G5 Cyber Security

g5cybersecurity.com

Guide

The Jamaica Data Protection Act (JDPA), 2020.

v1.0

Hi there!

This guide was developed by Shaista Peart for G5 Cyber Security, Inc. This guide's purpose is to help educate the public about Jamaica's Data Protection Act of 2020 in simple English terms.

This guide is for informational purposes only and does not constitute legal advice.

We encourage you to send us your feedback to support@g5cybersecurity.com

Get to know Shaista

Shaista Peart, CIPPE

Data Protection and Privacy Consultant

Shaista has experience in the public and private sector. She helps organisations to view data protection and privacy as a business enabler and to build a culture that promotes transparency, accountability, and trust with respective stakeholders.

Shaista is also interested in Smart Homes, Smart Cities and MedTech/SmartHealth. She has a great love for the performing arts and considers herself a musician.

Table of contents

1. Introduction

It is often said that we are now living in the digital and information age. Daily we use technology to shop online, research information, communicate with others and conduct business. While doing these activities, we generate digital footprints that identify us as unique individuals and potentially infringe on our privacy rights.

The generation of these large amounts of personal data highlights the valuable use of data for multiple purposes, such as:

- Businesses gaining insights to improve the products and services they offer.
- The Government using data to carry out its duties more efficiently and cost-effectively.
- Consumers acquiring tailored products and services to improve their quality of life.

These large amounts of data and the growing reliance on it create instances where personal data can be misused and thus requires adequate protection. Consequently, the Jamaican Government has developed the Data Protection Act 2020 to provide stronger privacy rights for individuals and govern how personal data is used.

Some key facts

- There are new compliance obligations for businesses and other entities that process personal data.
- The creation of an Information Commission to oversee and regulate compliance with the Data Protection Act 2020.
- There are new sets of rights afforded to individuals concerning their personal data.
- There are fines and penalties for non-compliance with the Data Protection Act 2020.

2. Key terms and definitions

"Personal data" means information which relates to a **living individual** or an individual who has been **deceased for less than 30 years** who can be identified:

(a) From that information, or

(b) From other information which is in the possession of, or likely to come into the possession of the data controller.

Note

Any expression of opinion about an individual and any intentions for them is also their personal data.

"Sensitive personal data" means personal data consisting of the following:

a) genetic data or biometric data;

b) filiation, or racial or ethnic origin;

c) political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature;

d) membership in any trade union;

e) physical or mental health or condition;

f) sex life;

g) the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject;

Note

Sensitive personal data needs to be treated with a higher degree of care due to the significant effects it can have on individuals if this type of data is misused or mishandled.

"Data Controller" means a person or public authority who alone, or jointly with others determine the purpose(s) and manner in which personal data should be processed.

Example
A bank collects personal data from its customers to provide banking services such as opening a bank account. The bank is classified as a Data Controller because they determine **why** the personal data will be collected and **how** it will be used.

"Data Processor" means any person, other than an employee of the Data Controller who processes personal data on behalf of the Data Controller.

Example
The bank in the previous example might obtain a call centre's services to manage incoming customer calls. The call centre in this scenario is the Data Processor, as they will be processing personal data on behalf of the bank to provide a supporting service.

Note
If a Data Processor processes personal data outside of the instructions of a Data Controller, they will become a Data Controller for the purpose of the Data Protection Act 2020 and all Data Controller obligations will apply to them.

"Data subject" means a named or identifiable individual who the personal data relates to.

Example
Continuing with the bank scenario, an individual who provides their personal data to the bank to open a bank account will be known as a data subject.

"Process or processing" means any operation(s) carried out on personal data, which includes the following:

a) Obtaining, recording or holding information or data
b) Organising, adaption or alteration of the information or data;
c) Retrieval, consultation or use of the information or data
d) Disclosure of the information by transmission, dissemination or making it available
e) Alignment, combination, blocking, erasure or destruction.

Note
Processing has an expansive definition and essentially means anything an organisation might do with personal data.

"Information Commissioner" means an office, which shall be a body corporate entrusted to oversee compliance with the Data Protection Act 2020.

3. Application of the Act

Entities established in Jamaica

The Act applies to Data Controllers established in Jamaica or any place where Jamaican law applies under international public law, and personal data are processed in the context of that establishment.

Each of the categories below should be treated as 'established in Jamaica:'

- An individual ordinarily resident in Jamaica.
- A body incorporated under the laws of Jamaica.
- A partnership or other unincorporated association formed under the laws of Jamaica.
- Any person who does not fall within the first three listed above but who maintains in Jamaica:
    a) an office, branch or agency through which the person carries on any activity; or
    b) a regular practice.

Entities not established in Jamaica

The Act also applies to Data Controllers who are not established in Jamaica but:

- Uses equipment in Jamaica for processing the personal data otherwise than for the purpose of transit through Jamaica; or
- Process the personal data of a data subject who is in Jamaica, and the processing of the personal data relates to:

a) Offering products or services to data subjects in Jamaica regardless of if payment is required or not; or
b) Monitoring the behaviour of data subjects as far as their behaviour takes place in Jamaica.

Companies outside of Jamaica that process personal data of persons within Jamaica will be caught by the Data Protection Act's extra-territorial effect. A Data Controller not established in Jamaica will need to appoint a representative who is established in Jamaica. (also known as a Data Controller Representative).

Action tips

- Determine whether your business is established within or outside of Jamaica.
- Assess the extent of the Act's application to the business.
- If established outside of Jamaica but process personal data of individuals in Jamaica, appoint a Data Controller Representative.

