

Complying with the Data Protection ACT

PRESENTED BY:

MR. DAVID GREY, DEPUTY INFORMATION
COMMISSIONER

The Data Protection Act

The Data Protection Act or Act No. 7 -2020 was signed into law by the Governor General on July 10, 2020.

On December 1, 2021 The Hon. Minister brought into operation Sections 2,4,56,57,60,66,74 ,77 as well as the first schedule of the Act.

The Office of the information Commissioner established.

The Data Protection Oversight Committee established.

Jamaica's first Information Commissioner appointed.

Personal data protected by the DPA

Information from which a person (living or deceased less than 30 years) can be identified:

Common identifiers – names, addresses, numbers, contact info

Genetic Data (DNA)

Biometric Data – Physical, Physiological, Behavioral

Sensitive Personal Information – sexual orientation, race, ethnicity, religion, biological relationship, health, membership/association, criminal allegation or proceedings, political opinion, philosophical belief, genetic or biological data



The Role of the Office of Information commissioner

- The Commissioner shall act as the Regulator with regards to the provisions of the Data Protection Act.
- The Act lists the following functions to be discharged:
 - a. Monitoring compliance with the Act and any relations made pursuant to the Act;
 - b. Give advise to the Minister as appropriate on any matter relating to the Act or otherwise for the protection of personal data;
 - c. Promote the observance of requirements to the Act and the following of good practice by data controllers;

— The Role of the office of the Information Commissioner

d. Arrange the method and delivery of information about the Act and its operations and give advice to any person about these matters in a manner the Commissioner thinks appropriate;

e. Prepare and disseminate or direct preparation of guidelines to be adhered to as good practice –where the Commissioner thinks appropriate and after such consultation with bodies which may have an interest in the subject matter as the Commissioner thinks appropriate.



What is Data Protection?

Data protection is concerned with:

- How personal data is used by organizations, businesses or the government;
- Keeping personal data safe from unauthorized access; and
- Empowering individuals to make their own decisions about who can process their personal data and for what purpose.

CORE TERMS

Data Subject

A named or otherwise identifiable individual who is the subject of the personal data



Data Controller

Is any person or public authority who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which personal data are, or are to be, processed



Data Protection Officer

An appropriately qualified person appointed by a data controller who shall be responsible for monitoring in an independent manner the data controllers' compliance with the Data Protection Act.



Data Processor

Any person, other than an employee of the data controller who processes the data on behalf of the data controller.



Process

The Act defines process or processing as obtaining, recording, or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data,



Personal Data

Any information, in the possession of a data controller, relating to an identified or identifiable living individual or an individual who has been deceased for less than 30 years.





Data Subject Rights

1. Right to Access

Data Subjects have the **right to access** information about the collection, use, storage, and disclosure of your personal data by a data controller. Here's what you need to know:

Upon written request, data controllers must provide details of the personal data they collect, its sources, purpose, and potential recipients.

Data controllers are required to respond to your access requests within **30 days**.

2. Right to Prevent Processing

Data Subjects have the right to request that a data controller not process or stop processing your personal data in specific situations:

- **Substantial damage or distress** caused by the Processing.
- Data is **incomplete or irrelevant** for its intended purpose.
- The Processing is **unlawful**.
- Data has been retained **beyond legal requirements**.
- Data controllers must respond to such requests within **21 days**.



3. Right to Data Portability

Data Subjects have the **right to transmit your data** from one data controller to another. The DPA ensures that data is transmitted in a structured and usable format.

4. Right to Avoid Automated Decisions

Decisions about Data Subjects, especially those with legal consequences, should not be made solely through automatic data processing. You have the right to conclusions based on **human review and consideration**. You are entitled to know the logic behind any automated decisions.

5. Right to Rectification

Data Subjects can request the correction of incomplete or inaccurate personal data held by data controllers. Data controllers must take reasonable steps to ensure data accuracy within **30 days**.

