

# DATA PROTECTION BILL, 2023

## EXPLANATORY NOTES

The Data Protection Bill, 2023 seeks to establish a new framework for managing the processing of personal data in Grenada. This Bill contains 8 parts and seeks to promote the protection of personal data processed by public and private bodies, to provide for the functions of the Information Commission and for related matters.

**PART I** of this Bill, *Clauses 1 – 6* deals with matters of a preliminary nature. *Clause 1* is the standard citation and commencement provision.

*Clause 2* sets out the interpretation of terms used in this Bill like “data”, “alternative format”, “document”, “processing” and “rectify” which have been carefully defined in order to ensure that the intended purpose of the legislation is achieved.

*Clause 3* set out the objects of this Bill *and clauses 4 and 5* set application of this Bill and the specific application to Parliament. *Clause 6* provides for the saving of certain laws.

**PART II** of this Bill, *Clauses 7 – 14* contain seven privacy and data protection principles: the general principle, the notice and choice principle, the disclosure principle, the security principle, the retention principle, the data integrity principle and the access principle.

**PART III** of this Bill, *Clauses 15 – 21* provide for the rights of data subjects. These rights include access to personal data and rectification of personal data.

**PART IV** of this Bill, *Clauses 22 – 23* deal with exemptions for personal data processed by a person only for the purpose of that individual’s personal, family or household affairs and further this Bill gives the Minister the power to make further exemptions by order published in the *Gazette*.

**PART V** of this Bill, *Clauses 24 – 28*, provide for the powers and functions of the Information Commission.

**PART VI** of this Bill, *Clauses 29 – 38*, specify the enforcement powers of the Information Commission. These powers include the investigation of complaints and the issuance of notices. Persons who suffer damage caused by the unlawful processing of data can apply to the Court for remedies.

*Clause 38* grants protection for persons who divulge information about breaches of the Act for which is this the Bill in their organisation. An employer would

therefore be prohibited from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee or denying the employee of any benefit.

**Part VII** of this Bill *Clauses 39-42* set out the offences under the Act for which this is the Bill.

*Clause 39* of this Bill makes it an offence for a person to willfully disclose information or maintain a personal information bank in contravention of the Act for which this is the Bill.

*Clause 40* of this Bill makes it an offence for a person to breach the confidentiality obligations under clause 38.

*Clause 41* of this Bill provides that where a corporation commits an offence, its officers, directors or agents who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to and commit an offence and would be liable to the punishment provided for the offence whether or not the corporation has been prosecuted or convicted.

*Clause 42* of this Bill sets out the penalties for offences under the Act for which this is the Bill.

**PART VIII** of this Bill, *Clauses 43-49*, deals with miscellaneous matters such as appeals to Court, protection from civil or criminal proceedings for actions done in good faith under the legislation, and regulation-making powers.

.....  
**Sen. the Hon. Claudette Joseph**  
**ATTORNEY-GENERAL**

# **DATA PROTECTION BILL, 2023**

## **ARRANGEMENT OF CLAUSES**

### **PART I PRELIMINARY**

1. Short title and commencement
2. Interpretation
3. Objects of Act
4. Application of Act
5. Application of Act to Parliament
6. Saving of certain laws

### **PART II PRIVACY AND DATA PROTECTION PRINCIPLES**

7. General Principle
8. Notice and Choice Principle
9. Disclosure Principle
10. Security Principle
11. Retention Principle
12. Data Integrity Principle
13. Access Principle
14. Data users to establish procedures for compliance

### **PART III RIGHTS OF DATA SUBJECTS**

15. Right of access to personal data
16. Notice and time where access is requested
17. Denial of access to personal data
18. Form of access
19. Right to rectification of personal data
20. Extent of disclosure of personal data
21. Processing of sensitive personal data

### **PART IV EXEMPTION**

22. Exemption
23. Power to make further exemptions

**PART V  
INFORMATION COMMISSION**

- 24. Establishment of the Information Commission
- 25. Functions and powers of the Commission
- 26. Appointment of staff of the Commission
- 27. Remuneration of members and staff of the Commission
- 28. Funds of the Commission

**PART VI  
ENFORCEMENT**

- 29. Receipt and investigation of complaints
- 30. Form of complaint
- 31. Notice of investigation
- 32. Information notice
- 33. Warrant to enter and search
- 34. Enforcement notice
- 35. Assessment of processing
- 36. Civil remedies
- 37. Obstruction
- 38. Whistleblower's protection

**PART VII  
OFFENCES**

- 39. Intentional disclosure of information
- 40. Breach of whistleblower's protection
- 41. Corporations that commit an offence
- 42. Penalties for offences

**PART VIII  
MISCELLANEOUS**

- 43. Appeals to High Court
- 44. Delegations
- 45. Protection from criminal or civil proceedings
- 46. Confidentiality
- 47. Report to Parliament
- 48. Amendment of schedules
- 49. Regulations

<b>SCHEDULE I</b>	<b>-</b>	<b>CONSTITUTION OF THE INFORMATION COMMISSION</b>
<b>SCHEDULE II</b>	<b>-</b>	<b>FORM OF OATH (AFFIRMATION) OF OFFICERS</b>

# DATA PROTECTION BILL, 2023

## GRENADA

### ACT NO. OF 2023

**AN ACT** to promote the protection of personal data processed by public and private bodies, to provide for the establishment of the Information Commission and for related matters.

