SUPPLEMENT PART I

OFFICIAL GAZETTE
THE BAHAMAS

PUBLISHED BY AUTHORITY

NASSAU | 11th December, 2025 | No. 50

DATA PROTECTION ACT, 2025

Arrangement of Sections

Section

PART I - PRELIMINARY **5**

1. Short title and commencement....5
2. Interpretation....5
3. Application....10

PART II - DATA PROTECTION PRINCIPLES **11**

4. Duty of data controller and data processor to comply with principles....11
5. Principles in relation to the processing of personal data....11
6. Conditions for processing the personal data of a data subject....12
7. Fairness in the processing of personal data....14
8. Transparency in the processing of personal data....16
9. Data storage limitation. 17
10. Accuracy of personal data....17
11. Data security....18

PART III - OFFICE OF THE DATA PROTECTION COMMISSIONER 18

12. Establishment of the Office of the Data Protection Commissioner....18
13. Appointment of the Commissioner....18
14. Independence of the Commissioner....19
15. Functions of the Commissioner....19
16. Removal of the Commissioner....21
17. Staff of the Office of the Data Protection Commissioner....22
18. Funds....23
19. Confidential information....23
20. Indemnity....24
21. Annual report....24
22. Codes of Conduct and Practice, Guidelines and data protection certification standards....25
23. International Cooperation....26

PART IV – DATA SUBJECT **26**

RIGHTS 26

24. Right of access to personal data....26
25. Right to file complaint....29
26. Right to rectification of inaccurate personal data....30

27. Right to object to the processing of personal data....30
28. Right to erasure of personal data....30
29. Right to restrict the processing of personal data....32
30. Right to prevent data processing....32
31. Right of data subject to receive and transfer data. 33
32. Right to compensation....33
CONSENT 34
33. Conditions for consent....34
34. Special conditions for consent of a child or a vulnerable person....34
35. Conditions for processing sensitive personal data....35
36. Sensitive personal data relating to health. 38
37. Consent required for direct marketing....39

PART V – DATA CONTROLLERS AND DATA PROCESSORS 40

38. Registration of data controllers and data processors....40
39. Application for registration....41
40. Registration certificate....41
41. Renewal of registration certificate....41
42. Register of Data Controllers....42
43. Register of Data Processors....42
44. Data processing records....43
45. Auditing of data controllers and data processors....44
46. Appointment of a data protection officer....45
47. Non-disclosure of personal data....46
48. Notification of breach of personal data....47
49. Communication of breach of personal data to a data subject....48
50. Automated data processing....49
51. Data protection impact assessment....49
52. Data processing by data processors....50
53. Security of processing....51

PART VI – TRANSFER OF PERSONAL DATA OUTSIDE THE BAHAMAS 52

54. General principle for transfer outside The Bahamas. 52
55. Conditions for transfer outside of The Bahamas....53
56. Requirement of data controller to review....54

PART VII – EXEMPTIONS TO DATA PROTECTION STANDARDS OR TO DISCLOSURE OF DATA SUBJECT REQUIREMENTS 55

57. National security....55
58. Law enforcement and taxation....55
59. Regulatory activities....56
60. Processing of personal data for journalism, artistic or literary purposes....57
61. Processing of personal data for research purposes....58
62. Information available to public by law....58

63. Disclosures required by law or made for the purpose of legal proceedings.....59
64. Parliamentary privilege.....59
65. Legal professional privilege.....59
66. Personal data processed for personal, family or household affairs and recreational purposes.....59
67. Confidential references given by a data controller.....59
68. Judicial appointments and honours.....60
69. Armed forces.....60
70. Correctional services.....60
71. Appointments to the public service.....60
72. Negotiations with the data subject.....60
73. Examinations.....60

PART VIII – ENFORCEMENT 61

74. Enforcement notice.....61
75. Cancellation of enforcement notice.....62
76. Request for assessment.....62
77. Information notice.....63
78. Commissioner to determine processing for journalism, artistic or literary purposes.....65
79. Restriction on enforcement in processing for journalism, artistic or literary purposes.....65
80. Failure to comply with notice. 65
81. Issue of warrants.....66
82. Execution of warrants.....67
83. Matters exempt from inspection and seizure.....67
84. Return of warrants.....67
85. Forfeiture.....68
86. Offences.....68

PART IX – DATA PROTECTION APPEAL TRIBUNAL 68

87. Establishment of Data Protection Appeal Tribunal.....68
88. Right of appeal.....69
89. Determination of appeals.....69
90. Penalty notices.....69

PART X – DATA PROTECTION OVERSIGHT COMMITTEE 71

91. Establishment of Data Protection Oversight Committee.....71
92. Functions of the Committee. 71
93. Powers of the Committee. 71

PART XI – GENERAL 72

94. Prosecutions.....72
95. Offences by officers of a body corporate.....72
96. Unlawful access, use, or disclosure of personal data.....72

97. Regulations. 73
98. Transitional....75
99. Savings....76
100. Act binds Crown....76
101. Repeal of No. 3 of 2003....76

FIRST SCHEDULE....77

SECOND SCHEDULE....80

No. 74 of 2025

DATA PROTECTION ACT, 2025

AN ACT TO REGULATE THE COLLECTION, KEEPING, PROCESSING, USE AND DISSEMINATION OF PERSONAL DATA; TO PROTECT THE PRIVACY OF INDIVIDUALS IN RELATION TO THEIR PERSONAL DATA; TO ESTABLISH THE OFFICE OF THE DATA PROTECTION COMMISSIONER AND TO ESTABLISH THE DATA PROTECTION OVERSIGHT COMMITTEE; TO REPEAL THE DATA PROTECTION (PRIVACY OF PERSONAL INFORMATION) ACT (CHAPTER 324A) AND FOR CONNECTED PURPOSES

[Date of Assent - 9th December, 2025]

Enacted by the Parliament of The Bahamas

PART I - PRELIMINARY

1. Short title and commencement.

(1) This Act shall be cited as the Data Protection Act, 2025.

(2) This Act shall come into operation on the date as the Minister may appoint by notice published in the *Gazette*, and different dates may be appointed in respect of different provisions of this Act.

