

DATA PRIVACY & PROTECTION COURSE



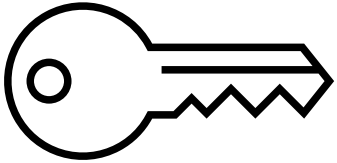
Module 1

Introduction to Data Privacy and Protection

Objective

The primary goal of this module is to help participants understand the fundamental concepts of data privacy and the critical importance of data protection. By the end of this module, learners should be able to define essential terms, understand the legal landscape both locally and internationally, and grasp the impact of data breaches in the tourism sector.





1

Key Terms in Data Privacy and Protection

Data Privacy

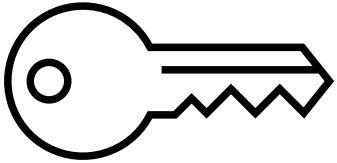
This term refers to the right of individuals to control or influence what information related to them is collected and used by organizations. It's about respecting user preferences regarding their data.

Data Protection

This involves the processes, policies, and technology that organizations use to protect personal data from misuse, unauthorized access, and loss. It ensures data integrity, availability, and confidentiality.

Sensitive Data

This type of data includes any information that can lead to significant consequences if disclosed, such as financial details, health information, personally identifiable information (PII), etc.



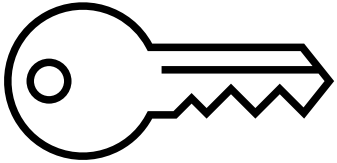
1

Key Terms in Data Privacy and Protection

Data Privacy

This term refers to the right of individuals to control or influence what information related to them is collected and used by organizations. It's about respecting user preferences regarding their data.

- **Opt-In Consent for Marketing Emails:** When you sign up for a new service, the website asks if you would like to receive marketing emails. By checking a box, you explicitly give the company permission to send you promotional content. This respects your right to control how your contact information is used.
- **Adjustable Privacy Settings on Social Media:** Social media platforms allow users to adjust their privacy settings, determining who can see their posts, personal information, and photos. This enables users to control their personal data exposure and manage their privacy according to their preferences.
- **Two-Factor Authentication (2FA):** Services that offer 2FA provide an additional layer of security by requiring not only a password and username but also something that only the user has on them, such as a physical token or a smartphone app to approve authentication requests. This protects sensitive data from unauthorized access.



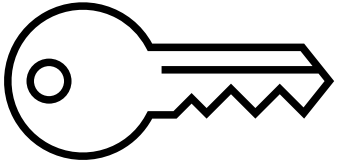
1

Key Terms in Data Privacy and Protection

Data Protection

This involves the processes, policies, and technology that organizations use to protect personal data from misuse, unauthorized access, and loss. It ensures data integrity, availability, and confidentiality

- **Encryption of Sensitive Data:** An organization encrypts sensitive data such as credit card numbers, personal identification numbers, and health records. By converting this information into a secure format that is unreadable without a decryption key, the data is protected against unauthorized access during storage and transmission.
- **Regular Software Updates and Patch Management:** Companies frequently update and patch their software and systems to protect against vulnerabilities. Regular updates ensure that security loopholes are closed, and the system's defenses are up-to-date.
- **Access Control Policies:** Access control mechanisms are used to ensure that only authorized personnel have access to sensitive data. The use of strong authentication methods, such as biometrics or smart cards, enhances the security of these controls.



1

Key Terms in Data Privacy and Protection

Sensitive Data

This type of data includes any information that can lead to significant consequences if disclosed, such as financial details, health information, personally identifiable information (PII), etc.

- **Health Records:** These include medical history, test results, and insurance information, which are confidential and vital for individual privacy and healthcare decisions.
- **Financial Information:** This category encompasses credit card numbers, bank account details, and financial statements that are crucial for financial security and privacy.
- **Social Security Numbers (SSN):** SSNs are used for identification purposes in many administrative systems and are highly sensitive, as their disclosure can lead to identity theft and fraud.

2. Overview of Data Protection Laws in Jamaica

Jamaica's approach to data protection is embodied in the Data Protection Act of 2020, which is designed to secure the confidentiality, availability, and integrity of personal data. The Act outlines requirements for data processing, rights of individuals, and obligations for data controllers and processors. It mirrors many principles found in international standards such as the GDPR, emphasizing accountability and the necessity of having explicit purposes and consent for data processing.

Key provisions include:

- **Consent:** Data subjects must give explicit consent for the processing of their data.
- **Right to Access:** Individuals have the right to access their data and see how it is being processed.
- **Data Minimization:** Only data that is directly relevant and necessary to the intended purposes may be collected.
- **Security Measures:** Adequate technical and organizational measures must be implemented to protect personal data from loss, misuse, unauthorized access, and disclosure.



3

Importance of Protecting Data within a Government Organization

For government organizations responsible for handling a range of sensitive information, protecting data is critical for several reasons:

- 1. Confidentiality of Stakeholder Information:** It is vital to ensure the confidentiality of data from various stakeholders, including citizens, businesses, and other government agencies. Protecting this information helps maintain trust and facilitates cooperation between all parties involved.
- 2. Regulatory Compliance:** Government bodies are legally obligated to comply with stringent data protection regulations to avoid legal and financial consequences. Failure to adhere to these laws can result in penalties, loss of public trust, and severe implications for national and international relations.
- 3. Operational Integrity:** Effective data management and protection are essential for maintaining the operational integrity and effectiveness of government projects. Ensuring data integrity involves preventing unauthorized access and manipulation of data, which is crucial for accurate decision-making and maintaining the functionality of governmental operations.



3

Importance of Protecting Data within a Government Organization

- 4. Security Against Cyber Threats:** With the increasing sophistication of cyber-attacks, government organizations must implement robust cybersecurity measures. This not only protects sensitive information but also secures infrastructure critical to national security and public services.
- 5. Safeguarding National Security:** Many government organizations handle data directly tied to national security. The protection of this data is paramount to prevent threats that could compromise the safety and stability of the country.
- 6. Building Public Confidence:** By demonstrating a commitment to data privacy and security, government organizations can strengthen public confidence and trust. This trust is foundational for effective governance and the successful implementation of policies and projects that rely on public cooperation and support.

Case Study:

JN Group Data Security Incident (2020)

Background

On the morning of Saturday, March 14, 2020, The Jamaica National Group experienced a data security breach due to a cyber-attack on systems through ransomware. On investigation, it was discovered that there was unauthorized access to the system which has impacted the ability to operate as usual.

- The JN Group's Information Technology and Cybersecurity teams immediately acted to contain the effects of the malware and sought to identify the source of the sophisticated attack.
- The Jamaica Constabulary Force's Major Organized Crime and Anti-Corruption Agency, and other security agencies were immediately contacted, to which they respond that they are investigating the matter.

(Source: <https://www.jngroup.com/update/>)



What services have been affected?

- JN Bank ATM and debit card services across the country.
- JN LIVE online banking
- JN Money Online remittance platform
- JN Fund Managers Online facility



Steps taken by JN Group to respond

- ✓ Notified the Police and security agencies locally and overseas
- ✓ Appointed a specialist IT security and forensic provider to investigate the incident
- ✓ Advised relevant banks
- ✓ Advised our credit card supplier, which is doing enhanced monitoring of credit card transactions
- ✓ Undertaken a complete review of our IT systems to further strengthen our infrastructure
- ✓ Implemented a special toll-free phone line to support customers who may have queries
- ✓ Established a process to help customers through this period, which could include credit remediation and identity protection services, such as LifeLock and Identity Force, for a period of six months



That is all for today!

THANK YOU