**BE IT ENACTED** by the King's Most Excellent Majesty by and with the advice and consent of the Senate and the House of Representatives and by the authority of the same as follows—

## PART I PRELIMINARY

### Short title and commencement

1. (1) This Act may be cited as the

### DATA PROTECTION ACT, 2023.

- (2) This Act shall come into operation on a day to be appointed by the Minister by Order in the *Gazette*, and the Minister may appoint different dates for different provisions of this Act.

### Interpretation

2. In this Act—

“**alternative format**” means, with respect to personal data, a format that allows a person with a sensory disability to read or listen to the personal data;

“**authorised officer**” means an officer under section 44 who has been authorised in writing for the purposes of Part VI;

“**Chief Executive Officer**” means the officer for the time being exercising the highest level of administrative functions within a public body or private body;

“**commercial transactions**” means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance;

**“Commission”** or **“Information Commission”** means the Information Commission established under section 24;

**“data”** means any record, document, correspondence, memorandum, book, plan, map, drawing, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of those things;

**“data subject”** means a natural or legal person who is the subject of personal data;

**“data processor”**, in relation to personal data, means any person other than an employee of the data user, who processes the data on behalf of the data user;

**“data user”** means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor;

**“document”** means any medium in which data is recorded, whether printed or on tape or film or by electronic means or otherwise and also means any map, diagram, photograph, film, microfilm, videotape, sound recording, or machine-readable record or any record which is capable of being produced from a machine-readable record by means of equipment or a programme, or a combination of both, which is used for that purpose by the public body or private body which holds the record;

**“intelligible form”** means a manner that can be reasonably understood by the person for which the data or information is intended and includes a written form and an audio format, as the case may be;

**“Minister”** means the Minister with responsibility for National Security;

**“personal data”** means, in respect of commercial transactions, any data that—

- (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should wholly or partly be processed by means of equipment under paragraph (a); or

- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

and relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject;

**“private body”** means a body, excluding a public body, that—

- (a) carries on any trade, business or profession, but only in that capacity; or
- (b) has legal personality;

**“processing”**, in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including—

- (a) collection, recording, organisation, structuring or storage;
- (b) adaptation or alteration;
- (c) retrieval, consultation or use;
- (d) disclosure by transmission, dissemination or otherwise making available;
- (e) alignment or combination; or
- (f) restriction, erasure or destruction;

**“public body”** means—

- (a) a ministry, a department or a division of the ministry or a constituency office of a member of Parliament, wherever located;
- (b) a statutory body for the purposes of the Public Finance Management Act, 2015;
- (c) a State-Owned Enterprise for the purposes of the Public Finance Management Act, 2015;
- (d) an embassy, consulate or mission of Grenada or an office of Grenada situate outside Grenada whose functions include the

provision of diplomatic or consular services for or on behalf of Grenada;

- (e) any other body designated by the Minister by Regulations made under this Act, to be a public body for the purposes of this Act;

**“rectify”** means, in relation to personal data, to alter the data by way of amendment, deletion, or addition;

**“sensitive personal data”** means any personal data of a data subject consisting of information as to—

- (a) an individual’s physical or mental health or condition;
- (b) an individual’s racial or ethnic origin, genetic data, biometric data that uniquely identifies an individual;
- (c) an individual’s sex life;
- (d) an individual’s political opinions;
- (e) an individual’s religious or philosophical beliefs or other beliefs of a similar nature;
- (f) the commission or alleged commission by an individual of any offence; or
- (g) any other personal data as the Minister may determine by Order published in the *Gazette*.

### **Objects of Act**

3. The objects of this Act are to safeguard personal data processed by public bodies and private bodies in an era in which technology increasingly facilitates the processing of personal data by balancing the necessity of—

- (a) processing personal data by public bodies and private bodies; and
- (b) safeguarding personal data from unlawful processing by public bodies and private bodies,

to promote transparency and accountability in the processing of personal data.



### **Application of Act**

4. (1) This Act applies to a person who processes or who has control over or authorises the processing of any personal data in respect of commercial transactions in Grenada.

(2) Subject to subsection (1), this Act applies to a person in respect of personal data if—

- (a) the person is established in Grenada and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or
- (b) the person is not established in Grenada, but uses equipment or network services in Grenada for processing the personal data otherwise than for the purposes of transit through Grenada.

(3) A person falling within subsection (2) (b) shall nominate for the purposes of this Act a representative established in Grenada.