2. Interpretation.

In this Act —

"automated means" means data processing carried out without human intervention, encompassing operations, with the collection, recording, and storage of data performed by technology;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a identifiable natural person, which allow or

confirm the unique identification of the identifiable natural person such as facial images or fingerprint data;

"business" includes a trade or profession;

"child" means an identifiable natural person below the age of eighteen years;

"Commissioner" means the Data Protection Commissioner appointed under section 13;

"consent" in relation to the processing of personal data of an identifiable natural person, means a freely given, specific, informed and unambiguous indication of the identifiable natural person's wishes, by which the identifiable natural person, in a written statement or by clear affirmative action, signifies agreement to the processing of personal data relating to that identifiable natural person;

"data" means information that —

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of equipment described in paragraph (a);

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

(d) does not fall within paragraphs (a), (b) or (c), but forms part of the educational record or health record of the data subject; or

(e) does not fall within paragraphs (a), (b), (c) or (d), but is recorded information held by a public body;

"data controller" means an identifiable natural person or a person, public body, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data;

"**data processor"** means an identifiable natural person, public body, agency or other body which processes personal data on behalf of the data controller;

"data protection impact assessment" means a systematic assessment carried out by a data controller or data processor to identify, evaluate, and mitigate the potential risks to the rights, freedoms, or legitimate interests of data subjects arising from the proposed processing of personal data;

"data subject" means an identifiable natural person to whom personal data relates;

"established in The Bahamas" means —

(a) an identifiable natural person who is ordinarily resident in The Bahamas;

(b) a body incorporated under the laws of The Bahamas;

(c) a partnership or other unincorporated association formed under the laws of The Bahamas;

(d) a person who does not fall under paragraphs (a) to (c), but who maintains in The Bahamas —

(i) an office, branch or agency through which the person carries on an activity of processing personal data; or

(ii) a regular practice of processing personal data;

"filing system" means a structured set of personal data that is accessible by reference to a data subject or according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

"fundamental rights and freedoms" mean the rights and freedoms of an identifiable natural person which are guaranteed by the Constitution of The Bahamas;

"genetic data" means personal data relating to the inherited or acquired genetic characteristics of an identifiable natural person that gives unique information about the physiology or health of the identifiable natural person, and which originates from an analysis of a biological sample from the identifiable natural person;

"health care professional" means a person who is registered to practice under —

(a) the Dental Act (*Ch. 226*);

(b) the Health Professions Act (*Ch. 233*);

(c) the Medical Act (*Ch. 224*);

(d) the Nurses and Midwives Act, 2023 (*No. 9 of 2023*);

(e) the Pharmacy Act (*Ch. 227*);

"health record" means a record which —

(a) consists of information relating to the physical or mental condition of an identifiable natural person; and

(b) has been made by or on behalf of a health care professional in connection with the care of an identifiable natural person;

"identifiable natural person" means one who can be identified, directly or indirectly, in particular by reference to an identifier, namely, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the identifiable natural person;

"legitimate interest" means an interest pursued by a data controller or by a third party, which requires the processing of personal data and does not override the fundamental rights and freedoms of the data subject;

"Minister" means the Minister responsible for the Office of the Data Protection Commissioner;

"non-disclosure provisions" mean the following provisions to the extent to which they are inconsistent with the disclosure in question —

(a) section 5(1)(a), to the extent to which it requires compliance with the conditions in sections 6 and 35;

(b) section 5(1)(b), (c), (d) and (e);

(c) sections 26, 28, 29, 30, 32, 37 and 50;

"person" includes a corporation, either aggregate or sole, and a club, society, association, public body;

"personal data" means information relating to an identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or, access to, personal data transmitted, stored or otherwise processed;

"process" or **"processing"** means an operation which is performed on personal data, whether or not by automated means, namely, the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"profiling" means any form of automated processing of personal data, including processing involving the use of artificial intelligence or other algorithmic techniques, consisting of the use of personal data to evaluate certain personal aspects relating to an identifiable natural person, in particular to analyze or predict aspects concerning an identifiable natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymization" means the processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, on the condition that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identifiable natural person;

"public body" means —

(a) a Government Ministry or Department;

(b) a corporation established by an Act of Parliament for public purposes; or

(c) a board, commission, committee or other body appointed by the Governor-General or appointed by a Minister;

"public interest" means an interest or purpose recognized by law, public policy, or established practice as being concerned with the welfare and well-being of the public;

"recipient" means an identifiable natural person or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

"repealed Act" means the Data Protection (Privacy of Personal Information) Act (*Ch. 324A*);

"representative" means a natural or legal person established in The Bahamas who is designated in writing by a data controller or data processor that is not established in The Bahamas, to act on behalf of that data controller or data processor with regard to their obligations under this Act;

"sensitive personal data" means personal data consisting of information on a data subject's —

(a) racial or ethnic origin;

(b) political opinions;

(c) religious beliefs or other beliefs of a similar nature;

(d) trade union membership;

(e) genetic data;

(f) biometric data for the purpose of uniquely identifying an identifiable natural person;

(g) sex life or sexual orientation;

(h) medical data;

(i) health record;

(j) financial record or financial position;

(k) criminal record;

(l) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of the proceedings or the sentence of any court of competent jurisdiction in the proceedings;

"scientific research purposes" includes references to processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity;

"statistical purposes" includes an activity that is reasonably undertaken for the carrying out of statistical surveys or for the production of statistical results but only where —

(a) the information that results from the processing, shall be aggregated and not identify any data subject; and

(b) the data controller shall not use the results, or any information derived from the surveying or production activity, in support of measures or decisions with respect to a particular data subject, who was the subject of the statistical activity;

"subject information provisions" mean —

(a) section 5(1)(a) to the extent to which it requires compliance with section 7(2); and

(b) section 24;

"third party" means a person other than —

(a) an identifiable natural person;

(b) a data subject;

(c) a data controller;

(d) a data processor; or

(e) a person authorized to process data on behalf of a data controller or data processor;

"Tribunal" means the Data Protection Appeal Tribunal established under section 87;

"vital interest" means the protection of the life, health, or safety of an identifiable natural person.

3. Application.

(1) This Act applies to —

(a) the processing of personal data in the context of the activities of a data controller or a data processor established in The Bahamas; and

(b) the processing of personal data of data subjects in The Bahamas by a data controller or a data processor not established in The Bahamas, where —

(i) the data controller or data processor uses equipment in The Bahamas to process personal data, other than processing of personal data for the purpose of its transit through The Bahamas; or

(ii) the processing activities are related to —

(aa) the offering of goods or services to data subjects in The Bahamas;

(bb) the monitoring of the behaviour of data subjects, to the extent that the behaviour takes place within The Bahamas.

(2) This Act does not apply to the processing of personal data by an identifiable natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.

PART II - DATA PROTECTION PRINCIPLES

4. Duty of data controller and data processor to comply with principles.

(1) Subject to the exemptions provided under Part VII of this Act, a data controller and a data processor shall take appropriate measures to ensure compliance with the data protection principles set out in this Part and shall, upon the request of the Commissioner, demonstrate their compliance with the data protection principles.

(2) A data controller and data processor shall take reasonable steps to ensure that their employees who have access to personal data comply with the data protection principles set out in this Part.

(3) A data controller or data processor who processes personal data contrary to the data protection principles set out in this Part commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years, or to both.