Obligations of Data Controllers

Register	Register with the Information Commissioner
Submit	Submit an annual data protection impact assessment
Record/log	Record/log data received and the date and time of any changes thereto
Provide	Provide data subjects who request it with a copy of their data
Comply	Comply with the 8 data protection standards
Report	Report any contravention or security breach to the IC within 72 hours
Notify	Notify every affected data subject of a contravention or security breach



Requirements for registration

Name, address and contact info

Whether a public authority

Name, address and contact info of representative

Name, address and contact info of DPO

Description of data to be processed

Categories of data subjects

Purposes for which data processed

Persons to whom disclosed

Territories to which transferred

Other prescribed information

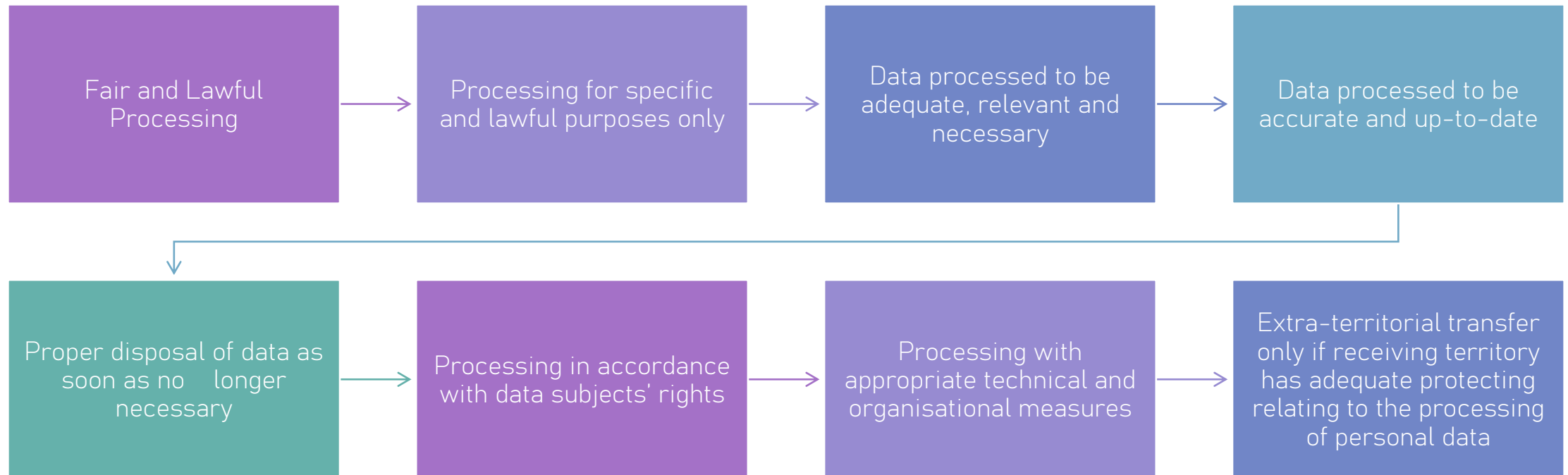
Prepare to Submit Data Protection Impact Assessment

- A data controller is required within ninety (90) days after the end of each calendar year to submit to the Commissioner a Data Protection Impact Assessment in respect of all personal data in the custody and control of the data controller.

The Data Protection Impact Assessment must include the following information –

- A detailed description of the envisaged processing of the personal data and the purposes of the processing, specifying, where applicable the legitimate interest pursued by the data controller.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.
- Please note: A Data Protection Impact Assessment Form will be provided in the Regulations currently being finalized and to be issued before December 1, 2023.

Complying with the 8 Data Protection Standards



Appointment of a Data Protection Officer

A data controller is required to appoint a data protection officer if it is a –

(a) Public authority

(b) Processes or intends to process sensitive personal data or data relating to criminal convictions.

(c) Processes personal data on a large scale; or

(d) Is required by a Commissioner's notice.


Functions of a Data Protection Officer

Ensuring that the Data Controller processes personal data in compliance with each data protection standard and in compliance with the Act and good practice.

Consulting with the Information Commissioner ("the Commissioner") to resolve any doubt about how the provisions of the Act and any regulations made under the Act are to be applied.

Notifying the Data Controller, immediately, that he/she has reason to believe the Data Controller has contravened a data protection standard or a provision of the Act and if he/she is not satisfied that the contravention has been rectified within a reasonable time after notification, report this contravention to the Commissioner.

Assisting data subjects in the exercise of their rights under the Act, in relation to the Data Controller concerned.



Are you a Large-Scale Processor? Do you need to appoint a DPO?

Who is a large-scale processor?

There are several factors data controllers should consider to determine whether they qualify as large-scale processors and need to appoint a DPO. These include:

The volume (in terms of actual quantity) and/or variety (the range or number of different types) of personal data being processed. Example: Insurance companies processing both health and financial information.

The number of individuals to whom the personal data relates and/or the proportion of the subject population represented. Example: Hospitals and other health service providers and educational institutions.