Reference

Section 3 – Application of Act

4. Data Protection Standards

The Data Protection Act consists of 8 standards that underpin how personal data must be processed. Data Controllers must comply with all 8 standards of the Data Protection Act when processing personal data.

Data Controllers are required to report non-compliance with any of the data protection standards within seventy-two (72) hours after becoming aware of the incident.

Standard 1 – Fair and lawful processing

Personal data must be processed in a fair, lawful, and transparent manner. It must not be processed unless one (1) of the lawful conditions (bases) under section 23 is met. In the case of sensitive personal data, at least one (1) of the lawful conditions (bases) under section 24 is also met.

To simplify, to process personal data lawfully, the following need to be achieved:

a) Processing personal data – Apply one of the conditions found in section 23.
b) Processing sensitive personal data – Apply one of the conditions found in section 23 and a condition found in section 24.

Fair processing of personal data

The way personal data was obtained is important to assess whether personal data are processed fairly. For example, was the person misled or deceived about the purpose(s) for processing their personal data.

For data to be considered as obtained fairly, it must be obtained:

- From a person who is authorised by or under an enactment to supply it; or
- From a person who is required to supply it under an enactment or through an instrument imposing an international obligation on Jamaica; or
- To determine a person's suitability for an honour, scholarship, prize, bursary or other award.

Additionally, personal data are not to be treated as processed fairly unless the personal data is obtained directly from the data subject, or a person authorised in writing to provide the personal data as instructed by the data subject or the Information Commissioner.

Fair processing information requirements

When personal data are obtained from the data subject or a person authorised to provide the personal data, the Data Controller must, as far as practicable and within a relevant time, provide them with the following information:

1. The identity of the Data Controller.
2. If required, the identity of its Data Protection Officer.
3. If required, the identity of the appointed Data Controller representative.
4. The purpose(s) for processing personal data.
5. The identity of the recipients of the personal data.
6. Whether providing the data is mandatory under law and the consequences of not providing the personal data.
7. The legal authority for seeking the personal data, where applicable.
8. The expected retention period of the personal data.
9. Any further information as seen fit to enable fair processing of personal data.

Action tips

- Develop new privacy notices (policies) or update existing ones to ensure all the required information about processing activities is included.
- Ensure information is clear, transparent, and easy for the layperson to understand.
- Ensure privacy notices (policies) are actively communicated to individuals.

Standard 2 – Purpose limitation

Personal data must only be obtained for one or more specified lawful purpose(s). The data should not be further processed in a manner that is incompatible with the initial purpose(s).

The purpose(s) for processing personal data can be specified in the fair processing information notice (privacy notice) under section 22(6) or provided as a notification particular to the Information Commissioner under section 16.

To determine whether any disclosure of personal data is compatible with the purpose it was obtained for, focus must be given to the purpose for which personal data are intended to be processed by any person the information is disclosed to.

Standard 3 – Data Minimisation

Personal data collected must be adequate, relevant, and limited to what is necessary for the purpose for processing.

Data Controllers should identify the minimum amount of personal data that is needed for the purpose for processing. Personal data must only be obtained for its necessary purpose and not because it might be useful in the future.

Example

A business uses the same application form to recruit factory workers and admin staff. The application form requests health background information necessary for health and safety protection for the factory workers. However, it would be excessive if the same amount of data were collected for admin staff who are not working in the same environment as the factory workers.

Standard 4 – Data Accuracy

Personal data processed must be accurate and kept up to date where necessary.

This standard is not violated if:

- The Data Controller took reasonable steps to ensure the accuracy of the personal data.
- The data subject informs the Data Controller that the personal data are inaccurate and are proven to be.

Standard 5 – Data Retention

Personal data collected must not be kept for longer than necessary for the specific purpose(s). Disposing personal data must be in accordance with the regulations under section 74(3)(g) of the Act.

Standard 6 – Consideration of data subjects' rights

Personal data must be processed in line with the rights afforded to data subjects under the Data Protection Act.

A Data Controller violates this standard if they:

- Fail to provide information under section 6 (right of access to personal data).
- Process personal data for the purposes of direct marketing without the required consent under section 10.
- Fail to comply with a justified notice under section 11 (right to prevent processing) or by failing to give a written statement under that section.
- Fail to comply with a notice under section 12 (automated decision making) or fail to give information or a written statement as required under that section.

Standard 7 – Data Security

Data Controllers must implement appropriate technical and organisational measures to prevent:

- Unauthorised or unlawful processing of personal data.
- Accidental loss, destruction, and damage of personal data.

Examples of technical and organisational measures are:

- Pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability of, and access to, personal data promptly in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure secure processing.
- Measures to ensure adherence to the technical and organisational requirements specified in the other provisions of the Act.

Taking into consideration the **development** of technology and the **cost** of implementing technical and organisational measures, these measures should ensure a level of security that matches:

- The harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, or damage; and
- The nature of the data to be protected.

The Data Controller is responsible for taking reasonable steps to ensure that agents and employees who have access to personal data are aware of and comply with relevant security measures.

Security breaches that affect or can affect personal data must be reported by Data Controllers to the Information Commissioner.

Data Processors

When processing of personal data is carried out on behalf of the Data Controller by Data Processors, the Data Controller must comply with the following:

- Select a Data Processor that provides sufficient guarantees relating to technical and organisational security measures surrounding processing activities and reports security breaches to the Data Controller; and
- Take reasonable steps to ensure compliance with these measures.

Data Processing Contract

The Data Processor's processing of personal data is only compliant with the seventh (7th) standard when there is a contract between the Data Controller and Data Processor. The contract must be in written form and state that the Data Processor should only act under the Data Controller's instructions.

The contract must impose equivalent technical and organisational security obligations on Data Processors as imposed on Data Controllers.