(4) It shall be a defence for a data controller or data processor charged with an offence under this Part to prove that the data controller or data processor —

(a) acted in good faith;

(b) took all reasonable steps; and

(c) exercised all due diligence,

to prevent the contravention.

5. Principles in relation to the processing of personal data.

(1) Personal data shall be —

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) obtained for one or more specified lawful purposes, and shall not be further processed in a manner that is incompatible with the lawful purpose;

(c) adequate, relevant and not excessive in relation to the purpose for which they are collected or processed;

(d) accurate and kept up to date;

(e) 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

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using technical or organizational measures.

(2) For the purposes of paragraph (b) of subsection (1), further processing shall be treated as processing which is compatible with the original purpose, where it is done —

(a) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and shall not be considered to be incompatible with the initial purposes where it is done; or

(b) for the purposes of demonstrating that processing of the personal data is being done in compliance with the requirements of this Act.

(3) For the purposes of paragraph (b) of subsection (1), where making a determination as to whether further processing is incompatible with the original purpose a data controller shall take into account, among other things —

(a) a link between the original purpose and the new purpose;

(b) the context in which the personal data was collected, including the relationship between the data subject and the controller;

(c) the nature of the processing and the determination of whether the processing relates to the processing of sensitive personal data;

(d) the possible consequences of the intended processing for data subjects;

(e) the existence of appropriate safeguards, namely, encryption or pseudonymization.

(4) For the purposes of paragraph (d) of subsection (1), every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which the personal data is processed, is erased or rectified without delay.

6. Conditions for processing the personal data of a data subject.

(1) The personal data of a data subject is processed lawfully, if it is processed based on one of the following conditions —

(a) the data subject has given his consent to the processing of his personal data for one or more specific purposes;

(b) the processing is necessary —

(i) for the performance of a contract to which the data subject is a party or the taking of a step at the request of the data subject, for the purpose of entering into a contract;

(ii) for compliance with a legal obligation to which the data controller is subject, other than an obligation imposed by contract;

(iii) in order to protect the vital interests of the data subject;

(iv) for the exercise of a function conferred on a person by or under a written law;

(v) for the exercise of a function of the Crown or a public body;

(vi) for the exercise of another function of a public nature exercised in the public interest by a person;

(vii) for the purposes of legitimate interests pursued by a data controller or by a third party to whom the personal data is disclosed, except if the processing is unwarranted by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject;

(viii) for the protection of the fundamental rights and freedoms of the —

(a) data subject; or

(b) identifiable natural person;

(ix) for the performance of a task carried out in the public interest or in the exercise of the functions of the data controller under this Act;

(x) for the purposes of a legitimate interest pursued by the data controller or by a third party, except where the interest is overridden by the legitimate interests or fundamental rights and freedoms of the data subject that require the protection of personal data, particularly where the data subject is a child;

(xi) for the exercise of functions of either House of Parliament;

(xii) for the exercise of a function conferred on a person by or under a written law; or

(xiii) for the administration of justice.

(2) Subparagraph (xii) of paragraph (b) of subsection (1) shall not apply to processing carried out by public bodies, in the performance of their tasks.

(3) For the purposes of subparagraph (xii) of paragraph (b) of subsection (1), the Minister may, after consultation with the Commissioner, make

regulations specifying particular circumstances in which the condition specified in subsection (1), shall complied with.

(4) For the purposes of subparagraph (vii) of paragraph (b) of subsection (1), examples of types of processing that may be necessary for the purposes of a legitimate interest include —

(a) processing that is necessary for the purposes of direct marketing, except where consent is required for the processing of the personal data of a data subject for the purpose of direct marketing under section 37;

(b) intra-group transmission of personal data, whether relating to clients, employees or other persons, where the intra-group transmission of personal data is necessary for internal administrative purposes; and

(c) processing that is necessary for the purposes of ensuring the security of network and information systems.

(5) For the purposes of subsection (4) —

(a) **"intra-group transmission"** means transmission between members of a group of undertakings or between members of a group of institutions affiliated to a central body;

(b) **"security of network and information systems"** means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible by means of those network and information systems.

7. Fairness in the processing of personal data.

(1) In determining whether personal data is processed fairly, regard is to be had to the method by which it is obtained, including in particular whether a person from whom the personal data is obtained is deceived or misled as to the purpose or purposes for which the personal data is to be processed.

(2) Subject to subsection (3), personal data is to be treated as having been obtained fairly if the personal data consists of information obtained from a person who is authorized by or under a written law to supply the data or required to supply the data by a convention or other instrument imposing an international obligation on The Bahamas.

(3) Personal data is not to be treated as processed fairly unless —

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has readily available to him, the following information —

(i) the identity of the data controller;

(ii) where a data controller has nominated a representative for the purposes of this Act, the identity of that representative;

(iii) the purpose or purposes for which the data is intended to be processed;

(iv) the identity of a third party to which disclosure of the personal data is contemplated;

(v) the legal authority for seeking the personal data, where applicable;

(vi) whether the provision, by the data subject, of the personal data sought is compulsory under a written law, and the consequences of not providing the personal data;

(vii) the expected period of retention of the personal data; and

(viii) further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair; and

(b) the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject is provided with, or has readily available to him, the information specified in subparagraphs (i) to (iv) of paragraph (a).

(4) For the purposes of subsection (3)(b), **"the relevant time"** means —

(a) the time when the data controller first processes the data; or

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged —

(i) if the data is in fact disclosed to a third party within that period, the time when the data is first disclosed;

(ii) if within that period the data controller becomes, or ought to become aware that the data is unlikely to be disclosed to a third party within that period, the time when the data controller does become, or ought to become, so aware; or

(iii) at the end of that period.

(5) The Minister may, after consultation with the Commissioner, make regulations prescribing categories of data controllers that may be exempted, in whole or in part, from the requirements of subsection (3), where the exemption is necessary and proportionate to reduce administrative burdens, having regard to the scale, nature and context of the processing carried out by the data processors.

(6) Regulations made under subsection (5) shall specify —

(a) the categories of data controllers to which the exemption applies;

(b) the provisions from which they are exempted; and,

(c) conditions subject to which the exemption applies.

8. Transparency in the processing of personal data.

(1) Where personal data relating to a data subject is collected from the data subject, the data controller shall, at the time when personal data is obtained, provide the data subject with the following —

(a) the identity and contact details of the data controller and his representative;

(b) the purpose of the processing;

(c) the legal basis on which the processing is based;

(d) the legitimate interests pursued by the data controller, where the processing is based on section 6(1)(b)(v);

(e) the types or categories of personal data intended to undergo processing;

(f) the period of time for which the personal data is retained;

(g) the data subject's right to —

(i) access to personal data under section 24;

(ii) object to the processing of data personal data under section 27;

(iii) rectification and erasure of personal data under sections 26 and 28;

(h) the identity of the recipient to whom the personal data may be disclosed;

(i) where the data controller intends to transfer the data to a recipient in a third country, territory or international organization, a description of the technical and organizational measures taken by the data controller under section 53(2).

