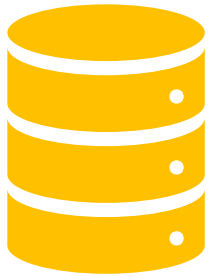
# Module 2

## Identifying and Classifying Sensitive Data

### Objective

Equip participants with the skills to accurately identify and classify different types of data that require protection, ensuring effective and secure data management practices.



# 1
# Data Types

## Definition of the Data Types:

**Personal Data:** Information that can be used to identify an individual, such as names, addresses, and email addresses.

**Sensitive Data:** Data that includes more protected aspects such as health information, racial or ethnic origin, political opinions, and religious beliefs.

**Confidential Information:** Data that must be restricted on a need-to-know basis within an organization, including trade secrets and proprietary information.

# 2

# Methods for Data Classification and Categorization

## Overview of Classification Levels

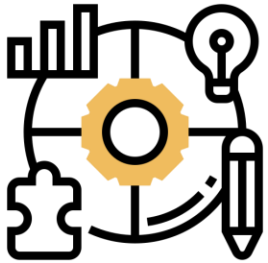
Data classification in data protection typically involves several levels of sensitivity, which help determine how data should be handled and protected. Common levels include:

**Public:** Data that can be made available to the general public without any harm to the organization or individuals. Examples include:

- Promotional materials
- Published reports

**Internal:** Data intended for use within the organization but not harmful if disclosed. This includes:

- Internal newsletters
- Operational procedures.



# 2

# Methods for Data Classification and Categorization

**Confidential:** Data that could cause damage to the organization or individuals if disclosed. This level often includes:

- Customer data,
- Contracts, and
- Personal employee information.

**Strictly Confidential:** Highly sensitive data whose unauthorized disclosure could have severe legal, financial, or security consequences. This includes:

- Social Security numbers,
- Credit card information, and
- Detailed financial records.

# 2

# Methods for Data Classification and Categorization

## Implementing Classification in Practice

By implementing these methods, organizations in the tourism sector can ensure that data is handled securely and in compliance with relevant data protection laws, thereby protecting the organization from legal risks and enhancing customer trust.

- **Policies and Procedures:** Establish clear policies that define each classification level and specify handling requirements. This includes access controls, encryption standards, and disposal methods for each category.

- **Training and Awareness:** Regular training sessions for all employees on the importance of data classification and the specific handling procedures for each category. This helps prevent accidental breaches and ensures consistent application of the classification system.

- **Audits and Monitoring:** Regular audits to ensure compliance with classification policies and to detect any misclassification or unauthorized access to sensitive data. Monitoring tools can also be used to automatically detect and correct classification errors or unauthorized data access attempts.

# 3

# Developing Internal Guidelines for Data Handling and Classification

Create robust internal guidelines that are easily understandable and applicable, enhancing the organization's data security practices.

## Steps for Developing Guidelines

- **Assessment of Data Types:** Begin by identifying and listing all types of data handled by the organization, from customer data to internal emails.
- **Definition of Classification Levels:** Clearly define each classification level and the security measures associated with each level.
- **Guideline Drafting:** Draft the guidelines using clear, concise language. Include examples for clarity and better understanding.
- **Review and Approval:** The draft guidelines should be reviewed by legal, compliance, and data security teams to ensure completeness and compliance with laws.
- **Training and Implementation:** Conduct training sessions for all employees to ensure they understand and can implement the guidelines effectively.