Breaches and offences

A person commits and offence if they wilfully and without lawful authority, use any means to breach any pseudonymisation or encryption applied to any personal data. They shall be liable upon conviction in a Parish Court to a fine not exceeding 2 million Jamaican dollars (J$2,000,000) or conviction in a Circuit Court to a fine.

A person does not commit an offence if the breach is:
- Necessary for the prevention, detection, or investigation of crime.
- Required or authorised by a court or under any law.
- Justifiable in the public interest.
- Justifiable for the purposes of journalism, literature, or art; or
- Justifiable in the public interest to test the effectiveness of the technical and organisational measures implemented by an organisation and the person:
    a) Acted without intending to cause, or threaten to cause, damage or distress to a person; and

b) Without undue delay and, where feasible, within seventy-two hours after the breach, notified the Commissioner, or a Data Controller concerned, of the breach.

A person does not commit an offence if the person acted in the reasonable belief that:

- The person is a data subject relating to the personal data concerned; or
- The person is the Data Controller regarding the personal data or acted with that Data Controller's consent.

Data Breaches

A Data Controller must report to the Information Commissioner any security breach which affects or may affect personal data within 72 hours after becoming aware of the breach.

The report should include the following:

- The facts surrounding the security breach.
- A description of the nature of the security breach, including the categories, the number of individuals affected, and the type and volume of personal data affected.
- The measures taken or proposed to be taken to mitigate or address the negative impact of the breach.
- The consequences of the breach.
- The name, address, and other contact information of the Data Protection Officer.

A Data Controller must also notify individuals whose personal data are affected by a security breach after becoming aware of it.

The information to be provided to individuals include the following:

- The nature of the security breach.
- The measures taken or proposed to be taken to mitigate or address the negative impact of the breach.
- The name, address, and other contact information of the Data Protection Officer.

Action tips

- Assess the security posture of the organisation to identify areas of concerns and ways to remediate them.
- Provide security training to staff so they understand their responsibilities.
- Develop necessary policies around data security and data breach reporting.
- Develop a robust data breach reporting process.
- Implement and test an incident response plan.

Reference

- Section 21 – Duty of Data Controller to comply with standards.
- Section 30 – Standard 7

Standard 8 – International transfers

Personal data must not be transferred to a territory outside of Jamaica unless that territory provides an adequate level of protection for data subjects' rights and freedoms concerning the processing of their personal data.

An adequate level of protection must consider the following:

- The nature of the personal data.
- The State or territory from which the personal data originates.
- The State or territory in which the personal data is transferred.
- The purposes for processing the personal data and the duration of processing.
- The laws in place in the state or territory the personal data will be transferred to.
- The international obligations of that State or territory.
- Relevant codes of conduct or other rules enforceable in that state or territory.
- Any security measures taken in respect of the personal data in the state or territory.

The transfer standard does not apply to transfers falling under the following cases except in cases prescribed by the Minister after consulting with the Information Commissioner:

- The data subject provides consent for the transfer to happen.
- The transfer is necessary for the performance of a contract between the data subject and the Data Controller or to take steps at the data subject's request with a view of the data subject entering into a contract with the Data Controller.
- The transfer is necessary for the conclusion or performance of a contract between the Data Controller and someone who is not the data subject but entered into at the data subject's request or is in the data subject's interest.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary for obtaining legal advice or establishing, exercising, or defending legal rights.
- The transfer is necessary to protect the vital interest of the data subject.

- The transfer is part of the personal data on a public register, and any conditions subject to which the register is open to inspection are complied with by any person to whom the personal data are or may be disclosed after the transfer.
- The transfer is made on terms that the Information Commissioner approves as ensuring adequate safeguards for data subjects' rights and freedoms.
- The Information Commissioner has authorised the transfer as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.
- The transfer is necessary for national security or to prevent, detect or investigate a crime.

The Minister can, by order, prescribe the following:

- Circumstances where a transfer is to be taken for the purposes of substantial public interest.
- Circumstances in which a transfer that is not required by or under an enactment is not to be taken for substantial public interest purposes.
- The States and territories which shall be deemed to have an adequate level of protection.

Any State or territory having an adequate level of protection as described above shall be included in the order only if the inclusion is necessary to fulfil Jamaica's international obligations, and the order may provide for such restrictions and conditions applicable under the international obligation.

Where there are questions as to whether a transfer should be made to a State or territory not included in an order made by the Minister, the matter shall be determined by the Information Commissioner, who will issue a notice covering the following:

- The relevant public authority responsible for protecting personal data in the State or territory concerned.
- The adequacy of the level of protection (listed above) in the State or territory concerned and
- If the Information Commissioner determines that the level of protection is not adequate, then the extent of that will be outlined.

5. Individuals' Rights

The Data Protection Act gives persons numerous rights, which can be found in Part 2 of the Act. Some of these rights are:

- Right of access to personal data.
- Right to prevent processing.
- Rights in relation to automated decision making.
- Consent required for direct marketing.
- Rectification of inaccuracies, etc.

Right of access to personal data

A data subject is entitled to be informed, free of charge, if a Data Controller or anyone on behalf of the Data Controller is processing personal data about them. If personal data are being processed, the data subject is entitled to a description of the following:

- The personal data being processed.
- The purposes for which the data are being processed or to be processed.
- The recipients or classes of recipients the personal data has been or may be disclosed to.

A data subject can also receive a copy of their personal data being processed by the Data Controller as well as the source of this data, but this will attract a fee. The Data Controller has 30 days to provide the data subject with this information. However, the time frame can be extended in special circumstances.