(4) For the purposes of subsections (2) and (3), a person is to be treated as established in Grenada as follows—

- (a) an individual who is physically present in Grenada for not less than one hundred and eighty days in one calendar year;
- (b) a body incorporated under the Companies Act, Chapter 58A;
- (c) a partnership or other unincorporated association formed under any written laws in Grenada; and
- (d) a person who does not fall within paragraph (a), (b) or (c) but maintains in Grenada—
  - (i) an office, branch or agency through which a person carries on any activity; or
  - (ii) a regular professional practice.

### **Application of Act to Parliament**

5. (1) Subject to this section, this Act applies to the processing of personal data by or on behalf of either House of Parliament as it applies to the processing of personal data by other persons.

(2) Where the purposes for which and the manner in which any personal data are, or are to be, processed are determined by or on behalf of either House of Parliament, the data user in respect of those personal data for the purposes of this Act shall be the Clerk to the Houses.

(3) Personal data are exempt from—

- (a) section 15; and
- (b) section 19 (1) and (4),

if the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

### **Saving of certain laws**

6. This Act shall not affect the operation of an enactment that makes provision with respect to the processing of personal data and does not conflict with this Act.

## **PART II PRIVACY AND DATA PROTECTION PRINCIPLES**

### **General Principle**

7. (1) A data user shall not—

- (a) process personal data about a data subject unless the data subject has given his or her consent to the processing of the personal data; or
- (b) process sensitive personal data about a data subject except in accordance with section 21.

(2) Notwithstanding subsection (1) (a) and subject to subsection (3), a data user may process personal data about a data subject if the processing is necessary—

- (a) to perform a contract to which the data subject is a party;
- (b) to take steps at the request of the data subject with a view to entering into a contract;
- (c) to comply with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- (d) to protect the interests of the data subject;

- (e) for the administration of justice;
  - (f) to exercise any functions conferred on a person by an enactment or rule of law; or
  - (g) for the exercise of a function of the State, a Minister of Government or a government department.
- (3) Personal data shall not be processed unless—
- (a) the personal data is processed for a lawful purpose directly related to an activity of the data user;
  - (b) the processing of the personal data is necessary for or directly related to that purpose; and
  - (c) the personal data is adequate but not excessive in relation to that purpose.

**Notice and Choice Principle**

8. Upon a request by a data subject, a data user shall inform the data subject—

- (a) of the purposes for which the personal data is being or is to be collected and further processed;
- (b) of any information available to the data user as to the source of that personal data;
- (c) of the data subject's right to request access to and to request rectification of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
- (d) of the class of third parties to whom the data user discloses or may disclose the personal data;
- (e) whether it is obligatory or voluntary for the data subject to supply the personal data; and
- (f) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he or she fails to supply the personal data.

**Disclosure Principle**

9. Subject to section 20, no personal data shall, without the consent of the data subject, be disclosed—

- (a) for any purpose other than—
  - (i) the purpose for which the personal data was disclosed at the time of collection of the personal data; or
  - (ii) a purpose directly related to the purpose referred to in subparagraph (i);
- (b) to any party other than a third party of the class of third parties as specified in section 8 (d).

**Security Principle**

10. (1) A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard—

- (a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;
- (b) to the place or location where the personal data is stored;
- (c) to any security measures incorporated into any equipment in which the personal data is stored;
- (d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- (e) to the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, ensure that the data processor—

- (a) provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) takes reasonable steps to ensure compliance with those measures.

**Retention Principle**

11. (1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(2) A data user shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

**Data Integrity Principle**

12. A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

**Access Principle**

13. A data subject shall be given access to his or her personal data held by a data user and be able to rectify that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or rectification is refused under this Act.

**Data users to establish procedures for compliance**

14. (1) Every data user shall establish formal procedures and implement compliance with the principles of this Part.

(2) In establishing procedures under subsection (1), a data user may consult the Commission for recommendations on the best practice and appropriate code of conduct for the data user in consideration of the size and structure of the data user, the nature of the activities of the data user and any other relevant feature of the data user.

(3) At least once in every five years, the data user shall review the procedures and conduct a self-assessment to determine—

- (a) the effectiveness of the procedures;
- (b) the level of compliance of the data user with the procedures; and
- (c) whether more efficient procedures may be adopted,

particularly in relation to the processing of personal data.

(4) For the purposes of section 25, the Commission may request, from a data user, particulars as to the procedures implemented by the data user to comply with the principles of this Part.

**PART III**

## **RIGHTS OF DATA SUBJECTS**

### **Right of access to personal data**

15. (1) Subject to the provisions of this Act, a public body or a private body shall, on the written request of and the payment of a processing fee by a person for access to personal data of which the person is the data subject—

- (a) inform the person whether personal data of which that person is the data subject is being processed by or on behalf of that body;
- (b) if personal data is being processed by or on behalf of that body, communicate to the person in an intelligible form a description of—
  - (i) the personal data of which that person is the data subject;
  - (ii) the purposes for which the personal data is being or will be processed;
  - (iii) the recipients or classes of recipients to whom personal data is or may be disclosed; and
  - (iv) any information available to the body as to the source of the data.