(2) The data controller shall provide the information required under this section to the data subject without charging a fee —

(a) in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(b) in writing or by electronic means or other means; and

(c) orally, upon the request of data subject on confirmation of the identity of the data subject.

(3) Subsection (1) shall not apply to the extent that —

(a) the data subject already has the information;

(b) the data controller is not able to provide the information to the data subject directly;

(c) there is an obligation of secrecy or confidentiality under a written law or an obligation of legal professional privilege that prohibits the disclosure of information; or

(d) the provision of the information proves impossible or would involve a disproportionate effort for the processing of personal data taking into account among other things —

(i) the number of data subjects involved;

(ii) the age of the personal data undergoing processing; and

(iii) the safeguards applied to the processing;

(e) the provision of the information, subject to the conditions in section 6 and the technical and organizational measures referred to in paragraph (i) of subsection (1), are likely to render impossible or seriously impair the objectives of the processing of the personal data of the data subject;

(f) where providing the information may render impossible, or seriously impair, the achievement of the objectives of the processing for which the personal data are intended to be used.

(4) Notwithstanding subsection (3), the data controller shall take appropriate measures to protect the data subject's fundamental rights and freedoms and legitimate interests, including making the information publicly available.

9. Data storage limitation.

(1) Notwithstanding section 5(1)(e), personal data may be stored for a period longer than is necessary for the purpose for which the personal data is processed where the personal data is processed solely for —

(a) archiving purposes in the public interest; or

(b) scientific research purposes or historical research purposes;

(c) statistical purposes, and

(2) Where personal data is stored under subsection (1), the data controller shall implement appropriate safeguards to protect the fundamental rights and freedoms of the data subject.

10. Accuracy of personal data.

(1) The data controller shall take all reasonable steps to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(2) Personal data shall be kept up to date —

(a) where it is necessary for the processing carried out by the data controller and to the extent that it is reasonable; and

(b) at the specific request of the data subject, under section 6(1)(b)(i).

11. Data security.

(1) Having regard to the state of technological development and the cost of implementation, the technical or organizational measures referred to in section 53(2) shall ensure a level of security appropriate to —

(a) the harm or distress that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage; and

(b) the nature of the personal data to be protected.

(2) In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, particularly from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

PART III - OFFICE OF THE DATA PROTECTION COMMISSIONER

12. Establishment of the Office of the Data Protection Commissioner.

(1) There is established the Office of the Data Protection Commissioner which shall be responsible for the regulation and enforcement of data protection and privacy.

(2) The Office of the Data Protection Commissioner shall be a body corporate with perpetual succession and common seal and shall, in its corporate name, be capable of —

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;

(c) entering into contracts; and

(d) doing other legal acts necessary for the proper performance of the functions of the Office of the Data Protection Commissioner.

13. Appointment of the Commissioner.

(1) Subject to subsection (3), the Governor-General, acting on the advice of the Prime Minister after consultation with the Leader of the Opposition, shall appoint a suitably qualified person as the Data Protection Commissioner.

(2) A person is suitably qualified for appointment as the Data Protection Commissioner if that person —

(a) holds a degree from an accredited institution in information and communications technology, law, compliance, risk management, information security, or another relevant discipline;

(b) has demonstrable expertise in data protection, privacy, information governance, or related regulatory frameworks; and

(c) has at least seven years' professional experience in legal, regulatory, compliance, risk management, or information governance matters relevant to the functions of the Commissioner.

(3) The Commissioner shall be appointed for a term of five years and is eligible for reappointment for one additional term of five years.

(4) The Commissioner may resign the office by submitting three months notice in writing to the Governor-General.

(5) A person shall be disqualified to be appointed as Commissioner, if he is —

(a) a member of either House of Parliament;

(b) a member of the judiciary;

(c) the holder of a public office within the meaning of *Article 137* of the Constitution of The Bahamas;

(d) a person who has a financial or other interest in an enterprise or an activity that is likely to affect the discharge of that person's functions as Commissioner; or

(e) a person who has been convicted of an offence involving dishonesty.

14. Independence of the Commissioner.

(1) For the purposes of this Act, the Commissioner shall act independently in the discharge of his functions under this Act and shall not be subject to the direction or control of a person or other body, except as provided in subsection (2).

(2) The Commissioner shall be subject to the oversight of the Data Protection Oversight Committee established under section 91.

(3) The Commissioner shall enjoy independence and autonomy in managing the Office of the Data Protection Commissioner.

15. Functions of the Commissioner.

The functions of the Commissioner are to —

(a) monitor and enforce the application of this Act;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(c) promote the awareness of data controllers and data processors of their obligations under this Act;

(d) monitor the processing of personal data, sensitive personal data, and other matters affecting the privacy of an identifiable natural person in respect of his personal data, and —

(i) report to the Minister on the results of the monitoring; and

(ii) make recommendations on the need for, or desirability of taking-action to give protection or better protection to the privacy of an identifiable natural person in respect of his personal data;

(e) investigate a complaint from an identifiable natural person concerning abuses in the processing of his personal data;

(f) conduct investigations on the application of this Act on the basis of information received from a public body;

(g) conduct, at the Commissioner's discretion or where required to do so by a data subject, an audit of the personal data processed by the data controller or data processor for the purpose of determining whether the personal data of the data subject is processed in accordance with this Act;

(h) upon request, provide information to a data subject concerning the exercise of his rights under this Act;

(i) receive and invite representations on a matter affecting the privacy of personal data of members of the public;

(j) consult and cooperate with other persons, bodies and organizations concerned with the privacy of an identifiable natural person in respect of his personal data;

(k) examine a proposed legislation or proposed policy of the Government and submit a report to the Minister on the results of that examination where the proposed legislation or policy —

(i) may, in the opinion of the Commissioner, affect the privacy of identifiable natural persons in respect of their personal data; or

(ii) provides for the collection of personal data of an identifiable natural person by a public body or the disclosure of the personal data by one public body to another public body;

(l) organize activities for children to educate them about the risks, rules, safeguards and rights in relation to the processing of personal data of an identifiable natural person;

(m) undertake research into, and monitor developments in, data processing and computer technology to ensure that adverse effects on the development on the privacy of an identifiable natural person

in respect of his personal data is minimized, and report to the Minister on the results of the research and the monitoring;

(n) inquire into a written law, practice or procedure, or technical development, to determine if the personal data of an identifiable natural person is being or may be infringed, as a result the written law, practice or procedure, or technical development;

(o) provide recommendations to a person in relation to a matter that concerns the need for, or the desirability of, an action by that person in the interest of the privacy of the personal data of an identifiable natural person;

(p) provide, at his discretion or where requested to do so, advice to a Minister, public body or person on a matter relevant to the operation of this Act;

(q) report to the Minister on the desirability of the acceptance, by The Bahamas, of an international instrument or an international framework relating to the privacy of persons in respect of their personal data;

(r) monitor the recent development of information and communication technologies and the commercial practices of information, to determine if these developments have an impact on the protection of personal data;

(s) prepare and maintain codes of practice and guidelines for the guidance of data controllers and data processors on the processing of personal data of an identifiable natural person;

(t) recommend the adoption and development of standard contractual clauses and standard data protection clauses under this Act;

(u) exercise other functions as are conferred or imposed on the Commissioner by or under a written law;

(v) create and maintain a public register of all processing operations according to notifications submitted to him as prescribed in regulations under this Act; and

(w) do anything incidental or conducive to the performance of the functions in paragraphs (a) to (u).