# 4

# Importance of Proper Data Handling Protocols

- **Purpose of Data Collection**

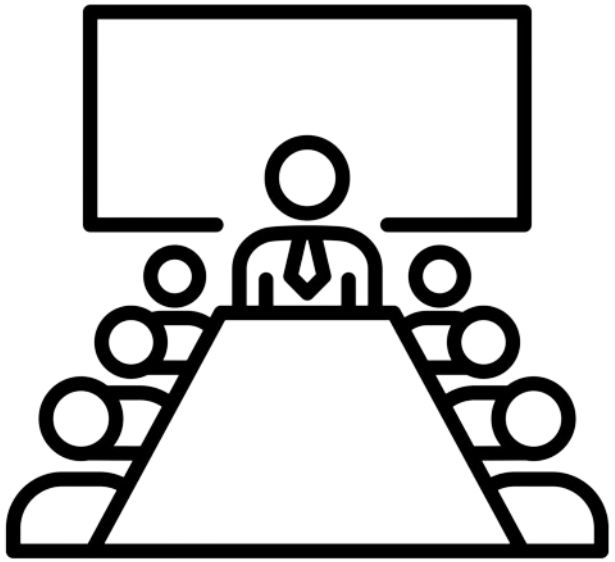
Data is collected across various scenarios, such as course enrollment, employee onboarding, and client engagement, to fulfill specific organizational needs.

- **Data Sharing and Collaboration**

Information gathered may be shared with internal teams or external partners to enhance service delivery, ensure compliance, or assess eligibility for specific programs or benefits.

- **Privacy and Security Protocols**

It is crucial to establish and maintain robust data handling protocols to protect sensitive information, ensure privacy, and comply with legal and ethical standards.



**Security Maintenance:** Proper guidelines help in maintaining data security by standardizing data handling across all operations.

**Compliance Assurance:** Helps ensure compliance with local and international data protection regulations, avoiding legal issues.

**Role Clarity:** Clear guidelines ensure that every team member knows their responsibilities regarding data protection, reducing the risk of data breaches due to human error.

# Importance of Guidelines

# **Case Study:** Office of Personnel Management (OPM) (2015)

**Background:**

The Office of Personnel Management (OPM) in the United States manages the civil service. In 2015, it was discovered that OPM had suffered multiple breaches that exposed the sensitive personal data of millions of current and former federal employees.


**Details of the Breach:**

**Data Exposed:** The breach compromised sensitive information including Social Security numbers, birth dates, home addresses, and more detailed security clearance information, affecting approximately 21.5 million individuals.

**Method of Attack:** Hackers gained access to OPM's database by using stolen credentials to install malware and create a backdoor. The intrusion went undetected for several months, partly due to outdated security practices and a lack of robust detection systems.

# Consequences

- The breach had a profound impact on federal employees, potentially exposing them to identity theft and blackmail, especially those with security clearances.

- OPM faced severe criticism for its inadequate cybersecurity measures. The incident led to the resignation of top officials, including the Director of OPM.

- The response to the breach, including providing credit monitoring to affected individuals and improving the security infrastructure, cost the government hundreds of millions of dollars.

According to Schneier (2017), a consolidated class-action lawsuit was led by the National Treasury Employees Union (NTEU) over the 2015 OPM Hack in the district court in Washington, D.C. Also, a class-action lawsuit by the American Federation of Government Employees consolidated other lawsuits from across the country. *Source (https://www.linkedin.com/pulse/2015-cyber-attack-against-office-personnel-management-jimmy-mora-ms/)*

# Response

In response, the Office of Personnel Management (OPM) implemented several measures aimed at both mitigating the immediate impacts and preventing future incidents. OPM's response included the following actions:

- **Credit Monitoring and Identity Theft Protection:** OPM offered credit monitoring services and identity theft insurance to the impacted individuals. These services were intended to help protect the personal information of those affected by the breach and assist them in recovering if their identities were compromised.
- **Strengthening Cybersecurity Measures:** OPM undertook significant efforts to upgrade its cybersecurity infrastructure. This included enhancing the security of its IT systems, implementing more stringent controls, and improving its ability to detect and respond to security incidents. They focused particularly on protecting high-value assets, though some systems were noted as needing additional security measures like data encryption.
- **Legislative and Policy Changes**: In the wake of the breach, OPM and other federal agencies were prompted to reevaluate and enhance their cybersecurity policies and practices. This included following recommendations from the U.S. Computer Emergency Readiness Team and other cybersecurity bodies to better protect sensitive personal and background investigation information.
- **Continuous Improvement and Oversight:** Post-breach evaluations indicated that while OPM had closed several of the security recommendations made by auditors, others remained open or partially addressed. Ongoing efforts were directed toward closing these gaps and continuously improving the security of OPM's systems.

