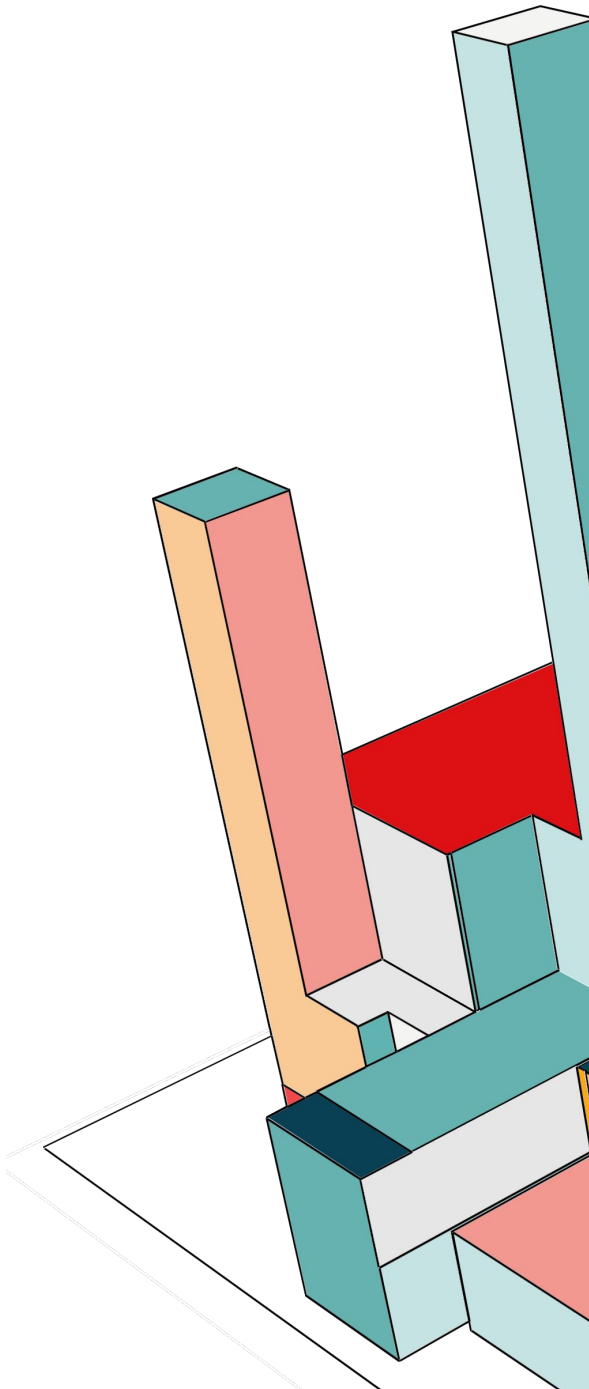
- Processes

> Organizations must obtain consent before collecting data.

> Data must be used only for purposes stated.

> Individuals have the right to access and correct their data.

> Companies must develop a data protection policy.



- Involve ICT Professionals

> Responsible for ensuring technical measures (e.g., encryption, secure servers).

> Must assess system vulnerabilities.

> Maintain records of consent and access controls.