(2) The Minister may prescribe the maximum processing fee for the purposes of subsection (1).

### **Notice and time where access is requested**

16. (1) Subject to section 17, where access to personal data is requested under section 15, the public body or private body to which the request is made shall, subject to subsection (2)—

- (a) within thirty calendar days after the request is received, give written notice to the person who made the request as to whether or not access to the personal data or a part thereof will be given; and
- (b) if access is to be given, within sixty calendar days after the request is received, give to the person who made the request access to the personal data or a part thereof.

(2) The Chief Executive Officer of a public body or private body may extend the time limit for compliance with a request for access to personal data—

- (a) by a maximum of thirty days if—
  - (i) meeting the original time limit would unreasonably interfere with the operations of the public body or private body; or
  - (ii) consultations are necessary to comply with the request that cannot be reasonably completed within the original time limit; or
- (b) by such period of time as is reasonable, if the additional time is necessary for converting the personal data into an alternative format,

by giving, in the prescribed form, notice of the extension and the length of the extension to the person who made the request, within thirty days after the request is received, and a statement that the person has a right to make a complaint to the Commission about the extension.

**Denial of access to personal data**

17. (1) A data user is not obliged to comply with a request for access to personal data—

- (a) unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the personal data which that person seeks;
- (b) if compliance with the request will be in contravention of the exemptions contained in Part IV or of any duty of confidentiality recognised by law;
- (c) where another person who can be identified from the personal data does not consent to the disclosure of his or her personal data to the person making the request; or
- (d) if the body obtains the written approval of the Commission to deny access to the personal data.

(2) Where a public body or a private body refuses to give access to personal data, its Chief Executive Officer shall state in the notice given pursuant to section 16 (2) (a)—

- (a) where applicable, that the personal data does not exist; or
  - (b) the specific provision of this Act on which refusal was based or the provision on which a refusal could reasonably be expected to be based if the personal data existed, and that the person who made the request has the right to make a complaint to the Commission about the refusal.
- (3) Where a Chief Executive Officer fails to give access to personal data requested under section 15 within the time limits set out in this Act, he or she shall, for the purposes of this Act, be deemed to have refused to give access.

### **Form of access**

18. (1) Where a data subject is to be given access to personal data requested pursuant to section 15, the public body or private body shall—

- (a) permit the data subject to examine the personal data; or
  - (b) provide the data subject with a copy of the personal data.
- (2) Where access to personal data is given under this Act and the data subject to whom access is to be given has a sensory disability and requests that access be given in an alternative format, access shall be given in an alternative format if—
- (a) the personal data already exists under the control of a public body or a private body in an alternative format that is appropriate for the person in the light of his or her sensory disability; or
  - (b) the Chief Executive Officer considers it to be reasonable to cause the personal data to be converted to an alternative format.

### **Right to rectification of personal data**

19. (1) Where personal data that is processed by a public body or a private body to which access has been given, contains personal data which the data subject claims—

- (a) is incomplete, incorrect, misleading, or excessive; or
  - (b) is not relevant to the purpose for which the document is held,
- the body shall, upon an application by the data subject, cause the data to be amended if the body is satisfied of the claim.

(2) An application under subsection (1) shall—



- (a) be in writing in the prescribed form; and
  - (b) as far as practicable, specify—
    - (i) the document containing the record of personal data that is claimed to require the amendment;
    - (ii) the personal data that is claimed to be incomplete, incorrect, misleading or irrelevant;
    - (iii) the reasons for the claim; and
    - (iv) the amendment requested by the data subject.
- (3) To the extent that it is practicable to do so, the public body or private body shall, when making an amendment to personal data in a document pursuant to this section, ensure that it does not destroy, conceal or redact the text of the document as it existed prior to the amendment.
- (4) Where a public body or a private body is not satisfied with the reasons for an application pursuant to subsection (1), it may—
- (a) refuse to amend the personal data;
  - (b) inform the data subject of its refusal and the reasons for the refusal; and
  - (c) inform the data subject that a complaint may be lodged in writing to the Commission.
- (5) A data subject who is aggrieved by a decision of a public body or a private body pursuant to subsection (4) may lodge a complaint in writing to the Commission within fifteen calendar days of the date of the receipt of the communication of refusal.
- (6) For the avoidance of doubt, this section does not apply to records prepared and maintained in accordance with—
- (a) the Registration of Births and Deaths Act, Chapter 280;
  - (b) the Passports Act, Chapter 226;
  - (c) the Citizenship Act, Chapter 54;
  - (d) the Marriage Act, Chapter 184;
  - (e) the Grenada Citizenship by Investment Act, 2013; and

- (f) any other enactment as prescribed by Regulations.

