Barbados – Data Protection Overview

INTRODUCTION

The Data Protection Act, 2019-29 of the Laws of Barbados ('the Act') came into effect (with the exception of certain provisions requiring registration of Data Controllers and Data Processors and the creation of official Registers of Data Controller and Data Processors, namely; sections 50, 51, 52, 55, 56 and 57 of the Act) on March 31, 2021. The Act, which is modelled on the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), became law upon proclamation by the Governor-General and publication in the Official Gazette on March 26, 2021. The sections of the Act excluded from coming into effect on March 31, 2021 are expected to take effect upon publication in the Official Gazette at a future date.

1. GOVERNING TEXTS

1.1. Key acts, regulations, directives, bills

The Act is the key piece of data protection legislation in Barbados.

1.2. Guidelines

The Act is set to establish the Data Protection Commissioner.

1.3. Case law

Not applicable.

2. SCOPE OF APPLICATION

2.1. Personal scope

The Act provides a regulatory framework for the processing of personal data. In this regard, it applies to data controllers and data processors (defined below), each of whom may be a natural person or a public or private legal entity.

2.2. Territorial scope

The Act has both territorial and extraterritorial scope. Under Section 3 of the Act, data controllers and data processors who are resident, incorporated/organised/registered, or otherwise formed in Barbados, or who maintain an office, branch, or agency in Barbados through which processing of personal data is carried out, must comply with the Act.

Further, data controllers/processors who are not resident, incorporated/organised/registered, or otherwise formed in Barbados will be subject to the Act where they process personal data of data

subjects in Barbados and such processing activities relate to the offering of goods or services to data subjects in Barbados.

2.3. Material scope

The Act applies to the processing of 'personal data' (as defined below) and includes provisions for the processing of sensitive personal data (as defined below). It also carves out rules where personal data is processed for specific purposes, using automated processing, and the rights of data subjects which are engaged in particular cases.

3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

3.1. Main regulator for data protection

The Data Protection Commissioner is responsible for the general administration of the Act and is the primary regulatory authority for data protection in Barbados.

3.2. Main powers, duties and responsibilities

Per Section 71 of the Act, the main powers, duties, and responsibilities of the Data Protection Commissioner are to:

- monitor and enforce the application of the Act;
- promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing;
- promote the awareness of data controllers and data processors of their obligations under the Act;
- organise activities addressed specifically to children to educate them about the risks, rules, safeguards, and rights in relation to processing;
- conduct audits for the purpose of ascertaining whether or not data is processed in accordance with the Act;
- upon request, provide information to any data subject concerning the exercise of their rights under the Act;
- monitor the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data, and:
    - report to the Minister on the results of that monitoring; and
    - where appropriate, make recommendations on the need for, or desirability of, taking legislative, administrative or other action to give protection or better protection, to the privacy of persons in respect of their personal data;
- examine any proposed legislation or proposed policy of the Government that:
    - the Data Protection Commissioner considers may affect the privacy of persons in respect of their personal data; or
    - provides for the collection of personal data by any public authority or the disclosure of personal data by one public authority to another public authority,
    - and report to the Minister the results of that examination;
- conduct investigations on the application of the Act, including on the basis of information received from a public authority;

- receive and invite representations from members of the public on any matter affecting the privacy of persons in respect of their personal data;
- undertake research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons in respect of their personal data is minimised, and report to the Minister the results of such research and monitoring;
- prepare appropriate codes of practice for the guidance of persons processing personal data; and
- investigate complaints from persons concerning abuses in the processing of personal data.

4. KEY DEFINITIONS

The definitions of the terms provided below are set out in Section 2 of the Act.

Data controller: Either:

- a person who alone, jointly or in common with others determines the purposes for which, and the manner in which, any personal data is or should be processed; or
- where personal data is processed only for the purpose for which the data is required by or under an enactment to be processed, the person on whom the obligation to process the data is imposed by or under an enactment.

Data processor: Any person, other than an employee of a data controller, who processes personal data on behalf of the data controller.

Personal data: Data which relates to an individual who can be identified:

- from that data; or
- from that data together with other information which is in the possession of or is likely to come into the possession of the data controller.

Sensitive data: Personal data consisting of information on a data subject's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a political body;
- membership of a trade union;
- genetic data;
- biometric data;
- sexual orientation or sexual life;
- financial record or position;
- criminal record; or
- proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings.

Health data: Any record which:

- consists of information relating to the physical or mental condition of an individual; and
- has been made by or on behalf of a health care professional in connection with the care of the individual.

Biometric data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

Data subject: An individual who is the subject of personal data.

5. LEGAL BASES

Section 6(1) of the Act sets out the bases on which personal data can be lawfully processed, as outlined below.