16. Removal of the Commissioner.

(1) The office of Commissioner shall become vacant —

(a) upon the expiration of the term for which the Commissioner is appointed; or

(b) if the Commissioner resigns or is removed from office in accordance with subsection (3).

(2) The Commissioner shall not engage in another occupation while holding the office of the Commissioner.

(3) The Commissioner may be removed from office on the grounds that the Commissioner —

(a) has become incapable of effectively performing the functions of Commissioner due to an infirmity of body or mind; or

(b) has engaged in misconduct.

(4) Where advice is given to the Governor-General that grounds exist for the removal of the Commissioner under subsection (3), the Governor- General shall, after consultation with the Prime Minister and the Leader of the Opposition, appoint a tribunal which shall consist of a Chairperson and not less than two other members selected from among persons who hold or have held office as a Justice of the Supreme Court or Justice of Appeal.

(5) The tribunal appointed under subsection (4) shall —

(a) enquire into the ground concerning the removal of the Commissioner; and

(b) report on the facts obtained from their enquiry to the Governor-General and advise the Governor-General as to whether the Commissioner ought to be removed from office.

(6) Sections 9 to 14 of the Commissions of Inquiry Act (*Ch. 184*) shall apply, with all necessary changes, in relation to a tribunal and members of the tribunal appointed under subsection (4).

(7) Where the question of removal of the Commissioner has been referred to a tribunal appointed under subsection (4), and the Tribunal has advised the Governor-General that the Commissioner be removed, the Governor-General shall by instrument in writing, remove the Commissioner from office.

17. Staff of the Office of the Data Protection Commissioner.

(1) The Commissioner may, subject to the terms and conditions as may be approved by the Minister, employ—

(a) a Deputy Commissioner;

(b) a legal, policy, technical, compliance, administrative, or other staff as may be necessary for the efficient performance of the functions of the Office; and

(c) public officers on secondment as may be required.

(2) The Commissioner may, with the approval of the Minister, engage consultants or advisers possessing expertise in information governance, data protection, law, policy, risk management, or information security, on the terms as may be determined.

(3) The Deputy Commissioner shall perform the functions of the Commissioner —

(a) during any period when the office of Commissioner is vacant; or

(b) during any period when the Commissioner is unable to perform the functions of the office,

and, when so acting, the Deputy Commissioner shall have all the powers and duties of the Commissioner.

(4) The employment of staff and consultants under this section shall be on the terms and conditions as the Commissioner may, with the approval of the Minister, determine.

18. Funds.

(1) The funds of the Office of the Data Protection Commissioner shall consist of —

(a) fees and other sums received by the Commissioner in the exercise of the Commissioner's functions; and

(b) sums of money as may be appropriated to the Office of the Data Protection Commissioner by Parliament for the purposes of the Office of the Data Protection Commissioner.

(2) There shall be paid from the funds of the Office of the Data Protection Commissioner —

(a) salaries, honorarium, allowances, pensions and gratuities of the staff of the Office of the Data Protection Commissioner;

(b) remuneration, reasonable travelling and subsistence allowances as the Office of the Data Protection Commissioner may determine, for its officers when engaged on the business of the Office of the Data Protection Commissioner;

(c) other expenses incurred by the Office of the Data Protection Commissioner in the performance of its functions.

19. Confidential information.

(1) The Commissioner and staff of the Office of the Data Protection Commissioner appointed under section 17(1) shall keep secret, all confidential information coming to his knowledge during the course of the administration of this Act.

(2) Subsection (1) shall not apply where disclosure is required —

(a) for the administration of this Act under sections 47 and 58(3);

(b) by law or made in connection with legal proceedings under section 63;

(c) by an order made by a court of competent jurisdiction;

(d) by a duty or obligation imposed by a written law;

(e) in an international agreement to which The Bahamas is a party.

(3) Subject to subsection (2), a person who discloses confidential information in contravention of subsection (1), commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or to a term of imprisonment not exceeding one year or to both.

(4) A person who —

(a) knowingly or recklessly discloses confidential information to any other person;

(b) discloses confidential information to any other person with the intent to obtain a benefit for himself or another person; or

(c) discloses confidential information to cause harm to another person,

commits an offence and is liable on summary conviction to a fine not exceeding twenty thousand dollars or to a term of imprisonment not exceeding two years or to both.

(5) In this section **"confidential information"** means information of whatever kind and in whatever form that —

(a) relates to a person or an identifiable natural person and is obtained by or on behalf of the Commissioner for the purpose of administering or enforcing this Act; or

(b) is prepared from information which relates to one or more persons or an identifiable natural person but does not include information that directly or indirectly reveals the person or an identifiable natural person to whom it relates.

(6) It shall be a defence for a person charged with an offence under this section to prove that the person acted in good faith and took all reasonable steps and exercised all due diligence to prevent the contravention.

20. Indemnity.

The Commissioner and the staff of the Office of the Data Protection Commissioner shall not be subject to an action, claim, or demand by, or liability to, a person in respect of anything done or omitted to be done in good faith in the discharge or in connection with the discharge of the functions conferred on the Commissioner and his staff under this Act.

21. Annual report.

(1) The Commissioner shall, not later than 30 June in each year, prepare and submit to the Minister an annual report on the activities and performance

of the Office of the Data Protection Commissioner during the preceding year.

(2) The report shall include—

(a) information on investigations, enforcement actions, and compliance activities undertaken during the year;

(b) the number and types of complaints received;

(c) guidance, codes of practice, or recommendations issued;

(d) outreach, public education, and policy initiatives undertaken; and

(e) any other matter the Commissioner considers relevant to the administration of this Act.

(3) The Minister shall lay or cause to be laid before both Houses of Parliament an annual report before 30 September in each year, and shall publish the annual report in the *Gazette* and on the official website of the Office of the Data Protection Commissioner.