**Extent of disclosure of personal data**

20. Notwithstanding section 9, personal data may be disclosed by a data user to a third party for any purpose other than the purpose for which the personal data was disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances—

- (a) the data subject consented to the disclosure;
- (b) the disclosure—
  - (i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or
  - (ii) was required or authorised by or under any enactment or by an order of a court; or
- (c) the disclosure is deemed by the Minister to be justified as being in the public interest in the circumstances.

**Processing of sensitive personal data**

21. (1) Subject to subsection (2) and Part II, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions—

- (a) the data subject has given his or her written consent to the processing of the sensitive personal data;
- (b) the processing is necessary—
  - (i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;
  - (ii) to protect the interests of the data subject or another person, in a case where—
    - (A) consent cannot be given by or on behalf of the data subject; or

- (B) the data user cannot reasonably be expected to obtain the consent of the data subject;
    - (iii) to protect the interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
    - (iv) for medical purposes and is undertaken by—
      - (A) a healthcare professional; or
      - (B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
    - (v) for the purpose of, or in connection with, any legal proceedings or pursuant to an order of the Court;
    - (vi) to obtain legal advice;
    - (vii) to establish, exercise or defend legal rights;
    - (viii) for the administration of justice;
    - (ix) to exercise any functions conferred on any person by or under any enactment or rule of law;
    - (x) to exercise a function of the State, a Minister of Government or a government department; or
    - (xi) for any other purposes as the Minister thinks fit; or
  - (c) the information contained in the personal data has been made public as a result of steps taken by the data subject.
- (2) The Minister may by Order published in the *Gazette*—
- (a) exclude the application of sub-paragraph (i), (viii) or (ix) of subsection (1) (b) in such cases as may be specified in the Order; or
  - (b) provide that, in such cases as may be specified in the Order, the condition in sub-paragraph (i), (viii) or (ix) of subsection (1) (b) is not to be regarded as satisfied unless such further conditions as may be specified in the Order are also satisfied.

(3) A person who contravenes subsection (1) commits an offence and shall, on conviction on indictment, be liable to a fine of two hundred thousand dollars or to imprisonment for a term not exceeding two years or to both.

(4) For the purposes of this section—

“medical purposes” includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation, the provision of care and treatment and the management of healthcare services;

“healthcare services” means services provided by healthcare professionals;

“healthcare professional” includes a medical practitioner, dental practitioner, pharmacist, psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist and other allied health practitioner and any other person involved in the giving of medical, health, dental, pharmaceutical and any other similar services.

## **PART IV EXEMPTION**

### **Exemption**

22. (1) There shall be exempted from the provisions of this Act personal data processed by an individual only for the purposes of that individual’s personal, family or household affairs, including recreational purposes.

(2) Subject to section 23—

(a) personal data processed for—

- (i) the prevention or detection of crime or for the purpose of investigations;
- (ii) the apprehension or prosecution of offenders;
- (iii) the assessment or collection of any tax or duty or any other imposition of a similar nature; or
- (iv) for the purpose of the Proceeds of Crime Act, and other legislation enacted for the purposes of anti-money-laundering and combating terrorist-financing,

shall be exempted from the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Access Principle and other related provisions of this Act;

- (b) personal data processed in relation to information on the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;
- (c) personal data processed for preparing statistics or carrying out research shall be exempted from the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Access Principle and other related provisions of this Act, unless—
  - (i) the personal data is processed for any other purpose; and
  - (ii) the resulting statistics or the results of the research are not made available in a form that identifies the data subject;
- (d) personal data that is necessary for the purpose of or in connection with any order or judgment of a court shall be exempted from the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Access Principle and other related provisions of this Act;
- (e) personal data processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Access Principle and other related provisions of this Act, if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or
- (f) personal data processed only for journalistic, literary or artistic purposes shall be exempted from the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Retention Principle, the Data Integrity Principle, the Access Principle and other related provisions of this Act, provided that—
  - (i) the processing is undertaken with a view to the publication by a person of the journalistic, literary or artistic material;
  - (ii) the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and

- (iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

**Power to make further exemptions**

23. The Minister upon the recommendation of the Commission may, by Order published in the *Gazette* exempt—

- (a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or
- (b) any data user or class of data users from all or any of the provisions of this Act.

**PART V**  
**INFORMATION COMMISSION**

**Establishment of Information Commission**

24. (1) There is hereby established a body corporate to be known as the Information Commission, to which section 49 of the Interpretation and General Provisions Act, Chapter 153 applies.

(2) The Information Commission shall consist of three members appointed by the Governor-General on the recommendation of the Prime Minister in consultation with the Leader of the Opposition, having expertise in one or more of the following—

- (a) information communication technology or other like skills;
- (b) data protection, privacy rights or other like skills; and
- (c) law.

(3) The Governor-General shall appoint from the membership under subsection (2), the Chairperson and the Deputy Chairperson of the Commission.

(4) The members of the Commission shall be subject to Schedule I and shall before assuming his or her functions, make and subscribe to the oath in the form set out as Schedule II.

(5) The provisions of Part XII of the Public Finance Management Act, 2015 shall apply in respect of the Information Commission.