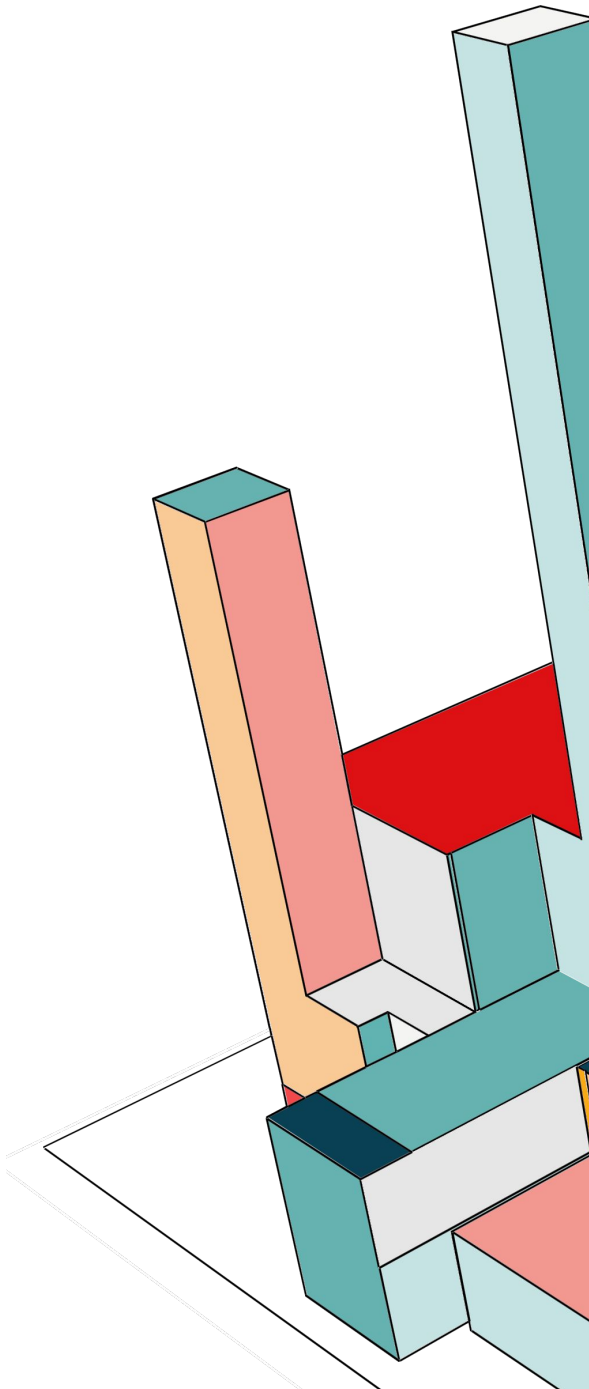
> Develop secure data management infrastructure.

- Enforcement and Penalties

> Handled by the Personal Data Protection Commission (PDPC).

> Financial penalties up to millions depending on severity.

> Non-compliance may also lead to reputational damage and restrictions.



DATA PRIVACY ACT OF 2012

- Definition

A law that protects the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.

- Area and Scope

> Applies to all individuals and entities in the Philippines.

> Covers personal and sensitive personal information.

> Applies to both government and private sector.