22. Codes of Conduct and Practice, Guidelines and data protection certification standards.

(1) The Commissioner may —

(a) issue Codes of Practice, Codes of Conduct, and Guidelines for data controllers, data processors, and data protection officers, setting out best practices for compliance with this Act;

(b) issue Data Protection Certification Standards in order to encourage compliance of processing operations with this Act;

(c) require certification or adherence to Codes of Practice, Codes of Conduct, and Guidelines by a third party;

(d) develop sector specific guidelines in consultation with relevant stakeholders in the areas of health, financial services, education, social protection and other areas as the Data Commissioner may determine,

that are necessary for the better carrying out of the provisions of the Act.

(2) The Commissioner shall publish all Codes of Practice and Guidelines, and Data Protection Certification Standards in the *Gazette and* on the official website of the Office of the Data Protection Commissioner.

(3) Codes of Practice, Codes of Conduct, and Guidelines issued under subsection (1), are not legally binding.

(4) A data controller, data processor, or data protection officer shall have due regard to any issued Code or Guideline under subsection (1), when carrying out their duties under this Act.

(5) In determining compliance with this Act, the Commissioner or a court may take into account any relevant Code or Guideline issued under this section.

23. International Cooperation.

The Minister may, after consultation with the Minister responsible for Foreign Affairs and the Commissioner, make regulations for the cooperation by the Office of the Data Protection Commissioner with authorities in Foreign States, who exercise functions similar to those of the Commissioner under this Act, in connection with the exchange of information between the Office of the Data Protection Commissioner and authorities in Foreign States.

PART IV – DATA SUBJECT

RIGHTS

24. Right of access to personal data.

(1) Subject to the exemptions provided under Part VII of this Act, a data subject shall —

(a) be informed by a data controller whether personal data of the data subject is being processed by or on behalf of the data controller;

(b) request from, and be given by the data controller, where personal data of the data subject is being processed by or on behalf of the data controller, detailed information of —

(i) the purposes for the processing of the personal data;

(ii) the categories of personal data being processed;

(iii) the recipients or categories of recipient to whom the personal data has been disclosed or shall be disclosed;

(iv) the recipients in other countries or international organizations to whom the personal data has been disclosed or shall be disclosed;

(v) the length of time for which the personal data shall be stored, and the criteria to be used to determine the length of time for storage;

(c) be given information on the right to request from the data controller —

(i) the rectification or erasure of his personal data;

(ii) the restriction of the processing of the personal data;

(iii) the method of objection to the processing of his personal data;

(d) be given information on the countries and territories outside of The Bahamas to which the data controller, whether directly or indirectly, transfers, intends to transfer, or wishes to transfer the personal data;

(e) be provided with details of the information and the source of the information, where the personal data is not collected from the data subject;

(f) be advised of general measures to be taken for the purpose of complying with the data protection principles specified in section 5(1); and

(g) be provided with other information required by the Commissioner.

(2) A data controller shall communicate with the data subject in a clear, intelligent and unambiguous manner, concerning —

(a) the data subject's personal data; and

(b) other information available to the data controller on the source used to obtain the personal data.

(3) If the personal data of the data subject has been processed by automated means and is used for the purposes of —

(a) evaluating matters relating to the data subject;

(b) evaluating the data subject's performance at work;

(c) assessing the creditworthiness of the data subject; and

(d) determining the reliability or conduct of the data subject,

and the personal data processed by automatic means constituted or is likely to constitute, the sole basis for a decision significantly affecting the data subject, the data subject shall be informed by the data controller of the reasons for that decision.

(4) A data controller shall not be obliged under subsections (1), (2) or (3) to supply personal data to a data subject unless the data controller has received —

(a) a request in writing; and

(b) the prescribed fee.

(5) Where a data controller reasonably requires further information in order to —

(a) be satisfied as to the identity of the data subject making the request; or

(b) to locate the information that the data subject seeks,

and has informed the data subject in writing of the requirement, the data controller is not obliged to comply with the request unless supplied with the further information requested.

(6) A data controller shall comply with a request under this section within thirty days (or other period as may be prescribed by regulations) of the date on which the data controller receives the request and the fee specified in subsection (4), but where the data controller has requested further information under subsection (5), the period to supply the information shall not commence until the information requested has been provided.

(7) If a data controller cannot comply with the request under subsection (4) without disclosing personal data relating to another data subject who can be identified from the personal data, the data controller is not obliged to comply with the request unless —

(a) the other data subject has consented to the disclosure of the personal data to the person making the request; or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other data subject.

(8) In subsection (7), the reference to personal data relating to another data subject includes a reference to personal data identifying the other data subject as the source of the personal data sought in the request.

(9) Subsection (7) shall not be construed as excusing a data controller from supplying that part of the personal data as can be supplied without disclosing the identity of the other data subject concerned, whether by the omission of names or other identifying particulars or otherwise.

(10) In determining for the purposes of subsection (7)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other data subject concerned, the data controller shall have regard to —

(a) a duty of confidentiality owed to the other data subject;

(b) steps taken by the data controller to seek the consent of the other data subject;

(c) whether the other data subject is capable of giving consent; and

(d) an express refusal of consent by the other data subject.

(11) If the Commissioner is satisfied on the application of a data subject who has made a request under this section that a data controller has contravened this section in failing to comply with the request, the Commissioner shall issue an enforcement notice under section 74 ordering the data controller to comply with the request.

(12) If a request made under this section is received by a data processor who is processing the personal data of the data subject on behalf of a data controller, the data processor shall inform the data subject of his right to make his request to the data controller.

(13) As regards the treatment of requests made under this section —

(a) the obligation imposed by subsection (2)(a) shall be complied with by supplying the data subject with a copy of the personal data in the format requested unless —

(i) the supply of the copy is not possible or would involve disproportionate effort; or

(ii) the data subject agrees not to be supplied with the copy;

(b) if any of the personal data referred to in subsection (2)(a) are expressed in terms that are not intelligible without explanation the copy shall be accompanied by an adequate explanation;

(c) if a data controller has previously complied with a request under this section by the data subject, the data controller is not obliged to comply with a subsequent identical or similar request under this section by the data subject unless the interval between compliance with the previous request and the making of the current request is reasonable;

(d) in determining whether the interval referred to in paragraph (c) is reasonable, regard shall be had to the nature of the personal data, the purpose for which the personal data is processed and the frequency with which the personal data is altered;

(e) information under subsection (3) shall not be provided if information as to the reasons of any decision-making constitutes a trade secret;

(f) personal data and other information supplied under this section shall be supplied by reference to the personal data in question at the time when the request for the personal data is received, except that account may be taken of an amendment or deletion to the personal data made between the time the request for the personal data was made and when the information is supplied;

(g) in carrying out its obligations under subsections (1) to (3), the data controller shall only be obliged to supply the confirmation, information and copies of personal data as the data controller is able to identify by carrying out a reasonable and proportionate search for the personal data.