### **Functions and powers of the Commission**

25. (1) The functions of the Commission include—

- (a) monitoring compliance by public bodies and private bodies with the provisions of this Act, including issuing notices;
- (b) advising public bodies and private bodies of their obligations under this Act;
- (c) receiving and investigating complaints about alleged violations of the data protection principles of data subjects, and in respect thereof make reports to complainants;
- (d) undertaking educational programmes to promote understanding of this Act;
- (e) undertaking research into and monitoring developments in data processing and information technology to ensure the continued protection of personal data through administrative, legislative or other methods, and to report to the Minister the results of such research and monitoring; and
- (f) exercising and performing such other functions as are conferred or imposed on the Commission by or under this Act or any other enactment.

(2) The Commission shall have powers, for the purpose of carrying out the functions of the Commission, to do all such acts as are necessary for or in connection with the carrying out of these functions.

### **Appointment of staff of the Commission**

26. (1) The Commission shall appoint staff of the Commission, comprising—

- (a) Information Officers;
- (b) Information Technology Technicians;
- (c) the Secretary to the Commission;
- (d) administrative officers; and

(e) such other staff as may be necessary to give effect to this Act.

(2) A person appointed under this section or authorised to perform any functions pursuant to the provisions of this Act, shall before assuming his or her functions, make and subscribe to the oath in the form set out as Schedule II.

### **Remuneration of members and staff of the Commission**

27. The salaries and allowances of the members and staff of the Commission shall be determined by a resolution of the House of Representatives.

### **Funds of the Commission**

28. The funds of the Commission shall consist of—

- (a) fees and other sums received by the Commission in exercise of its functions;
- (b) such sums as may be allocated by Parliament from time to time;
- (c) such other sums as may lawfully be paid to the Commission.

## **PART VI ENFORCEMENT**

### **Receipt and investigation of complaints**

29. (1) The Commission may, on a complaint made by a data subject or at the instance of the Commission, investigate or cause to be investigated whether any provisions of this Act or the Regulations have been, are being or are likely to be contravened by a public body or a private body in relation to the data subject.

(2) Where a complaint is made to the Commission under subsection (1), the Commission shall—

- (a) within a prescribed time, investigate or cause the complaint to be investigated by an authorised officer, unless the Commission determines that it is frivolous or vexatious; and
- (b) within a prescribed time, notify the data subject in writing of the decision of the Commission in relation to the complaint and that the data subject may, if aggrieved by the Commission's decision, appeal to the High Court against the decision.

(3) Nothing in this Act precludes the Commission from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorised by the data subject to act on behalf of the data



subject, and a reference to a complainant in any other section includes a reference to a person so authorised.

### **Form of complaint**

30. (1) A complaint pursuant to this Act shall be made to the Commission in the prescribed form, unless the Commission authorises otherwise.

(2) The Commission shall give such reasonable assistance as is necessary in the circumstances to enable a data subject who wishes to make a complaint to the Commission, to put the complaint in writing.

### **Notice of investigation**

31. Before commencing an investigation of a complaint pursuant to this Act, the Commission shall serve a notice of investigation in the prescribed form, on the Chief Executive Officer which shall include the substance of the complaint.

### **Information notice**

32. The Commission may, by an information notice in the prescribed form, served on a data user, request that person to furnish in writing in the time specified therein—

- (a) access to personal data;
- (b) information about and documentation of the processing of personal data;
- (c) information related to the security of the processing of personal data; and
- (d) any other information in relation to matters specified in the notice as is necessary or expedient for the performance of functions and exercise of powers of the Commission under this Act.

### **Warrant to enter and search**

33. (1) If a Magistrate is satisfied by information on oath supplied by an authorised officer that there are reasonable grounds for suspecting that an offence under this Act has been or is being committed, and that evidence of the commission of the offence is to be found on any premises specified by the authorised officer, the Magistrate may issue a warrant authorising the authorised officer—

- (a) to enter the premises;
- (b) to search the premises;

- (c) to inspect, examine, operate and test any equipment found on the premises and which is used, or intended to be used, for the processing of personal data;
- (d) to inspect and seize any documents or other material found on the premises and which may constitute evidence of the commission of the offence;
- (e) to ask any person on the premises to provide an explanation of any document or other material found on the premises; and
- (f) to ask any person on the premises to provide other information as may reasonably be asked to determine whether the data user has committed the offence.

(2) The authorised officer, upon the authority of a warrant issued by a Magistrate and accompanied by members of the Police Force, may at any time enter any premises, for the purpose of discharging any functions or duties under this Act or Regulations.

#### **Enforcement notice**

34. (1) Where the Commission determines that a public body or a private body has committed or is committing an offence under this Act, the Commission may, subject to subsection (2) serve an enforcement notice on the public body or private body, requiring it to take such steps as are specified in the enforcement notice within such time as may be so specified to comply with the provision concerned.