The number of employees processing the personal data and/or the number of locations at which the data is processed. Example: BPOs and financial institutions with hundreds of employees in branches islandwide.

The geographical extent of processing i.e. whether local only or also regional or international. Example: Airline companies and travel agencies processing personal data of travelers in various countries.

Whether the processing involves regular systematic monitoring of individuals' behavior. Example: Internet service providers capturing data for advertising.

How the data is processed i.e. whether the filing system is singular or complex and/or the duration or permanence of the processing including how long data is retained. Example: Financial institutions storing customer data for several years to meet regulatory requirements and provide ongoing financial services.

Penalties for Non-compliance

General:

- Fines up to \$10M
- Imprisonment up to 10 years

For corporations, their officers or members:

- 4% of previous year's annual gross worldwide turnover
- Payable by any or all of the following:
 - a) the entity
 - b) any officer or member proven to be 'guilty'
 - c) Anyone acting in the capacity of an officer or member and proven to be 'guilty'.



Enforcement Mechanism

- Enforcement Notices
- Assessment Notices
- Information Notices
- Fixed Penalty Notices

-
- Service of Enforcement Notice, Assessment Notice, Information Notice and a Fixed Penalty Notice
 - Criminal Prosecution
 - Person – may be subject to imprisonment or fine
 - Where a body corporate commits an offence under the Act, the body corporate shall be liable to a fine not exceeding 4% of the annual gross worldwide turnover of that body corporate for the preceding year of assessment
 - Civil Suit – an individual who suffers damage by reason of any contravention by a data controller of any requirements of the Act is entitled to compensation from the data controller for that damage

Monitoring & Regulation of Data Controllers

Registration – Know who is processing what and how

Tracking – Review DPIAs to know the changes in processing, risks and measures

Assessment – At the request of a DC, determine whether processing activities are in compliance

Investigation – Conduct checks to determine the accuracy of reports, allegations and complaints received including by warrant

Enforcement – Issue of Notices (Enforcement, Assessment, Information, etc.) or initiation of prosecution for breaches/offences

Assessments as a monitoring tool

- Annual DPIAs
- Assessments at the request of a data controller
- Assessments at the request of any individual (possibly, actually or potentially) affected

N.B. Notice by statute or by request

- Controller required to permit/facilitate access to premise, documents, information, equipment, processes and personnel

PSOJ Members: The impact of the Jamaica Data Protection Act (DPA) and What to do now?

Accounting & Auditing:

The impact of the Jamaica Data Protection Act (DPA)

- The DPA may impact financial firms in terms of how they handle client information, especially in auditing processes and managing financial data.

What to do now?

- Ensure strict confidentiality of client financial data.
- Implement robust access controls for financial records.
- Educate employees on data protection and compliance.

Administrative & Support Services:

The impact of the Jamaica Data Protection Act (DPA)

- Businesses in this sector often handle personal information as part of their services, and the DPA would require them to ensure data protection measures are in place.

What to do now?

- Secure customer and employee data.
- Develop data protection policies and procedures.
- Train staff on data protection best practices.

Agriculture:

The impact of the Jamaica Data Protection Act (DPA)

- Agriculture may involve the collection and processing of personal data, especially in areas like employee information or customer data.

What to do now?

- Protect employee and customer data.
- Implement secure data storage and transmission practices.
- Educate employees about data protection.

Arts, Entertainment, Recreation:

The impact of the Jamaica Data Protection Act (DPA)

- Entertainment and event planning businesses may collect customer information, and they must comply with data protection regulations when managing ticket sales, reservations, and marketing.

What to do now?

- Safeguard customer information, especially for ticket sales and reservations.
- Train staff to handle personal data with care.
- Develop a privacy policy and communicate it to customers.

Automotive:

The impact of the Jamaica Data Protection Act (DPA)

- Car dealerships and service centers may collect customer information for sales, service, and marketing purposes, necessitating compliance with the DPA.

What to do now?

- Protect customer data for sales, service, and marketing.
- Implement access controls for customer databases.
- Educate employees about data protection.

Banking, Insurance, and Financial Services:

The impact of the Jamaica Data Protection Act (DPA)

- These sectors deal extensively with sensitive financial and personal data. Compliance with data protection laws is crucial to maintain trust and legal requirements.

What to do now?

- Secure sensitive financial and personal data.
- Comply with international financial data security standards.
- Conduct regular data protection training for employees.