25. Right to file complaint.

(1) A data processor, data subject or an agent of a data controller, may file a complaint with the Commissioner if the data subject considers that the processing of personal data by a data controller contravenes this Act.

(2) The Commissioner shall assess all complaints received under subsection (1), and following the assessment, inform the complainant in writing whether the complaint shall be investigated and the reasons for the investigation of the complaint.

26. Right to rectification of inaccurate personal data.

(1) The data subject has the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning the data subject.

(2) The data subject shall, having regard to the purposes of the processing, have the incomplete personal data completed by the data controller through the provision of a supplementary statement.

(3) The data controller shall —

(a) communicate any rectification of personal data to each recipient to whom the personal data has been disclosed unless this proves impossible or involves disproportionate effort; and

(b) inform the data subject of those recipients referred to in paragraph (a) where the data subject requests the information.

27. Right to object to the processing of personal data.

(1) A data subject is entitled at any time, by notice in writing to a data controller, to object, on grounds relating to his particular situation, to the processing and profiling of personal data under section 6(1)(b)(iv) and (v).

(2) The data controller shall, within twenty-one days of receiving a notice under subsection (1), comply with the notice unless the data controller demonstrates compelling legitimate grounds for the processing which override the fundamental rights and freedoms of the data subject or for the purpose of legal proceedings.

(3) Where, in accordance with subsection (2), the data controller refuses to comply with a notice under subsection (1), the data controller shall provide to the data subject the reasons for the non-compliance with the notice.

(4) If, on the application of a data subject who has given notice under subsection (1), the Commissioner is satisfied that the data controller in question has failed to comply with the notice, the Commissioner may issue an enforcement notice under section 74.

(5) The failure by a data subject to exercise the right conferred by subsection (1) does not affect any other right conferred on the data subject by this Act.

28. Right to erasure of personal data.

(1) Under subsection (2), the data subject has the right to require the data controller to erase personal data concerning him without undue delay.

(2) The data controller shall erase personal data without undue delay where one of the following grounds applies —

(a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

(b) the data subject withdraws consent where the processing occurs in accordance with section 6(1)(a) or section 37(1)(a), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing of personal data under section 27 and there are no overriding legitimate grounds for the processing, or the data subject does not consent to the processing of personal data for the purposes of direct marketing under section 37;

(d) the personal data has been unlawfully processed; or

(e) the personal data has to be erased in compliance with a legal obligation in The Bahamas to which the data controller is subject.

(3) A data controller who has made the personal data of the data subject public, shall —

(a) erase the personal data of the data subject under this section;

(b) in considering the available technology and cost, take reasonable steps to inform other data controllers who are processing the personal data of the data subject, that the data subject has requested —

(i) the erasure of the personal data;

(ii) the removal of the personal data from all internet links; and

(iii) the destruction of all copies of the personal data.

(4) The right of the data subject to have the personal data erased under this section, is overridden by the data controller to the extent that processing of the personal data is necessary for —

(a) exercising the right to freedom of expression and information;

(b) complying with a legal obligation that requires the processing of personal data by a written law to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of the authority vested in the data controller;

(c) reasons of public interest, specifically, public health;

(d) archiving for research purposes under section 61; or

(e) the purpose of legal proceedings.

(5) The data controller shall —

(a) communicate any erasure of personal data to each recipient to whom the personal data has been disclosed unless this proves impossible or involves disproportionate effort; and

(b) inform the data subject of those recipients referred to in paragraph (a) where the data subject requests the information.

29. Right to restrict the processing of personal data.

(1) The data subject shall have the right to require the data controller to restrict the processing of the personal data of the data subject if —

(a) the accuracy of the personal data is contested by the data subject;

(b) the processing is unlawful;

(c) the data subject objects to the erasure of the personal data;

(d) the data controller no longer needs the personal data for the purposes of the processing;

(e) the personal data is required by the data subject for the purpose of legal proceedings;

(f) the data subject has, under section 27, objected to processing pending the verification of whether there exists legitimate grounds of the data controller to override the rights of the request of the data subject.

(2) Where processing has been restricted under subsection (1), the personal data of the data subject shall, with the exception of storage, only be processed —

(a) with the data subject's consent;

(b) for the purpose of legal proceedings;

(c) for the protection of the rights of another person; or

(d) for reasons of public interest.

(3) The data controller shall —

(a) communicate the restriction of the processing of personal data of the data subject, to each recipient to whom the personal data has been disclosed, unless the communication to the recipient proves impossible or involves disproportionate effort; and

(b) inform the data subject of the recipients to whom the personal data of the data subject has been disclosed.

30. Right to prevent data processing.

(1) Subject to subsection (2), a data subject shall, by written notice, require the data controller to cease, or not to begin the processing of the personal data of the data subject, whether or not the processing of the personal data is for a specified purpose or processed in a specified manner, on the ground that —

(a) the processing of the personal data of the data subject by the data controller, is causing or is likely to cause, substantial damage or distress to the data subject or another identifiable natural person;

(b) the substantial damage or distress to the data subject or another identifiable natural person is or would be unwarranted.

(2) Subsection (1) does not apply —

(a) in a case where the conditions specified in section 6(1)(a) or 6(1)(b)(i) to (iv) are satisfied; or

(b) in other cases as the Minister may prescribe by order.

(3) A data subject who is desirous of exercising his right under this section, shall comply with the regulations made under this Act.

31. Right of data subject to receive and transfer data.

(1) A data subject shall have the right to receive the personal data concerning him, which a data subject has provided to a data controller, in a structured, commonly used and machine-readable format, and shall have the right to transmit the personal data to another data controller without hindrance from the data controller to which the personal data was originally provided.

(2) The right to receive and transfer personal data under subsection (1) applies where —

(a) the processing is based on the data subject's consent or on a contract to which the data subject is a party; and

(b) the processing is carried out by automated means.

(3) In exercising the right referred to in subsection (1), a data subject may request that the personal data be transmitted directly from one data controller to another, where this is technically feasible.

(4) The exercise of the right under this section shall not adversely affect the fundamental rights and freedoms of other persons.

(5) The Minister, upon the recommendation by the Commissioner, shall by regulation, prescribe the form, format and technical standards for the secure and efficient exercise of the right specified in subsection (1).

32. Right to compensation.

(1) A data subject who has suffered material damage as a result of a breach of his rights under this Act by a data controller or data processor, may commence proceedings in the Supreme Court against that data controller or data processor, to recover compensation for the damage suffered.

(2) In any proceedings under subsection (1), a data controller or data processor shall not be liable if he proves that he took all reasonable steps and exercised all due diligence to comply with this Act.