(2) An enforcement notice shall be in writing in the prescribed form and shall—

- (a) specify the provision of this Act that, in the determination of the Commission, the public body or private body has contravened or is contravening and the reasons for the Commission having formed that determination; and
- (b) specify the action that the Commission requires the public body or private body to take to rectify the contravention.

(3) An enforcement notice may, without prejudice to the generality of subsection (2), require the public body or private body—

- (a) to rectify or erase personal data; or

- (b) to supplement the personal data with statements concerning the matters dealt with by the personal data as the Commission may approve.

(4) Where a public body or a private body complies with a requirement under subsection (3), it shall, as soon as practicable and in any event not later than thirty days after such compliance, notify—

- (a) the data subject concerned; and
- (b) where the Commission considers it reasonably practicable to do so, any person to whom the personal data was disclosed twelve months before the date of the service of the enforcement notice concerned and ending immediately before such compliance,

of the rectification, erasure or statements made, if the compliance materially modifies the personal data concerned.

(5) The Commission may cancel an enforcement notice and, shall in writing notify the public body or private body on whom it was served of the cancellation.

### **Assessment of processing**

35. (1) The Commission may from time to time, or upon a request made by or on behalf of a person who is, or believes himself or herself to be, directly affected by the processing of personal data by a public body or a private body, carry out an assessment of the processing of personal data to determine whether it is carried out in compliance with this Act.

(2) The Commission shall conduct an assessment in such manner as appears to be appropriate.

(3) If following an assessment under subsection (1), the Commission considers that a public body or a private body has not complied with the provisions of this Act, the Commission shall provide the Chief Executive Officer of the public body or private body with a report—

- (a) containing the findings of the assessment;
- (b) directing the body to comply with the specified provisions of this Act; and
- (c) making any recommendations that the Commission considers appropriate.

(4) A report made by the Commission under subsection (3) may be included in a report made to Parliament pursuant to this Act.

### **Civil remedies**

36. (1) A data subject who suffers damage by reason of the contravention of any of the provisions of this Act, by a public body or private body, may institute civil proceedings in the High Court.

(2) In proceedings brought against a public body or a private body by virtue of this section, it is a defence to prove that the public body or private body has taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.

### **Obstruction**

37. (1) A person shall not obstruct the Commission or any authorised officer in the conduct of their duties and functions under this Act.

(2) A person who contravenes this section commits an offence and is liable on summary conviction to a fine of five thousand dollars or to imprisonment for a term of six months.

### **Whistleblower's protection**

38. An employer, whether or not being a public body, shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee of a benefit, because—

- (a) the employee acting in good faith and on the basis of reasonable belief has—
  - (i) notified the Commission that the employer or any other person has contravened or is about to contravene this Act;
  - (ii) done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Act; or
  - (iii) refused to do or stated the intention of refusing to do anything that is in contravention of this Act; or
- (b) the employer believes that the employee will do anything described in paragraph (a).

## **PART VII OFFENCES**

### **Intentional disclosure of information**

39. (1) A person who intentionally discloses personal information in

contravention of this Act commits an offence.

(2) A person who collects, stores or disposes of personal information in a manner that contravenes this Act, commits an offence.

### **Breach of whistleblower's protection**

40. A person who contravenes section 38 commits an offence.

### **Corporations that commit an offence**

41. Where a corporation commits an offence under this Act, any officer, director or agent of the corporation who directed, authorised, assented to, or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence.

### **Penalties for offences**

42. (1) A person who commits an offence under this Act for which a penalty is not specifically provided for is liable upon—

(a) summary conviction, to a fine of fifty thousand dollars or to imprisonment for a term of three years; and

(b) conviction on indictment, to a fine of one hundred thousand dollars or to imprisonment for a term of five years or to both.

(2) Where an offence under this Act for which a penalty is not specifically provided is committed by a body corporate, the body corporate shall be liable upon—

(a) summary conviction, to a fine of two hundred and fifty thousand dollars; and

(b) conviction on indictment, to a fine of five hundred thousand dollars.

## **PART VIII MISCELLANEOUS**

### **Appeals to High Court**

43. An appeal lies to the High Court against—

(a) a requirement specified in an enforcement notice or an information notice;

(b) a decision of the Commission in relation to a complaint; or

(c) any decision of the Commission in respect of the conduct of its duties and powers under this Act.

### **Delegations**

44. The Chief Executive Officer or the Commission may delegate any power or function under this Act to an authorised officer.

### **Protection from criminal or civil proceedings**

45. (1) No criminal or civil proceedings shall lie against the Commission or against a person acting on behalf or under the direction of the Commission, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise, discharge, or performance of any power, duty or function of the Commission under this Act.

(2) For the purpose of any law relating to libel or slander—

- (a) anything said, any information supplied or any document or thing produced in good faith in the course of an investigation carried out by or on behalf of the Commission under this Act is privileged; and
- (b) any report made in good faith by the Commission under this Act is privileged.