Communication:

The impact of the Jamaica Data Protection Act (DPA)

- Telecommunication companies and media outlets collect and process customer data, so they must ensure compliance with data protection regulations.

What to do now?

- Protect customer data and communications.
- Implement robust cybersecurity measures.
- Educate employees on data protection in communication.

Construction, Engineering, and Real Estate:

The impact of the Jamaica Data Protection Act (DPA)

- These industries may handle employee data, customer information, and supplier data, necessitating data protection measures.

What to do now?

- Secure employee, customer, and supplier data.
- Develop data protection policies for document management.
- Train staff on data protection procedures.

Education:

The impact of the Jamaica Data Protection Act (DPA)

- Educational institutions manage extensive student and staff information, requiring strict compliance with data protection regulations.

What to do now?

- Protect student and staff information.
- Develop strict data protection policies.
- Educate staff and students about data protection.

Energy, Environment, and Climate:

The impact of the Jamaica Data Protection Act (DPA)

- These sectors may collect data related to energy consumption or environmental impact, which requires secure handling and compliance.

What to do now?

- Safeguard data related to energy consumption and environmental impact.
- Comply with data protection regulations for data storage and sharing.
- Conduct employee training on data protection.

Food & Beverage:

The impact of the Jamaica Data Protection Act (DPA)

- Restaurants and food-related businesses often collect customer data for reservations and loyalty programs, and they need to ensure data protection.

What to do now?

- Protect customer data collected for reservations and loyalty programs.
- Develop data protection policies for customer information.
- Train staff on data protection in the food and beverage industry.

Health:

The impact of the Jamaica Data Protection Act (DPA)

- Healthcare organizations handle highly sensitive patient data and must comply with strict data protection regulations.

What to do now?

- Safeguard patient and employee data.
- Comply with healthcare data security standards.
- Provide extensive training on data protection for healthcare professionals.

Legal:

The impact of the Jamaica Data Protection Act (DPA)

- Law firms manage clients' confidential information and must ensure data protection and client confidentiality.

What to do now?

- Protect client confidential information.
- Develop strict data protection policies for law firms.
- Educate legal professionals on data protection in the legal industry.

Manufacturing:

The impact of the Jamaica Data Protection Act (DPA)

- This sector may involve employee data and supply chain information, necessitating data protection measures.

What to do now?

- Secure employee and supply chain data.
- Implement data protection policies for manufacturing processes.
- Train employees on data protection measures.

Marketing:

The impact of the Jamaica Data Protection Act (DPA)

- Marketing agencies often handle customer data for targeted campaigns and must ensure compliance with data protection laws.

What to do now?

- Safeguard customer data used for marketing campaigns.
- Develop data protection policies for marketing databases.
- Educate marketing professionals on data protection

Media:

The impact of the Jamaica Data Protection Act (DPA)

- Media companies collect viewer or reader data and should manage this information in compliance with data protection regulations.

What to do now?

- Protect viewer or reader data.
- Implement cybersecurity measures for media outlets.
- Educate employees on data protection in the media industry.

Mining & Quarrying:

The impact of the Jamaica Data Protection Act (DPA)

- These industries may have employee data and may collect data on mining operations, requiring data protection measures.

What to do now?

- Protect employee and operational data.
- Implement data protection policies for mining and quarrying data.
- Train employees on data protection best practices.

Pharmaceuticals/Cosmetics:

The impact of the Jamaica Data Protection Act (DPA)

- These sectors handle customer and patient data and must ensure compliance with data protection regulations.

What to do now?

- Safeguard customer and patient data.
- Comply with healthcare data security standards.
- Educate employees on data protection in the pharmaceutical and cosmetics industry.

Professional, Scientific & Technical Activities:

The impact of the Jamaica Data Protection Act (DPA)

- Businesses in these sectors may collect and process client data, making data protection crucial.

What to do now?

- Protect client data and sensitive scientific information.
- Develop data protection policies for scientific and technical activities.
- Train employees on data protection practices.

Retail:

The impact of the Jamaica Data Protection Act (DPA)

- Retailers often collect customer data for sales and marketing, necessitating data protection compliance.

What to do now?

- Secure customer data for sales and loyalty programs.
- Develop data protection policies for customer information.
- Train retail staff on data protection measures.

Telecommunication & Technology:

The impact of the Jamaica Data Protection Act (DPA)

- These sectors handle extensive customer data, and compliance with data protection laws is essential to protect user privacy.