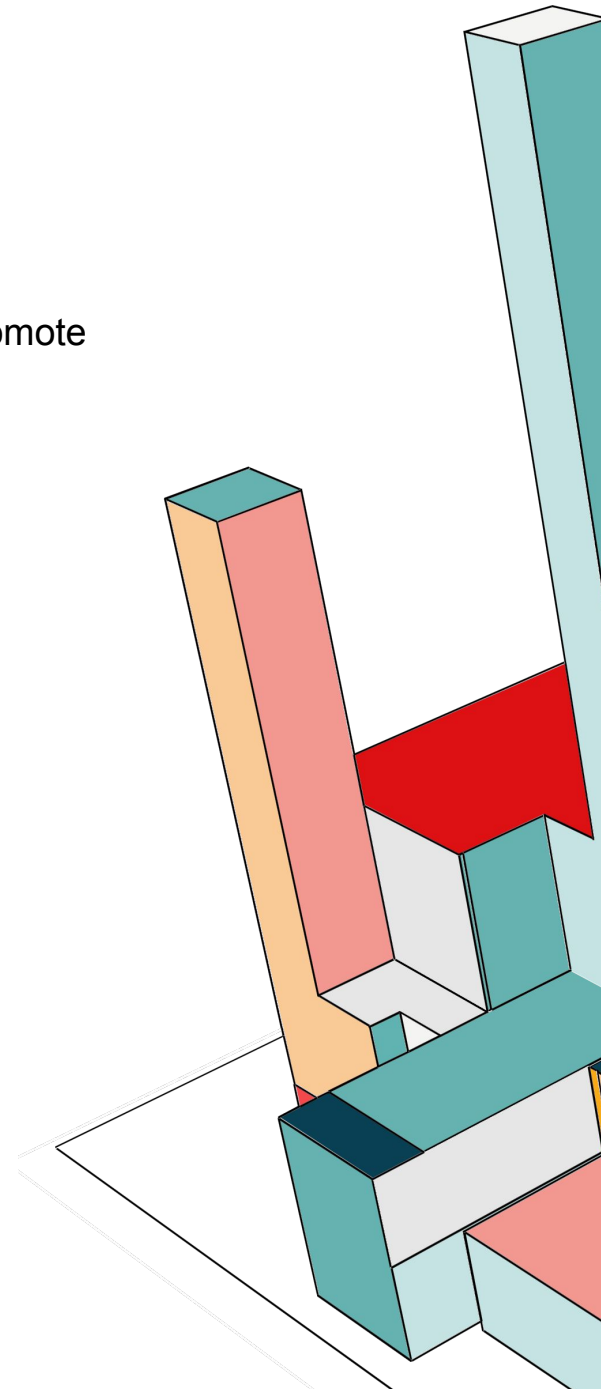
- Processes

> Requires consent before data processing.

> Organizations must appoint a Data Protection Officer (DPO).

> Regular risk assessments and privacy impact assessments.

> Report data breaches to the National Privacy Commission (NPC) within 72 hours.



- Involve ICT Professionals

> Set up systems to secure data transmission and storage.

> Ensure encrypted communication and access control.

> Monitor for intrusions and system vulnerabilities.

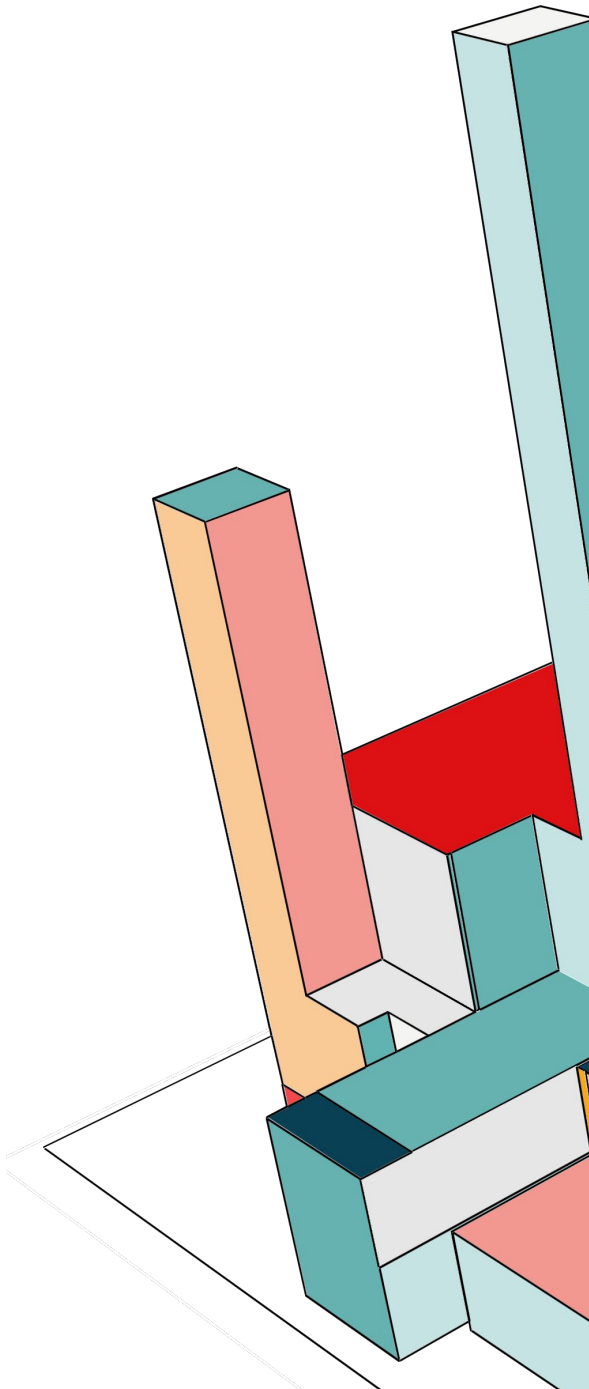
> Support in creating breach response strategies.

- Enforcement and Penalties

> Enforced by the National Privacy Commission (NPC).