5.1. Consent

Data processing is considered lawful where the data subject has given consent to the processing of their personal data for one or more specific purposes (Section 6(1)(a) of the Act).

5.2. Contract with the data subject

Data processing is considered lawful where the processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract (Section 6(1)(b)(i) and (ii) of the Act).

5.3. Legal obligations

Data processing is considered lawful where the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract (Section 6(1)(b)(iii) of the Act).

5.4. Interests of the data subject

Data processing is considered lawful where the processing is necessary in order to protect the vital interests of the data subject (Section 6(1)(b)(iv) of the Act).

5.5. Public interest

Data processing is considered lawful where the processing is necessary for the exercise of any functions of a public authority (Section 6(1)(b)(vii) of the Act).

5.6. Legitimate interests of the data controller

Data processing is considered lawful where the processing is necessary for the purposes of legitimate interests pursued by (Section 6(1)(b)(ix) and (x) of the Act):

- the data controller or by the third party to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; or
- the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.7. Legal bases in other instances

In addition to the above, data processing is considered lawful (Section 6(1)(b) of the Act):

- for the administration of justice;
- for the exercise of any functions of either House of Parliament; or
- for the exercise of any functions conferred on any person by or under any enactment.

Sensitive personal data

Under Section 9 of the Act, the processing of sensitive personal data is only permitted where:

- the data subject gives consent to the processing;
- the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- the processing is necessary in order to protect the vital interests of the data subject or another person;
- the processing is carried out in the course of its legitimate activities by non-profit organisation that exists for political, philosophical, religious or trade union purposes and:
    - is carried out with appropriate safeguards for the rights and freedoms of data subjects;
    - relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
    - does not involve disclosure of the personal data to a third party without the consent of the data subject;
- the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- the processing is necessary for the purpose of, or in connection with, any legal proceedings and/or prospective legal proceedings, and/or for the purpose of

obtaining legal advice, or otherwise for the purposes of establishing, exercising or defending legal rights;
- the processing is necessary for the administration of justice;
- the processing is necessary for the exercise of any functions of either House of Parliament;
- the processing is necessary for the exercise of any functions conferred on any person by or under an enactment and/or the exercise of any functions of a public authority;
- the processing is necessary for medical purposes and is undertaken by a health care professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
- the processing is of sensitive personal data consisting of information as to racial or ethnic origin and is necessary for the purpose of identifying or keeping under review, the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained and is carried out with appropriate safeguards for the rights and freedoms of data subjects.

6. PRINCIPLES

Section 4 of the Act sets out data protection principles which data controllers must be in compliance with when processing personal data. Specifically, Section 4 of the Act provides that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data controllers are further required to take reasonable steps to ensure that employees who have access to personal data comply with the principles.

7. CONTROLLER AND PROCESSOR OBLIGATIONS

7.1. Data processing notification

Section 50 of the Act (not yet in effect) requires data controllers to be registered in the Register of Data Controllers. Further, data controllers that operate outside of Barbados are required to appoint a representative established in Barbados.

Section 55 of the Act (not yet in effect) requires data processors to be registered in the Register of Data Processors.

7.2. Data transfers

Section 22 of the Act restricts the transfer of personal data to a country or territory outside Barbados unless that country or territory provides for:

- an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and
- appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.

7.3. Data processing records

Pursuant to Section 60(1) of the Act, data controllers and, where applicable, data controllers' representatives are required to maintain a record of their processing activities which must contain all of the following:

- the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative and the data privacy officer ('DPO');
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;
- where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in Section 26 of the Act, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data; and
- where possible, a general description of the technical and organisational security measures.

Pursuant to Section 60(2) of the Act, data processors and, where applicable, data processors' representatives are required to maintain a record of their processing activities which must contain all of the following:

- the name and contact details of the data processor or data processors and of each data controller on behalf of whom the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the DPO;
- the categories of processing carried out on behalf of each data controller;

- where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in certain cases, the documentation of suitable safeguards; and
- where possible, a general description of the technical and organisational security measures.

7.4. Data protection impact assessment

Under Section 65 of the Act, data controllers must undertake a Data Protection Impact Assessment ('DPIA') on the protection of personal data where a type of processing, in particular one using new technologies, is likely to result in a high risk to the rights and freedoms of an individual. A DPIA must, in particular, be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning an individual or similarly significantly affect the individual; or
- processing on a large scale of sensitive personal data; or
- a systematic monitoring of a publicly accessible area on a large scale.

7.5. Data protection officer appointment

Section 67 of the Act provides for the appointment of a DPO. Accordingly, data controllers and data processors must designate a DPO in any case where:

- the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
- the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

7.6. Data breach notification

Section 63 of the Act requires data controllers to notify the Data Protection Commissioner of any personal data breach not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of an individual.

