Introduction to Data Privacy

WESTERN LEYTE COLLEGE OF ORMOC CITY, INC.
WISDOM LEADERSHIP COMMITMENT
FOUNDED
1945
• ORMOC CITY •

Topics

- Data Privacy
- Importance of Data Privacy
- Differences Between Data Privacy, Security, and Protection
- Fundamental Privacy Principles

Data Privacy

- Data privacy, also known as “information privacy”, refers to the rights and expectations of individuals to control how their personal information is collected, used, and shared.
- Ensuring data privacy helps maintain trust between individuals and organizations, supports compliance with legal regulations, and upholds ethical standards in data handling.

Importance of Data Privacy

- Protects Personal Information
  - Personal data includes sensitive information such as names, addresses, financial details, medical records, and online activities.
  - **Example**

    A data breach at a bank can expose customer financial information, leading to fraudulent transactions.

Ensures Compliance with Laws and Regulations

- Governments and regulatory bodies enforce data privacy laws to protect individuals' rights.

- Organizations must comply with laws like:

  - GDPR (General Data Protection Regulation) – EU law protecting user data.

  - CCPA (California Consumer Privacy Act) – Protects California residents' personal information.

  - HIPAA (Health Insurance Portability and Accountability Act) – Safeguards medical records in the U.S.

Builds Trust Between Businesses and Consumers

- Prioritize data privacy to gain customer trust and loyalty.
- Customers are more likely to do business with companies that respect their privacy and handle data responsibly.
- Example

  A social media platform that transparently explains how user data is used will attract more trust compared to one involved in data scandals.

Prevents Data Breaches and Cyberattacks

- Strong data privacy policies help protect against hacking, phishing, and ransomware attacks.

- Cybercriminals exploit weak data protection to steal and sell personal information on the dark web.

- Example

  In 2021, a major data breach at Facebook exposed 533 million users' personal data, which was later found on hacker forums.

Protects Freedom and Prevents Discrimination

- Misuse of personal data can lead to discrimination based on race, gender, health status, or financial history.

- Data privacy helps prevent mass surveillance, government overreach, and unauthorized tracking of individuals.

- Example

  Employers using AI-powered hiring systems must ensure personal data isn't used unfairly in hiring decisions.

Data Security

Data security refers to the technical measures and practices used to protect data from unauthorized access, breaches, theft, or corruption. It ensures that sensitive information remains confidential, intact, and available only to authorized individuals.

Types of Data Security

- **Encryption**

  Is the use of algorithms to scramble data and hide its true meaning.

- **Data erasure**

  Is **the process of securely deleting data** so that it cannot be recovered.

- **Data masking**

  Is a technique used to hide real data by replacing it with fictitious but realistic data.

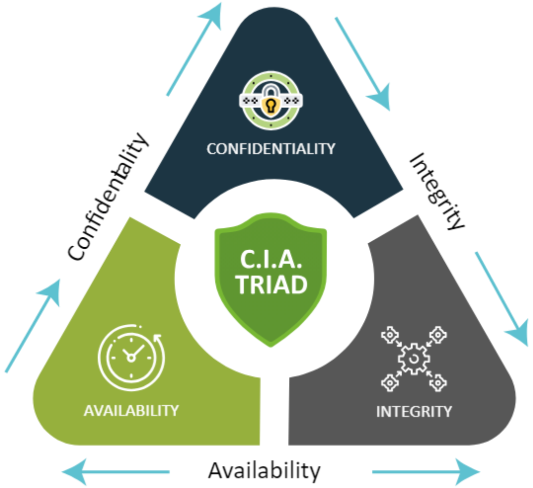
- **Data resiliency**

  Refers to the ability of a system to recover quickly and maintain availability after a disruption, cyberattack, or hardware failure.

Data Protection

Data protection refers to set of practices, policies, and technologies aimed at safeguarding data from loss, corruption, theft, or unauthorized access. It ensures that data remains secure, accurate, and accessible while upholding privacy standards.

The CIA Triad



1 ***Confidentiality***

Ensures that sensitive information is accessed only by an authorized person.

2 ***Integrity***

Ensures that the information is true and correct to its original purpose.

3 ***Availability***

Ensures that information and resources are available to those who need them.

Data Protection

Data protection is vital for regulatory compliance, ensuring organizations follow global data privacy laws like GDPR, CCPA, and the Data Privacy Act to safeguard sensitive information.

Fundamental Privacy Principles

Serve as the foundation for data protection laws and organizational policies to ensure individuals' personal data is handled responsibly.