If a Data Controller fails to comply with a request for access to personal data, the data subject has the right to complain to the Information Commissioner. If the Information Commissioner believes the complaint is valid, they can order the Data Controller to comply with the request.

Transfer of personal data to other Data Controllers

An individual can request that the personal data they provided to the Data Controller be transferred to another Data Controller after paying a fee. This transfer must be done in a structured, commonly used, and machine-readable format.

Action tips

- Assess how a steady flow of access requests would impact the business's resources and affect current processes.
- Develop and implement a process to deal with these requests timely and efficiently.
- Train staff to quickly identify and deal with these requests.

Right to prevent processing

A data subject can write to a Data Controller asking them not to start or to stop processing personal data about them.

An individual can request to prevent processing based on the following:

- Processing their personal data is causing or likely to cause substantial damage or distress to them or another person, and such damage or distress is unwarranted.
- The personal data are incomplete or irrelevant in relation to the purpose for processing.
- The processing of the personal data or the processing of the personal data for that purpose or in that manner is not allowed under any law.
- The personal data has been retained for longer than what is required under any law.

A Data Controller has 21 days to respond to a request to prevent processing in writing and provide a statement to include the following:

- The Data Controller has complied with the request or intends to comply.
- An explanation as to why the request is unjustified and to what extent (if any) they will comply with the request.

Rights in relation to automated decision making

This right relates to a decision that has been taken using personal data processed solely by automated means. At any time in writing, a data subject can require a Data Controller not to make automated decisions using their personal data to evaluate matters relating to them (for example, the individual's performance at work, creditworthiness, reliability, or conduct).

If the Data Controller does not receive a request from someone under this right, they should, as reasonably as possible, inform the individual that a decision will be taken through solely automated means.

The individual has 30 days after receiving the information from the Data Controller to write and ask the Data Controller to reconsider the decision or take a new decision not based solely on automated means. A Data Controller who receives this request must respond to the individual within 30 days specifying the next steps to take to comply with the request.

Consent required for direct marketing

A Data Controller must not process personal data for the purpose of direct marketing unless:

- The data subject has consented to the processing for that purpose; or
- The data subject is a customer, and the requirements under 10(4) are met.

Those requirements are:

- The Data Controller has obtained the contact details of the data subject in the context of the sale of goods and services.
- The Data Controller markets its own similar goods are services.
- The data subject has been given reasonable opportunity to object, free of charge, free of unnecessary formality to the use of their personal data for direct marketing:
    a) At the time the personal data was collected; and
    b) At each communication point where direct marketing is sent to the data subject

A Data Controller should not approach a data subject whose consent is required more than once to request that consent.

Action tips

- Marketing departments and agencies should review their marketing lists to determine which lists comply with either of the two conditions outlined in this right.
- Review the current standard of consent obtained from customers to determine if it meets the standard of consent within the Act.

Rectification of inaccuracies

A data subject can write to request that a Data Controller rectifies inaccurate personal data about them that is in their possession or control.

Inaccuracy means: Error or omission.

Rectify means: Amend, block, erase, and destroy to correct the accuracy. Where a Data Controller receives a rectification request in writing, they have 30 days to determine whether a rectification is required.

If rectification is required, the Data Controller must make the rectification and inform the requester. If reasonable and practicable, the Data Controller must also notify all entities and persons the personal data was disclosed to within 12 months before the request was made. These entities and persons must make a corresponding rectification as well.

If rectification is not required, the Data Controller must inform the requester that no rectification was made.

Protect your business

Below are highlights of services we offer. Please visit our service portfolio at g5cybersecurity.com/services.

Cyber Security	Data Privacy

Security Services	Privacy Services
Vulnerability Scanning	Outsourced DPO Services
End-point Detection and Response	Privacy Compliance Assessment
Penetration Testing (Internal and External)	Data Protection Impact Assessment (DPIA)
Network Device Configuration Audits	Document Review and Drafting Services
Web Application Security Assessments	Personal Data Mapping Services

Schedule a meeting with us at g5cybersecurity.com/meeting.

6. Conditions for processing personal and sensitive personal data

There are conditions (often called lawful bases) that must be met to process personal data in compliance with the Data Protection Act.

At least one of the conditions below must be met to justify lawful processing of personal data.

Consent

The individual has provided valid consent to the standard described under the Act to process their personal data. (Informed, specific, unequivocal, and freely given).

Performance of a contract

The processing of personal data is necessary to enter into or for the performance of a contract with the data subject. This lawful basis covers any processing that allows the contract to materialise and process personal data for its duration.

Legal obligation

Processing personal data is necessary for the Data Controller to comply

Example

An organisation needs to process personal data of its employees to share employment information such as salary with the Tax Administration of Jamaica (TAJ) to pay taxes to the Government.

Vital interests

Processing personal data is necessary to protect the vital interests of the data subject. A definition of vital interest has not been provided in the Act, but in other data protection law, the condition is used in dire circumstances where it is a matter of life or death. This condition will most likely be used in the health industry where a patient is unconscious; therefore, consent cannot be obtained, but sensitive personal data (medical history) needs to be used to provide lifesaving care.

Public interest/task

Processing personal data is necessary for administering justice or for exercising statutory, governmental, or other public functions that are in the public interest. (official functions).

Legitimate interest

Processing personal data is necessary for legitimate interests pursued by the Data Controller or by any other third party the personal data is disclosed to. This condition can be subjective and can be seen to be in favour of the Data Controller, so certain requirements must be met.

E.g.
A case-by-case assessment must be taken to ensure the processing of personal data is not unwarranted and does not prejudice individuals' rights and freedoms.

The regulations made under the Data Protection Act will provide further requirements for processing personal data under the legitimate interest condition.