Where the notification to the Data Protection Commissioner is not made within 72 hours, it must be accompanied by reasons for the delay.

Data processors are required notify the appropriate data controller without undue delay after becoming aware of a personal data breach.

Further, under Section 64 of the Act, where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.

7.7. Data retention

Pursuant to Section 58(5) of the Act, the contract between a data controller and a data processor must stipulate that the data processor delete or return all personal data to the data controller after the end of the provision of services relating to processing, and delete existing copies unless storage of the personal data is required by statute.

7.8. Children's data

The Act defines 'child' as a person under the age of 18 years. Under Section 8 of the Act, the processing of a child's personal data will be lawful only where and to the extent that consent is given or authorised by the parent or guardian of the child and data controllers are required to make reasonable efforts to verify in such cases that such consent is duly given or authorised.

Further, under Section 21 of the Act, any communication required to be made by a data controller to a data subject relating to processing of the data subject's personal data, and in particular for any information addressed specifically to a child, must be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

7.9. Special categories of personal data

Under Section 31 of the Act, personal data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax, duty or other imposition of a similar nature is exempt from the requirement in Section 4(1) of the Act which provides that personal data be processed lawfully, fairly, and in a transparent manner in relation to the data subject. This exemption applies except to the extent to which it requires compliance with the conditions in Sections 6 (bases for lawful processing) and 9 (processing of sensitive personal data).

7.10. Controller and processor contracts

Under Section 58(4) of the Act, processing by a data processor must be governed by a written contract between the data processor and the data controller which sets out the following:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects;
- the obligations and rights of the data controller;
- that the data processor processes the personal data only on documented instructions from the data controller;
- that the data processor ensures that persons authorised to process the personal data have committed themselves to confidentiality;
- that the data processor, taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights under the Act;
- that the data processor assists the data controller in ensuring compliance with the relevant Sections of the Act, taking into account the nature of processing and the information available to the data processor; and
- that the data processor, on the determination of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of

services relating to processing, and deletes existing copies unless storage of the personal data is required under statute.

8. DATA SUBJECT RIGHTS

8.1. Right to be informed

Under Section 10(2) of the Act, where personal data is transferred to another country or to an international organisation the data subject will have the right to be informed of the appropriate safeguards specified in Section 24 of the Act.

In addition, per Section 19(1) of the Act, data controllers are required to provide certain information to data subjects at the time when personal data is collected, namely:

- the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- the contact details of the DPO, where applicable;
- the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- where the processing is done pursuant to Section 6(1)(b)(x) of the Act, the legitimate interests pursued by the data controller or by a third party;
- the recipients or categories of recipients of the personal data, if any; and
- where applicable, the fact that the data controller intends to transfer personal data to another country or international organisation and the existence or absence of an adequacy decision by the European Commission, or in the case of transfers to the appropriate safeguards referred to in Section 24 of the Act and the means by which to obtain a copy of them or where they have been made available.

Section 19(2) of the Act requires that additional information necessary to ensure fair and transparent processing must be provided to the data subject, namely:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is done pursuant to Section 6(1)(a) or Section 9(1)(a) of the Act, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Data Protection Commissioner;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Further, under Section 19(3) of the Act, where the data controller intends to further process the personal data for a purpose other than that for which the personal data was collected, they must provide the data subject prior to that further processing with information on that other purpose and with any relevant further information referred to in Section 19(2) of the Act (see above).

Pursuant to Section 20(1) of the Act, where personal data has not been obtained from the data subject, the data controller must provide the data subject with the information set out in Section 19(1) of the Act (see above).

In addition, pursuant to Section 20(2) of the Act, the data controller must provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- where the processing is done pursuant to Section 6(1)(b)(x) of the Act, the legitimate interests pursued by the data controller or by a third party;
- the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is done pursuant to Section 6(1)(a) or Section 9(1)(a) of the Act, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Data Protection Commissioner;
- the source from which the personal data originated, and if applicable, whether it came from publicly accessible sources; and
- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Further, according to Section 20(4) of the Act, where personal data is to be processed for a purpose other than that for which the personal data was obtained, data controllers must inform the data subject of that other purpose and any relevant further information as referred to in Section 20(2) of the Act (see above).

8.2. Right to access

Data subjects' rights of access in connection with their personal data are set out in Section 10 of the Act. Data subjects have the right to be given a copy of the personal data undergoing processing. They are also entitled:

- to be informed whether their personal data is being processed by or on behalf of the data controller;
- where personal data of the data subject is being processed by or on behalf of the data controller, to request from, and to be given by, the data controller, a description of:
    - the purposes of the processing;
    - the categories of personal data concerned;

- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the Data Protection Commissioner; any available information as to their source, where the personal data is not collected from the data subject; and
- the existence of automated decision-making, including profiling, referred to in Section 18 of the Act and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

8.3. Right to rectification

Per Section 11 of the Act, data subjects have the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning them. In addition, data subjects are entitled to have incomplete personal data completed by the data controller, including by means of providing a supplementary statement.