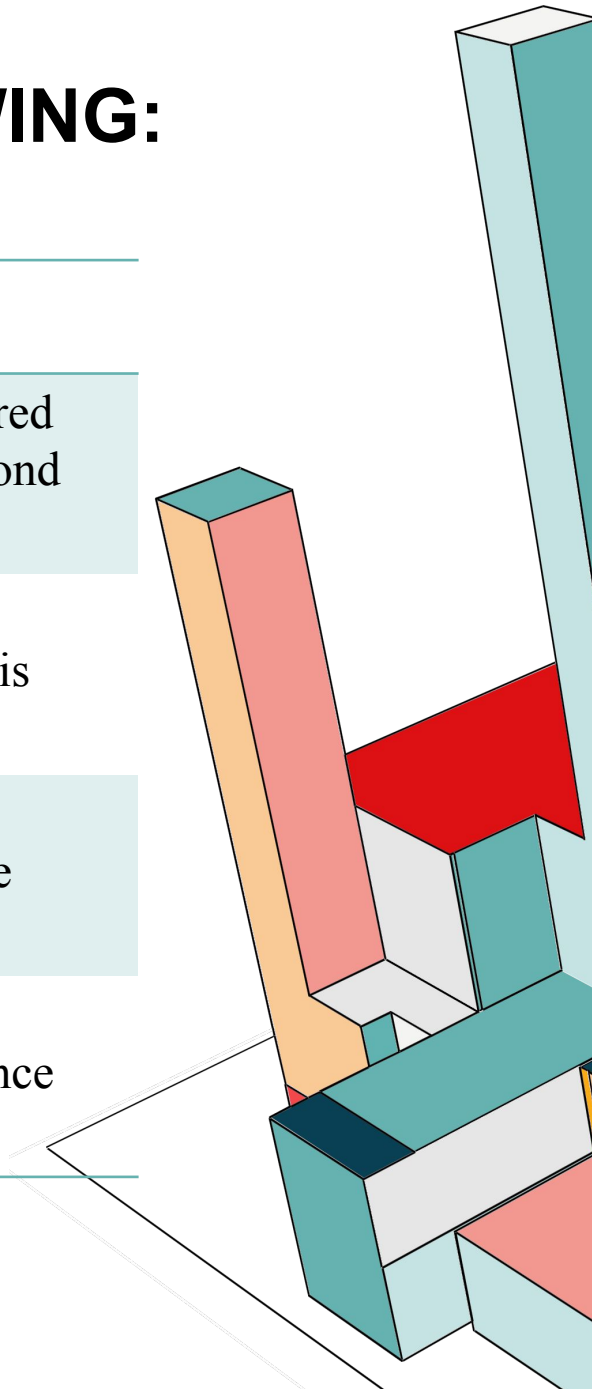
> Penalties range from ₱500,000 to ₱5 million or more.

> Includes imprisonment for serious violations (e.g., unauthorized access, malicious disclosure).



PROVIDE ETHICAL CHALLENGES ON THE FOLLOWING:

Data Collection	Data Storage	Data Sharing
Informed Consent: Users may not fully understand what data they are agreeing to share.	**Security Risks:** Improper storage can lead to breaches.	**Third-Party Misuse:** Shared data may be exploited beyond intended use.
Over-Collection: Collecting more data than necessary.	**Retention Duration:** Storing data longer than needed raises privacy concerns.	**Lack of Consent:** Users unaware of who their data is shared with.
Deceptive Practices: Data gathered without transparency.	**Data Ownership:** Unclear who owns the stored data.	**Cross-border Transfer:** Different jurisdictions have different standards.
Minors and Vulnerable Groups: Extra sensitivity required, often overlooked.	**Cloud Storage Ethics:** Storing in third-party systems may conflict with privacy assurances.	**Loss of Control:** Original collector loses oversight once data is shared.



EXAMPLES OF PRIVACY VS. SECURITY TRADE-OFFS

1. CCTV in public areas: Reduces crime but records individuals without consent.

2. Airport body scanners: Helps detect threats but scans bodies revealing personal data.

3. Employee monitoring software: Increases company data security, but intrudes on employee privacy.

4. Contact tracing apps (COVID-19): Protects public health but collects location and health data.