Personal data made public

Processing personal data can take place because the data subject has publicly published the personal data.

Note

While personal data has been made public by the data subject, certain elements must be considered before using the personal data, such as:

- The nature of the personal data (level of sensitivity)
- The reasonable expectations of the data subject that their personal data would be further processed.
- How different the purpose for processing is from the initial purpose/reason the personal data was made public.

Conditions for processing sensitive personal data

When processing sensitive personal data, at least one of the conditions for processing personal data must be met. Additionally, at least one of the conditions below must also be met.

- The data subject provides written consent for their sensitive personal data to be processed.
- Processing sensitive personal data is necessary for the Data Controller to comply with legal obligations relating to employment or social security benefits.
- Processing sensitive personal data is necessary to protect the vital interest of the data subject or another person in cases where consent cannot be obtained, or the Data Controller cannot be reasonably expected to obtain consent.
- Processing of sensitive personal data is carried out during legitimate actions by anybody or association which is non-profit or exists for political, philosophical, religious or trade union purposes.
- The person has deliberately made the sensitive personal data public.
- Processing sensitive personal data is necessary in relation to legal proceedings, for obtaining legal advice, or otherwise for establishing, exercising, or defending legal rights.
- Processing sensitive personal data is necessary for administering justice or for exercising statutory or governmental functions.
- The processing includes the disclosure of sensitive personal data by a member of an anti-fraud organisation or any other processing necessary to prevent fraud.
- Processing sensitive personal data is necessary for medical purposes and is undertaken by a health professional or by someone subject to an equivalent duty of confidentiality.
- Processing sensitive personal data is necessary for monitoring equality of opportunity or treatment between individuals of different racial or ethnic origins and is carried out with appropriate safeguards for individuals' rights.
- Sensitive personal data are processed in circumstances outlined in an order by the Minister in accordance with section 74(3)(e).

7. Registration

A Data Controller who wants to process personal data must provide certain registration details to the Information Commissioner who will maintain them on a **register.** Data Controllers must keep the Information Commissioner informed if there are any changes to their registration details. The Information Commissioner must maintain the register and make it available to the public.

Data Controllers must provide the following registration details:

- The Data Controller's name, address, and other relevant contact information.
- If required, the name, address and other relevant contact information of the representative appointed by the data controller.
- If required, the name, address, and other relevant contact information of the appointed Data Protection Officer.
- A description of the personal data to be or is being processed by or on behalf of the Data Controller and the categories of data subjects.
- A description of the purpose(s) for which personal data is being processed or to be processed.
- A description of any recipients that the Data Controller discloses data or intends to disclose data.
- The names of territories outside of Jamaica that the Data Controller directly or indirectly transfers or intends to transfer data directly or indirectly.
- The fact that the Data Controller is a public authority.
- Any other information as prescribed under the regulations.

Data Controllers will be required to pay a prescribed annual fee under regulations made by the Information Commissioner and approved by the Minister for the maintenance of the registered details. No entry shall remain in the register beyond 12 months unless payment is made.

A Data Controller, who processes personal data without registering under section 16, commits an offence and is liable upon summary conviction before a Parish Court to imprisonment not exceeding 6 months and a fine not exceeding 2 million dollars (J$2,000,000).

Note

The purpose of registration details is to promote transparency and openness regarding how Data Controllers process people's personal data within Jamaica. This approach is essential since the Act is new, and the principles of transparency and openness will need to be developed.

Action Tip

Conduct an organisation-wide audit of the data currently being processed by the different departments within the organisation to better understand what registration details to submit to the Information Commissioner.

Reference

Sections 15 – 18

8. Information Commissioner's powers and duties

The powers and duties of the Information Commissioner are dotted across the Data Protection Act, but some of the main powers and duties are:

- Monitor and enforce compliance with the Data Protection Act.
- Maintain the public register of processing details.
- Handle complaints from data subjects about the processing of their personal data.
- Submit an annual report to the House of Parliament detailing the functions of the Information Commissioner.
- Assess and provide advice on data protection impact assessments submitted by Data Controllers on an annual basis.
- Conduct investigations into the practice of Data Controllers and issue assessment, information, or enforcement notices.
- Serve Data Controllers with a fixed penalty notice if they have committed an offence under the Data Protection Act.
- Prepare and submit to the Minister a code of practice referred to as a 'data sharing code'.

9. Enforcement

Enforcement notices

In cases where the Information Commissioner is satisfied that a Data Controller has violated, or is violating any of the data protection standards, the Information Commissioner may serve the Data Controller with an enforcement notice requiring the Data Controller to do one of the following to become compliant:

- Take steps within a specific time, or refrain from taking specified steps after a specified time.
- Refrain from processing any personal data or personal data with a specific description.
- Refrain from processing personal data for a specified purpose or in a specified manner after a specified time.

Specified means, as specified within the enforcement notice.

In deciding whether to serve a notice, the Information Commissioner will consider whether the violation has caused or likely to cause damage or distress to individuals.

An enforcement notice will contain the following:

- A statement of the data protection standard or standards which the Information Commissioner is satisfied are being violated, and the Information Commissioner's reasons for reaching that conclusion.
- Information on the right to appeal under section 53 of the Act.

A Data Controller does not have to comply with any of the provisions within an enforcement notice before the end of the period in which an appeal can be brought against the notice. If such an appeal is made, the requirements do not have to be complied with until there is a determination, or the appeal has been withdrawn.

The Information Commissioner may cancel or change the enforcement notice if they believe that all or any of the notice does not have to be complied with to ensure compliance with the data protection standards.