What to do now?

- Protect extensive customer data.
- Comply with strict data protection standards in the tech industry.
- Educate employees on data protection in technology and telecommunications.

Training and Consultancy Services:

The impact of the Jamaica Data Protection Act (DPA)

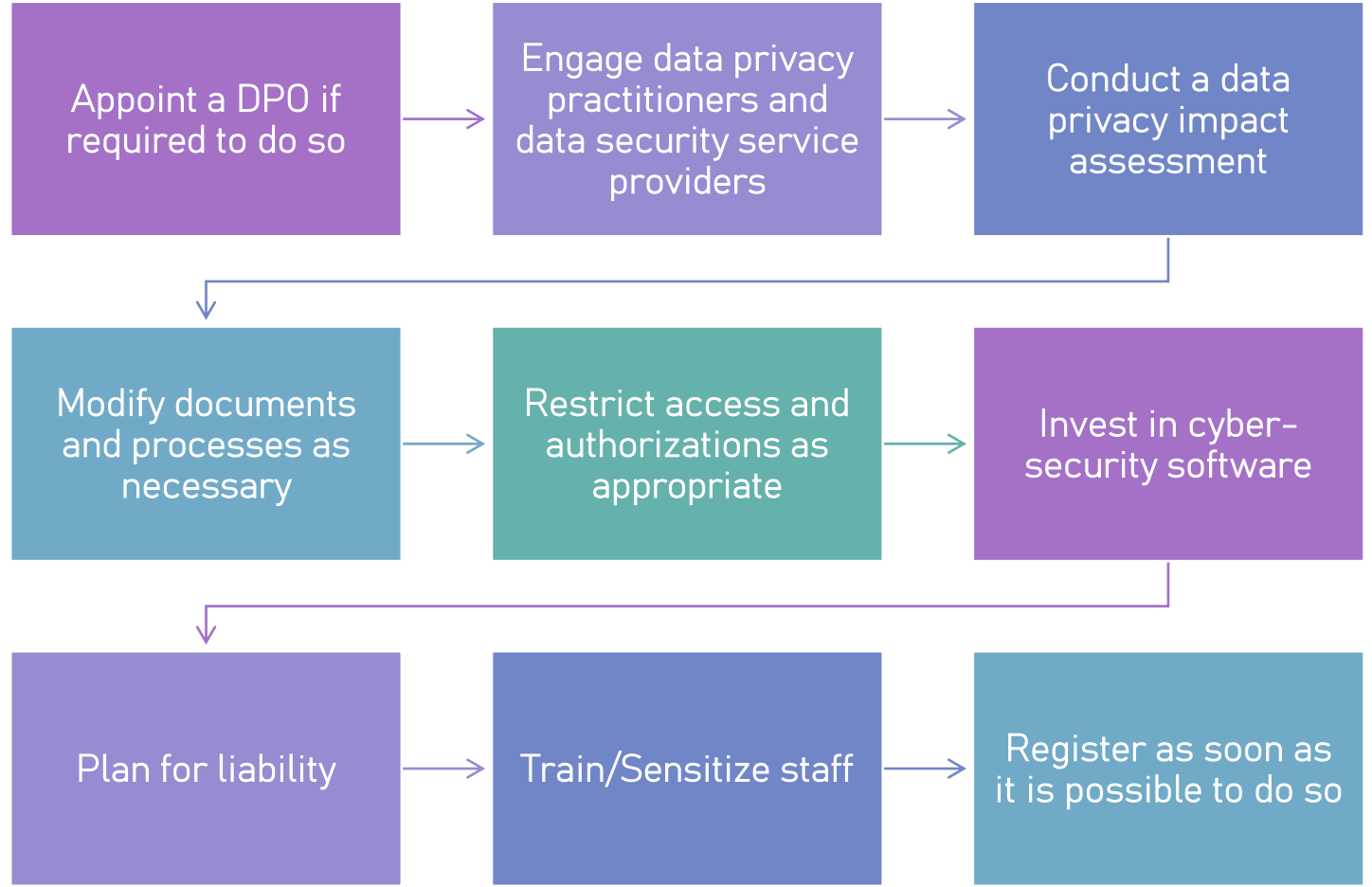
- These businesses may handle client data and must ensure compliance with data protection regulations.

What to do now?

- Secure client and employee data.
- Develop data protection policies for training and consultancy services.
- Train staff on data protection best practices.



What to do now





THE END