**Lessons Learned:**

- ✓ Regular audits and updates to security protocols are essential. OPM's systems were found to be outdated and vulnerable to relatively straightforward cyberattacks.
- ✓ The breach highlighted the importance of having advanced intrusion detection systems in place. OPM did not detect the breach for several months, which allowed the hackers to access more data.
- ✓ Post-breach analysis suggested that more stringent access controls and better training on recognizing phishing attempts could have prevented the use of stolen credentials.

As the lead plaintiff in a lawsuit against the Office of Personnel Management (OPM) over its failure to protect employees' personal data that led to one of the largest data breaches in U.S. history, the American Federation of Government Employees (AFGE) reported that a settlement of $63 million has been reached to help data breach victims recover losses.

# Practical Activity

## Data Identification & Classification

**Scenario:**

Loans Marts is preparing to launch a new loan product aimed at small business owners. As part of this launch, the company plans to collect various types of data from applicants, including personal, sensitive, and financial information.

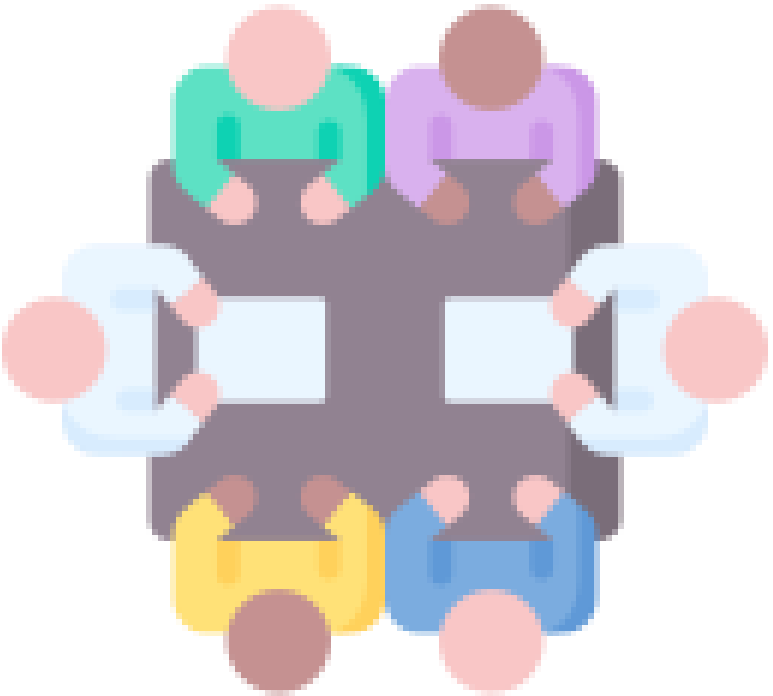
**Task:** A list of data types that Loans Marts will collect during the application process. Your task is to classify each data type into the correct category (Personal, Sensitive, or Confidential) based on the definitions and guidelines provided in this module.

**Data Types to Classify:**

- Applicant's full name
- Business registration number
- Annual revenue of the business
- Personal health information disclosed during the financial assessment
- Email addresses of the business owners
- Ethnic origin of the applicant
- Credit card information used for processing application fees

**Classification Task:** Review each data type listed. Assign each data type to one of the following categories: Personal Data, Sensitive Data, Confidential Information. Justify your classification decision based on the criteria provided in this module.

**Division into Groups**: Participants are divided into small groups to encourage discussion and diverse perspectives. Each group will work together to classify data in various scenarios provided.



That is all for today!

THANK YOU