### **Confidentiality**

46. Subject to this Act, no person who is or has been a member of the Commission, or acting on behalf or under the direction of the Commission shall disclose any information that comes to their knowledge in the conduct of their functions under this Act, except by an order of a court.

### **Report to Parliament**

47. (1) The Commission shall, within three months after the conclusion of the financial year, prepare a report on the activities of the Commission as it relates to the Act during that year and cause a copy of the report to be laid before Parliament.

(2) Notwithstanding subsection (1), the Commission may, at any time, prepare and have laid before Parliament a special report referring to and commenting on any matter within the scope of the powers and functions of the Commission where, in the opinion of the Commission, the matter is of such urgency or importance that a report thereon should not be deferred until the time provided for transmission of the next annual report of the Commission pursuant to subsection (1).

### **Amendment of schedules**

48. The Minister may, by Order, amend any schedule to this Act.

**Regulations**

49. (1) The Minister may make Regulations for giving effect to the provisions of this Act and for prescribing anything required or authorised by this Act to be prescribed.

(2) Notwithstanding the generality of subsection (1), Regulations made under this section may prescribe—

- (a) guidelines for the disposal of personal data held by a public body or a private body;
- (b) special procedures for giving a person access pursuant to section 18, to personal data; and
- (c) codes of practice.

(3) All Regulations made under this Act shall be subject to negative resolution.

**SCHEDULE I**  
**CONSTITUTION OF THE INFORMATION COMMISSION**

*(section 24 (4))*

**Disqualification from membership**

1. A person shall not become, or continue to be appointed as a member of the Commission, if the person—

- (a) is a member of Parliament;
- (b) has a financial or other interest in any enterprise or activity likely to affect the discharge of the person's functions as a member of the Commission;
- (c) is affected by bankruptcy action;
- (d) is or has been convicted of an indictable offence; or
- (e) is or has been convicted of an offence pursuant to the provisions of this Act.

**Tenure of office**

2. A member of the Commission shall hold office for a period not exceeding three years and shall be eligible for re-appointment.

**Resignation**

3. (1) A member, other than the Chairperson, may at any time resign his or her office by instrument in writing addressed to the Governor-General and transmitted through the Chairperson, and from the date specified in the instrument of resignation, that person shall cease to be a member of the Commission.

(2) The Chairperson may at any time resign his or her office by instrument in writing addressed to the Governor-General and from the date specified in the instrument of resignation, he or she shall cease to be a member of the Commission.

**Vacating office**

4. A member of the Commission is taken to have vacated his or her office if the member—

- (a) resigns his or her position on the Commission pursuant to paragraph 2;
- (b) cannot continue as a member pursuant to paragraph 1;



- (c) is absent without the permission of the Commission, from three consecutive meetings of the Commission and he or she has not given due notice;
- (d) dies;
- (e) is appointed as a public officer;
- (f) is nominated for election as a representative in the House of Representatives or in the Senate.

### **Revocation of appointment**

5. The Governor-General may revoke the appointment of a member if the Governor-General is satisfied that—

- (a) the person is unable to exercise the functions of his or her office whether arising from infirmity of mind or body or any other cause; or
- (b) the person has committed misconduct in the exercise of the functions of his or her office.

### **Vacancy in membership**

6. If a vacancy occurs in the membership of the appointed members, that vacancy shall be filled by the appointment of another person from the same category which that person was appointed in the first instance for the remainder of the current term.

### **Quorum**

7. The quorum for a meeting of the Commission shall be two.

### **Meetings of the Commission**

8. (1) The Chairperson shall preside at all meetings of the Commission at which he or she is present.

(2) If the Chairperson is absent from a meeting of the Commission, but the Deputy Chairperson is present, the Deputy Chairperson shall preside.

### **Decisions of the Commission**

9. All decisions of the Commission shall be decided by a majority of members voting and, in the event of an equality of votes, the Chairperson of the Commission shall have a casting vote.

**Seal of the Commission**

10. (1) The seal of the Commission shall be such device as the Commission shall determine and shall where the Commission so directs, be kept in the custody of the Secretary to the Commission.

(2) The affixing of the seal shall be authenticated by the signature of the Chairperson, or the Deputy Chairperson, and the Secretary or such other person authorised on his or her behalf by a resolution of the Commission.

## **SCHEDULE II**

*(sections 24 (4) and 26 (2))*

### **FORM OF OATH (AFFIRMATION) OF MEMBER/OFFICER**

I, ..... (name) having been appointed as ..... (position), do [swear/solemnly affirm] that I will faithfully bear true allegiance to Grenada and will uphold the Constitution and the law, and that I will conscientiously, impartially and to the best of my knowledge, judgement and ability discharge the functions of my office and do right to all manner of people after the laws and usages of Grenada without fear or favour, affection or ill-will.

Passed by the House of Representatives this 14<sup>th</sup> day of March, 2023.



.....  
**Clerk to the House of Representatives**

Passed by the Senate this       day of       , 2023.

.....  
**Clerk to the Senate**