Privacy Principles

- Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality (Security)
- Accountability

Transparency

- Organizations must inform individuals about how their data is collected, used, shared, and stored.

- Example:

  Privacy policies on websites detailing data practices.

Purpose Limitation

- Personal data should only be collected for specific, clear, and legitimate purposes.

- Example

  A company should not use customer data for advertising if it was collected for account verification.

Data Minimization

- Organizations should only collect the minimum amount of personal data necessary for a specific purpose.

- Example

  A mobile app requiring only an email, not a full address, for account creation.

Accuracy

- Personal data must be kept accurate, up-to-date, and corrected when necessary.

- Example

  Banks allowing customers to update personal details to prevent errors.

Storage Limitation

- Personal data should not be retained longer than necessary for its intended purpose.

- Example:

  A business deleting inactive customer accounts after a set period.

Integrity and Confidentiality (Security)

- Organizations must protect data against unauthorized access, breaches, or loss using strong security measures.

- Example

  Encryption, firewalls, and access controls for sensitive financial data.

Accountability

- Companies and organizations must be responsible for complying with privacy laws and demonstrating their adherence.

- Example

  Appointing a Data Protection Officer (DPO) to oversee compliance with privacy laws.

Legal and Regulatory Frameworks

Legal and Regulatory Frameworks

- General Data Protection Regulation (GDPR) – European Union
- California Consumer Privacy Act (CCPA) – United States (California)
- Data Privacy Act of 2012 (Republic Act 10173)

General Data Protection Regulation (GDPR) – European Union

- Is the toughest privacy and security law in the world.
- It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.
- The regulation was put into effect on May 25, 2018.
- The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

Key Principles of GDPR

- Requires clear user consent before collecting data (*like name, email address, location information, ethnicity, gender, biometric data, web cookies)*.
- Grants users the "Right to be Forgotten" (deleting their data upon request).
- Data breach notifications must be sent within 72 hours.

Key Principles of GDPR

- Enforces strict penalties for violations (up to €20 million or 4% of annual revenue).

- Example Violation

Meta (Facebook) was fined €1.2 billion in 2023 for transferring EU user data to the U.S. without proper safeguards.

California Consumer Privacy Act (CCPA) – United States (California)

- The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them

Privacy Rights for Consumers

- The right to know what data is collected and how it is used.
- The right to opt-out of data sales or sharing of their personal information.
- The right to request deletion of personal information.
- The right to non-discrimination for exercising their CCPA rights.

Privacy Rights for Consumers

- On January 1, 2023, the CCPA added an additional privacy protection, granting new consumer rights to privacy.

  - The right to correct inaccurate personal information that a business has about them; and

  - The right to limit the use and disclosure of sensitive personal information collected about them.

Privacy Rights for Consumers

- Example Violation

  Sephora was fined $1.2 million in 2022 for failing to disclose data tracking and not allowing customers to opt out of data sales.

Data Privacy Act of 2012 (Republic Act 10173) – Philippines

- Is a Philippine law designed to protect the privacy of individuals by regulating how personal data is collected, stored, and processed by both government and private entities, ensuring the secure handling of personal information within information and communication systems across the country.

- Establishes the National Privacy Commission (NPC) to oversee its implementation

National Privacy Commission (NPC)

- The National Privacy Commission, or NPC, is an independent government body in the Philippines created under Republic Act No. 10173 or the Data Privacy Act of 2012

- The Commission is mandated to administer and implement the provisions of the Act, and to monitor and ensure compliance of the country with international standards set for data protection.

Data Privacy Act of 2012 (Republic Act 10173) – Philippines

- Applies to any organization processing personal data of Philippine citizens.

- Key Features
  - Requires Data Protection Officers (DPOs) in organizations
  - Consumers have the right to access, correct, and delete their personal data
  - Imposes penalties on businesses that misuse or fail to protect personal data

Data Privacy Act of 2012 (Republic Act 10173) – Philippines

- Applies to any organization processing personal data of Philippine citizens.

- Key Features
  - Requires Data Protection Officers (DPOs) in organizations
  - Consumers have the right to access, correct, and delete their personal data
  - Imposes penalties on businesses that misuse or fail to protect personal data

Data Privacy Act of 2012 (Republic Act 10173) – Philippines

- Example Violation

COMELEC Data Breach (2016) – The Philippine Commission on Elections suffered a massive voter data leak, exposing 55 million records.

Why Are These Laws Important?

- Protects consumer rights and ensures data is handled responsibly.
- Encourages companies to implement stronger security measures.
- Reduces identity theft, fraud, and unauthorized data use
  Holds organizations accountable for data misuse.