Request for assessment

A request for assessment may be made to the Information Commissioner by someone or on behalf of someone who believes to be directly affected by any processing of personal data. The assessment is to determine whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of the Data Protection Act.

Where the Information Commissioner has received a request for assessment, it must inform the individual whether an assessment has been conducted and the conclusions formed, or actions taken as a result of the request.

Assessment notices

The Information Commissioner may serve a Data Controller with an assessment notice to determine if the Data Controller has complied with or is complying with the data protection standards.

An assessment notice requires the Data Controller to do all or any of the following:

- Allow the Information Commissioner entry to specified premises to determine compliance with the data protection standards.
- Direct the Information Commissioner to any documents of a specified description on the premises.
- Assist the Information Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises.
- Comply with any request from the Information Commissioner for copies of any documents the Information Commissioner was directed to and copies of any information the Information Commissioner viewed.
- Direct the Information Commissioner to any equipment or other material on the premises which are of a specified description.

- Allow the Information Commissioner to inspect or examine any of the documents, information, equipment, or material to which the Information Commissioner is directed or which the Information Commissioner is assisted to view.
- Allow the Information Commissioner to observe the processing of any personal data that takes place on the premises.
- Make available such specified persons or the persons of a specified description who process personal data on behalf of the Data Controller to the Information Commissioner for interviews.

An assessment notice will include the following:

- In relation to any requirements imposed on the Data Controller, the notice should specify the time or period in which the requirement should be complied with.
- Information on the right to appeal under section 53.
- The Information Commissioner may cancel an assessment notice in writing and must issue a code of practice around how it will carry out its function relating to an assessment notice.

Information notices

The Information Commissioner may serve the Data Controller with an information notice, requiring the Data Controller to provide specific information relating to compliance with the Data Protection Act.

The cases in which an information notice may be served are:

- When the Information Commissioner has received a request under section 46 (request for assessment).
- When information is reasonably required to determine whether a Data Controller has complied or is complying with the Data Protection Act.
- When there are reasonable grounds for suspecting, that in cases where proceedings have been stopped under section 36(4), the personal data are not being processed only for special purposes and are not being processed with a view to being published by any person of any journalistic, literary or artistic material which the data controller has not previously published.

10. Data Protection Officer

Data Controllers who meet the requirements must appoint an appropriately qualified Data Protection Officer to independently monitor the Data Controller's compliance with the Act. A person should not be selected if it is likely to cause a conflict of interest in the Data Protection Officer's role and any other role carried out by that person.

Requirements to appoint a Data Protection Officer

- The organisation is a public authority.
- Processes or intends to process sensitive personal data or data relating to criminal convictions.
- Processes personal data on a large scale; or
- Falls within a class prescribed by the Information Commissioner by notice published in the Gazette as being a class of Data Controllers to whom Data Protection Officer appointment applies.

The functions of the Data Protection Officer are:

- To ensure that the Data Controller processes personal data in compliance with the data protection standards and in compliance with the Act and good practice.
- To consult with the Information Commissioner to resolve any doubt about how the provisions of the Act and any regulations made under the Act are to be applied.
- To ensure that any violation of the data protection standards or any provisions of the Act by the Data Controller is dealt with in accordance with subsection (5); and
- To assist data subjects in exercising their rights under the Act in relation to the Data Controller concerned.

A Data Controller must notify the Information Commissioner of the name, address and any other relevant contact details of the Data Protection Officer and any changes.

Where the Data Protection Officer believes the Data Controller has violated a data protection standard or any other aspect of the Act, the DPO must:

- Notify the Data Controller in writing of the non-compliance.
- If the Data Controller has not satisfactorily rectified the non-compliance within a reasonable time, then report it to the Information Commissioner.

Action Tips

- Assess whether it is required for your organisation to appoint a Data Protection Officer based on the criteria.
- Assess if there are appropriately qualified individuals within the organisation who would fit the Data Protection Officer role or whether you will need to recruit outside of the organisation.
- Ensure the appointment of the Data Protection Officer does not create a perceived conflict of interest.

Reference

Section 20 – Appointment of Data Protection Officers

11. Data Protection Impact Assessment

Each calendar year, within ninety (90) days after the end of the relevant calendar year and in a form prescribed by the Information Commissioner, Data Controllers are required to submit a data protection impact assessment to the Information Commissioner regarding all personal data in the custody or control of the Data Controller.

The Information Commissioner shall evaluate each data protection impact assessment received and issue directions to the Data Controller to comply with the data protection act. Directions such as:

- For the Data Controller to make amendments to their systems of operation or other activities; or
- To implement other recommendations.

The data protection impact assessment shall include at least the following:

- 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.
- An assessment of the risks to the rights and freedoms of data subjects referred to in subsection (5) and
- 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 this Act, considering the rights and legitimate interests of data subjects and other persons concerned.

The Information Commissioner may publish a notice in the Gazette, or in other ways to bring the notice to the attention of Data Controllers, specifying the classes or kinds of personal data, or Data Controllers, to which a data protection impact assessment shall or shall not apply.

In determining any class or kind, the Information Commissioner shall consider the likely level of risk to the rights and freedoms of data subjects involved in processing the data concerned, considering the nature, scope, context, and purposes of the processing.

12. Exemptions under the DPA

The Data Protection Act requires Data Controllers to comply with all the data protection standards as well as disclose relevant information (disclosure obligations) to individuals about their personal data. However, under Part 5 of the Act, nine (9) exemptions are found in sections 32 to 43, which exempts Data Controllers from some of the mentioned obligations.

Applying these exemptions will depend on the reasons for processing the personal data and the type of entity or person processing the personal data. An overview of the exemptions is listed below.

