A Snapshot of the Data Protection Act

The Data Protection Act, enacted on July 10, 2020, came into partial effect on December 1, 2021, marking the conclusion of a two-year transitional period on November 30, 2023. Presently, the Act is fully operational, with a six-month extension from December 1, 2023, facilitating the completion of implementation and registration with the Information Commissioner.

Territorial Scope: The Data Protection Act applies to data controllers with an establishment in Jamaica or under Jamaican law. It encompasses the processing of personal data within the business context of the establishment. Additionally, the Act extends to businesses not established in Jamaica if they use processing equipment, process the personal data of Jamaican data subjects, or offer services or products to Jamaican data subjects. In the latter case, a data subject must appoint a local representative in Jamaica.

What is Protected? The Act safeguards Personal Data and Sensitive Personal Data. Personal data includes information, either alone or aggregated, identifying a natural person. Sensitive personal data covers biometric data, political and religious ideas, health information, and sexual orientation. The Act outlines eight principles governing data protection obligations.

1. **Lawful and Fair Processing**
2. **Purpose Limitation**
3. **Data Minimization**
4. **Accuracy**
5. **Limited Retention**
6. **Subject Rights**
7. **Security Measures**
8. **Data Transfer Safeguards**

In contrast to the GDPR, there are no obligations on data processors. Data controllers, however, must impose terms for processing personal data on data processors similar to those imposed on controllers.

Who is Protected? The Data Protection Act shields the personal data of identifiable natural living persons for their lifetime plus thirty years. The individual in question is the data subject.

Rights of the Data Subject:

1. **Access to Personal Data**
2. **Consent to Processing**
3. **Prevent Processing**
4. **Consent to Direct Marketing**
5. **Rights in Automated Decision-Making**
6. **Right to Rectification**

Notably, the Act lacks a right to be forgotten, and it's implied that data controllers likely need to appoint a Data Protection Officer. The Officer should be qualified, having a conflict of interest-free status and expertise in privacy implementation and global data protection laws.

Role of the Data Protection Officer:

1. **Ensure Compliance:** Oversee that the data controller processes personal data in compliance with data protection standards and applicable laws.
2. **Consultation:** Collaborate with the Commissioner to clarify the application of the Data Protection Act provisions.
3. **Reporting:** Report any contraventions of the Act to the Information Commissioner if the data controller fails to rectify them.
4. **Assist Data Subjects:** Aid data subjects in exercising their rights under the law.

Data controllers obligated to appoint a Data Protection Officer include public authorities, those processing sensitive personal data or data relating to criminal convictions, or those processing personal data on a large scale. The Office of the Information Commissioner monitors and enforces compliance with the Data Protection Act.