8.4. Right to erasure

Per Section 12 of the Act, data subjects have a right to the erasure of their personal data by a data controller without undue delay. Further, data controllers must erase personal data where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws consent where the processing is done pursuant to Section 6(1)(a) or Section 9(1)(a) of the Act, and where there is no other legal ground for the processing;
- the data subject objects to the processing on the basis that it is likely to cause damage or distress and there are no overriding legitimate grounds for the processing, or the data subject objects to processing for purposes of direct marketing;
- the personal data has been unlawfully processed; or
- the personal data has to be erased in compliance with a legal obligation in Barbados to which the data controller is subject.

Per Section 12(3) of the Act, where a data controller is obliged to erase the personal data and he has made that data public, the data controller must take reasonable steps to inform other data controllers who are processing the personal data that the data subject has requested the erasure the personal data.

8.5. Right to object/opt-out

Per Section 13 of the Act, data subjects have the right to obtain a restriction on processing of personal data from the data controller where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing pursuant to Section 16 of the Act pending the verification whether the legitimate grounds of the data controller override those of the data subject.

Where processing has been restricted pursuant to the above, the personal data can only be processed:

- with the data subject's consent;
- for the establishment, exercise or defence of legal claims;
- for the protection of the rights of another person; or
- for reasons of important public interest of Barbados.

8.6. Right to data portability

Per Section 15 of the Act, data subjects have the right to receive their personal data which they have provided to a data controller, in a structured, commonly used and machine-readable format.

Data subjects are also entitled to transmit their personal data to any another data controller without hindrance where the processing is based on consent pursuant to Section 6(1)(a) or Section 9(1)(a) or on a contract pursuant to Section 6(1)(b)(i) and the processing is carried out by automated means.

In exercising the right to data portability pursuant to the above, the data subject will have the right to have their personal data transmitted directly from one data controller to another, where technically feasible.

8.7. Right not to be subject to automated decision-making

Per Section 18 of the Act, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or similarly significantly affects him. This right does not apply where the automated processing or profiling of personal data is:

- necessary for entering into, or performance of, a contract between the data subject and a data controller;
- authorised by any enactment to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's consent.

Notwithstanding, the exemptions noted above will not apply in respect of sensitive personal data unless it is in the public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

8.8. Other rights

Right to prevent processing likely to cause damage or distress

Section 16 of the Act affords data subjects the right to require the data controller, at the end of a 21-day period, to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which they are the data subject, on the ground that:

- the processing of the data or the data controller's processing for that purpose or in that manner is causing or is likely to cause substantial damage or distress to the data subject or another; and
- the damage or distress is or would be unwarranted.

Right to compensation

Section 93 of the Act provides that an individual who suffers damage or distress due to any contravention of the Act by a data controller or data processor is entitled to compensation from that data controller/data processor for that damage.

Right to prevent processing for purposes of direct marketing

Section 17 of the Act provides that a person is entitled at any time, by a written notice to a data controller, to require the data controller, at the end of a 21 day period, to cease processing for the purposes of direct marketing, personal data in respect of which they are the data subject.

Automated individual decision-making, including profiling

Section 18 of the Act provides that a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

9. PENALTIES

The Act provides the following penalties:

- A person who operates as a data controller without being registered in the Register of Controllers is guilty of an offence and is liable on summary conviction to a fine of BBD 10,000 (approx. €4,150) or to a term of imprisonment of two months or to both (Section 50(4) of the Act).
- A data controller who is not established in Barbados and who does not nominate a representative pursuant to Section 50(3) of the Act is guilty of an offence and is liable on summary conviction to a fine of BBD 10,000 (approx. €4,150) or to a term of imprisonment of two months or to both (Section 50(5) of the Act).

- A person who operates as a data processor without being registered in the Register of Controllers is guilty of an offence and is liable on summary conviction to a fine of BBD 10,000 (approx. €4,150) or to a term of imprisonment of two months or to both (Section 55(4) of the Act).
- A data processor that is not established in Barbados and who does not nominate a representative is guilty of an offence and is liable on summary conviction to a fine of BBD 10,000 (approx. €4,150) or to a term of imprisonment of two months or to both (Section 55(5) of the Act)
- Data processors and any persons acting under the authority of a data controller/data processor, who have access to personal data, are guilty of an offence and liable on summary conviction to a fine of BBD 500,000 (approx. €207,600) or to a term of imprisonment of three years or to both if they process data without instructions from the data controller, unless required to do so by any enactment. (Section 59 of the Act).

9.1 Enforcement decisions

Not applicable.