National Security

The Minister for National Security may issue a certificate for the purpose of protecting national security to exempt the following provisions when processing personal data:

- The data protection standards
- Rights of data subjects and others (Part 2)
- Requirements of Data Controllers (Part 3)
- Enforcement (Part 6)
- Unlawfully obtaining personal data, etc. (Section 61)

This certificate must:
- Be signed by the Minister responsible for national security.
- Identify the personal data to which it applies, and
- Specify which provisions, mentioned above, the processing of the personal data is exempt from.

Any person directly affected by a certificate that was issued can appeal to the Court against that issued certificate. On an application for judicial review, the Court may allow an appeal and quash the certificate if they find the Minister did not have reasonable grounds for issuing the certificate.

Law enforcement, taxation, statutory functions, etc

Personal data processed for the following purposes below are exempt from the first data protection standard (fair and lawful processing), except to the extent that the standard requires a lawful basis under sections 23(1) and 24(1) of the Act and are exempt from the rights of access to personal data under section 6.

- The prevention, detection, or investigation of crime.
- The apprehension or prosecution of offenders; or Law enforcement, taxation, statutory functions.
- The assessment or collection of any tax or duty or of any imposition of a similar nature.

Personal data obtained from a person who had the information for any of the purposes mentioned above and the data is processed for the purpose of discharging statutory functions are exempt from section 6 (right of access to personal data) and section 22 (4) and 22 (6) information to be provided to individuals.

These exemptions apply if complying with the provisions outlined above would likely affect the purposes mentioned above.

A Data Controller, who is a public authority, processing data to carry out a risk assessment for the following purposes below is exempt from section 6 (right of access to personal data) to the extent the exemption is required in the interest of carrying out the operations of that risk assessment system.

- The assessment or collection of any tax or duty or any imposition of similar nature; or
- The prevention, detection or investigation of crime, or apprehension or prosecution of offenders, where the offence concerns an unlawful claim for payment or unlawful application of public money.

The definition of 'public money' in the Act uses the meaning assigned to it in section 2 of the Financial Administration and Audit Act.

Regulatory Activity

Personal data processed for discharging any function relating to regulatory activity are exempt from section 6 (right of access to personal data), and section 22 (4) and 22 (6) information to be provided to individuals to the extent the application of those requirements will likely prejudice (affect) the regulatory activity.

Regulatory activity applies to:

- A person given public responsibilities that is exercised in the public interest and is connected to either;
    - Public safety
    - Breaches of ethics for regulated professionals; and
    - Important national economic or financial interest such as monetary or budgetary or taxation matters.

- A function designed to protect members of the public against;
    - Mal-administration by public authorities
    - The failure of a public authority to provide service; or
    - Conduct of any trade or business, which may adversely affect the public interest.

- Where there is a design for regulating agreements or conduct that aims to prevent, restrict, or distort competition of any commercial activity; or conduct undertaking which amounts to abusing a dominant market position.

- Situations relating to the consideration of any complaint referred to in the Child Care and Protection Act by the Children's Advocate or a relevant authority as defined by that Act.

Journalism, Literature and Art

Personal data processed only for the special purposes such as Journalism, Literature and Art are exempt from the following provisions in the Act:

- The data protection standards, other than the seventh standard (data security).
- Section 6 (right to access of personal data).
- Section 11 (right to prevent processing).
- Section 12 (rights in relation to automated decision making).
- Section 13(3) and (4) (rectification of inaccuracies).

The above applies if:

a) Processing is undertaken for the publication by any person of any journalistic, literary, or artistic material.
b) The Data Controller reasonably believes there is special importance of the public interest in the freedom of expression or the right to seek, receive, distribute, or disseminate information, opinions, and ideas through any media publication and that it would be in the public interest.
c) The Data Controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

Considering whether the belief in (b) above is reasonable, focus must be given to the Data Controller's compliance with any code of practice relevant to the publication in question and is designated by the Information Commissioner.

"Publish" in relation to journalistic, literary, or artistic material means to make available to the public or any section of the public.

Research, History and Statistics

Taking into consideration the second standard (purpose limitation), the further processing of personal data only for research purposes and in compliance with the relevant conditions will not be seen as incompatible with the purposes for which the personal data were initially obtained.

The relevant conditions are:

- Personal data are not processed to support measures or decisions relating to particular individuals; and
- Personal data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Personal data processed only for research purposes may be kept indefinitely if the relevant conditions above are met.

Personal data processed only for research purposes are exempt from section 6 (right to access of personal data) if the following are met:

- The relevant conditions above.
- The results of the research or any resulting statistics are not made available in an identifiable form.

Personal data must not be treated as processed otherwise than for research purposes merely because the personal data are disclosed:

- To any person, for research purposes only.
- To the data subject or to a person acting on his behalf.
- At the request, or with the consent, of the data subject or a person acting on his behalf, or
- In circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within the first three listed.

A Data Controller must not be considered as breaching the data protection standards if personal data is disclosed by that Data Controller for research purposes if:

- The research purposes cannot reasonably be accomplished unless the personal data are provided in a form which identifies the individuals.
- The personal data are disclosed under the conditions that:
    a) It is not used to contact a person to participate in research, and
    b) The party to whom it is disclosed complies with the data protection standards.
- The relevant conditions are met.

A Data Controller may disclose personal data for archival or historical purposes if the relevant conditions are met and:

- The personal data relate to an individual who has been deceased for thirty (30) years or several years as may be prescribed for this exemption.
- The personal data are in a record which has been in existence for thirty years or such number of years as may be prescribed for this exemption.

For this exemption, 'research purposes' includes statistical or historical purposes.

Information available to the public by or under any enactment

Personal data that the Data Controller is obliged by or under any law (other than the Access to Information Act) to make available to the public are exempt from:

a) The requirement for Data Controllers to provide individuals with certain information about their personal data under section 22(4) and 22(6) and (right of access to personal data) under section 6 of the Act.
b) The fourth data protection standard (data accuracy)
c) Sections 13(3) and (4) of the Act (rectification of inaccuracies)

d) The non-disclosure provisions which are the following:
   - The first data protection standard (Fair and lawful processing), except to the extent to which disclosure is required for compliance with lawful bases in sections 23 and 24.
   - The second (purpose limitation), third (data minimisation), fourth (data accuracy) and fifth (data retention) data protection standards.
   - Section 11 (right to prevent processing) and section 13(3) and (4) (rectification of inaccuracies).

This exemption applies whether by publishing the information, making it available for inspection, or otherwise. Also, whether voluntary or on paying a fee.

Disclosures required by law or made in connection with legal proceedings, etc.

Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by order of a court.

Personal data are exempt from the non-disclosure provisions where the disclosure is necessary:

- For, or in connection with, any legal proceedings (including prospective legal proceedings); or
- For obtaining legal advice, or is otherwise necessary for establishing, exercising or defending legal rights.

Parliamentary privilege

Personal data are exempt from the following if the exemption is required to avoid infringing on the privileges of either House of Parliament:

- The first data protection standard (fair and lawful processing) except to the extent the standard requires compliance with the lawful bases in sections 23(1) and 24(1).
- The second (purpose limitation), third (data minimisation), fourth (data accuracy) and fifth (data retention) data protection standards.
- Section 6 (right to access of personal data), sections 11 (right to prevent access) and 13(3) and (4) (rectification of inaccuracies).

Parliamentary privilege refers to rights and immunities that are deemed necessary for Parliament to fulfill its functions. Members of Parliament are granted protection from civil or criminal liability for statements made or actions done in the course of their legislative duties.

Domestic purposes

Personal data processed by an individual only for that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection standards and Part 2 (rights of data subjects) and 3 (requirements for data controllers) of the Act.

13. Offences under the Act

There are various offences under the Data Protection Act. A few are listed below.

Failure to comply with data protection standards

Data Controllers who are non-compliant with any of the data protection standards commits an offence under section 21(2) and shall be liable to:

- Summary conviction in a Parish Court to a fine not exceeding two million dollars (J$2,000,000) or to imprisonment for a term not exceeding two (2) years; or
- Conviction on indictment in a Circuit Court to a fine or imprisonment for a term not exceeding seven (7) years.

Processing without registration

A Data Controller who processes personal data without providing the required registration details to the Information Commissioner under section 16 commits an offence under section 18. They shall be liable upon summary conviction before a Parish Court to a fine not exceeding two million dollars (J$2,000,000) or imprisonment for a term not exceeding six (6) months.

Unlawfully obtaining, disclosing, etc. personal data

A person commits an offence under section 61 if they intentionally and recklessly obtain or disclose personal data without the Data Controller's consent. A person who commits this offence is liable to:

- Summary conviction before a Parish Court to a fine not exceeding five million dollars or to imprisonment for a term not exceeding five (5) years; or
- Conviction on indictment in a Circuit Court to a fine or imprisonment for a term not exceeding ten (10) years.

Failure to comply with notice
A person who fails to comply with an enforcement notice, an assessment notice or an information notice commits an offence under section 52(1).

When complying with an information notice or an assessment notice, a person who knowingly makes a false statement or recklessly makes a false statement in a material respect commits an offence under section 52 (2). They shall be liable upon conviction in a Parish Court to a fine not exceeding one million dollars (J$1,000,000).

14. Penalties and Liabilities

Company Penalty

Under section 68, where a company commits an offence under the Act, they will be liable to a fine not exceeding four percent (4%) of their annual gross worldwide income for the previous year of assessment in accordance with the Income Tax Act.

Individual liability

Where an offence under section 68(3) of the Act has been committed by a company and is proved to have been committed with the consent, involvement of, or linked to any neglect on the part of, any director, manager, secretary, a similar officer of the company or any person who claimed to act in any such capacity, they shall be liable along with the company and punished accordingly.

Penalty notice

Under section 62, the Information Commissioner may issue a fixed penalty to a Data Controller if it believes that a Data Controller has committed an offence that was:

- Likely to cause substantial damage or distress.
- Deliberate or, the Data Controller knew or should have known that there was a risk the offence would occur and that such offence would be likely to cause substantial damage or distress but failed to take reasonable steps to prevent the offence.

Liability for damage

Under section 69, an individual who suffers damage or distress because of non-compliance with the Act by the Data Controller is entitled to compensation from the Data Controller for that damage or distress.

Prosecutions and penalties

The Director of Public Prosecution (DPP) or the Information Commissioner (with consent from the DPP) shall begin proceedings against companies and individuals for offences.

Protect your business

Below are highlights of services we offer. Please visit our service portfolio at g5cybersecurity.com/services.

Cyber Security	Data Privacy

Security Services	Privacy Services
Vulnerability Scanning	Outsourced DPO Services
End-point Detection and Response	Privacy Compliance Assessment
Penetration Testing (Internal and External)	Data Protection Impact Assessment (DPIA)
Network Device Configuration Audits	Document Review and Drafting Services
Web Application Security Assessments	Personal Data Mapping Services

Schedule a meeting with us at g5cybersecurity.com/meeting.

Thank you for reading our guide. We hope you've found it useful.

Please visit our website to learn more.

Web: g5cybersecurity.com

Email: support@g5cybersecurity.com

G5 Cyber Security, is incorporated in the USA and Belize.