(3) The Supreme Court may, in awarding compensation, take into account —

(a) the nature, gravity, and duration of the contravention;

(b) the degree of fault or negligence of the data controller or data processor;

(c) the actions taken to mitigate the damage suffered; and,

(d) the conduct of the data subject in relation to the matter.

(4) Nothing in this section limits any other right or remedy available under law in respect of the same facts.

CONSENT

33. Conditions for consent.

(1) Where the processing of personal data is based on the consent of the data subject, the data controller shall provide clear and verifiable evidence that the data subject has given consent to the processing of his personal data.

(2) Where the consent of the data subject is given in a written declaration that also deals with other matters, the request for consent must be presented —

(a) in a manner that is clearly distinguishable from the other matters;

(b) intelligibly and in an easily accessible form; and

(c) using clear and plain language.

(3) The data controller, prior to the giving of consent by a data subject, shall inform the data subject of his right to withdraw his consent.

(4) A data subject has the right to withdraw his consent in respect of the processing of his personal data at anytime.

(5) The withdrawal of consent by the data subject does not affect the lawfulness of the processing of the personal data, based on the consent given by the data subject prior to withdrawal.

(6) For the purposes of determining whether a data subject freely gives consent to the processing of personal data, the data controller shall take into account whether the consent of the data subject is conditional to the performance of a contract and the service provided in the contract.

34. Special conditions for consent of a child or a vulnerable person.

(1) Where the data subject is —

(a) a child, the rights of the child under this Act shall be exercised by the parent or legal guardian of the child, except to the extent that the Commissioner determines that the child has sufficient

understanding to exercise the rights of the child on his own behalf; or

(b) a vulnerable person, the rights of a vulnerable person under this Act shall be exercised by the guardian or conservator appointed under the Mental Health Act, 2022 (*No. 40 of 2022*).

(2) The data controller shall not process the personal data of a child or vulnerable person unless consent is given by the parent or legal guardian of the child or the legal guardian of a vulnerable person.

(3) A data controller shall make every reasonable effort, to verify that consent is given or authorized by the parent or legal guardian of a child or the legal guardian of a vulnerable person.

(4) A data controller shall take appropriate measures to verify —

(a) the age of a child;

(b) the consent of the parent or legal guardian of the child;

(c) the consent of the legal guardian of the vulnerable person,

in the processing of personal data under this section.

(5) For the purposes of this section —

"vulnerable person" means an identifiable natural person aged eighteen years or above —

(a) whose ability to make informed decisions in relation to his rights under this Act is temporarily or permanently impaired by reason of a physical, mental, or cognitive condition; or

(b) who is subject to an order of guardianship or conservatorship from the Supreme Court; or

(c) who is the donor of ~~to~~ an enduring power of attorney or similar legal arrangement, under any written law by reason of the impairment.

(6) Notwithstanding (a), (b) and (c), for the purposes of this Act, an identifiable natural person is not to be regarded as a vulnerable person merely by reason of age or disability, unless the impairment materially affects their ability to exercise their rights under this Act.

35. Conditions for processing sensitive personal data.

(1) The sensitive personal data of a data subject shall not be processed without the consent in writing of the data subject.

(2) Notwithstanding subsection (1), the processing of the sensitive personal data of the data subject shall be processed by the data controller, where the sensitive personal data is necessary for —

(a) the purposes of exercising or performing a right, or obligation, conferred or imposed by a written law on the data controller, in connection with the employment of the data subject;

(b) the purpose of legal proceedings;

(c) the purpose of obtaining legal advice;

(d) the purposes of establishing, exercising or defending legal rights;

(e) medical purposes and is undertaken by —

(i) a health care professional; or

(ii) a person who owes a duty of confidentiality equivalent to that which would arise if that person were a health care professional;

(f) the work of a court or tribunal;

(g) the administration of justice;

(h) the exercise of functions conferred on a person by or under a written law;

(i) the exercise of functions of the Crown, Parliament or a public body;

(j) the processing for archiving purposes in the public interest and for the purposes of scientific research purposes, historical research purposes or statistical purposes;

(k) the purposes of preventing or detecting an unlawful act including offences of fraud, money-laundering and terrorism;

(l) providing confidential counselling, advice or support or of another similar service which is provided confidentially;

(m) protecting an identifiable natural person from neglect or physical, mental or emotional harm, where an identifiable natural person is under the age of eighteen or is otherwise susceptible to emotional harm;

(n) the exercise of a protective function which is intended to protect members of the public against —

(i) dishonesty, malpractice or other seriously improper conduct;

(ii) unfitness or incompetence;

(iii) mismanagement in the administration of a body or association; or

(iv) failures in services provided by a body or association;

(o) the purposes of complying with, or assisting another person to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has —

(a) committed an unlawful act; or

(b) been involved in dishonesty, malpractice or other seriously improper conduct;

(p) reasons of substantial public interest and the processing of sensitive personal data —

(i) consists of the disclosure of sensitive personal data for the special purposes of journalism, academic expression, artistic expression, or literary expression;

(ii) is carried out in connection with the following matters, whether alleged or established —

(aa) the commission of an unlawful act by a person;

(bb) dishonesty, malpractice or other seriously improper conduct of a person;

(cc) unfitness or incompetence of a person;

(dd) mismanagement in the administration of a body or association;

(ee) a failure in services provided by a body or association;

(iii) is carried out with the intention of publishing the sensitive personal data of the data subject;

(q) the purposes of the political activities of a person and the processing is —

(i) of the sensitive personal data of the data subject revealing political opinions;

(ii) carried out by a person or organization;

(iii) unlikely to cause substantial damage or distress to a person;

(r) the purposes of measures designed to identify or prevent doping which are undertaken by or under the responsibility of a body or association that is responsible for eliminating doping in a sport, at a sporting event or in sport generally;

(s) the purposes of providing information about doping, or suspected doping, to a body or association.

(3) For the purposes of paragraph (e) of subsection (2), **"medical purposes"** includes the purposes of preventative medicine, medical diagnosis, the provision of care and treatment, the management of health care services and reasons of public health.

(4) Notwithstanding subsection (1), the processing of the sensitive personal data of the data subject is necessary in order to protect the vital interests —

(a) of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data

controller cannot reasonably be expected to obtain the consent of the data subject; or

(b) of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

(5) Notwithstanding subsection (1), the processing of the sensitive personal data of the data subject may be carried out —

(a) by the data controller in the course of its legitimate activities by a body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade union purposes;

(b) by the data controller with appropriate safeguards for the fundamental rights and freedoms of the data subject;

(c) where the processing of sensitive data relates only to identifiable natural persons who are members of the non-profit organization or who maintain regular and direct contact with the organization in furtherance of, or directly related to, its stated purposes, objectives or initiatives; and

(d) where the processing of sensitive data does not involve disclosure of the personal data to a third party without the consent of the data subject.

(6) The sensitive personal data of a data subject may be processed where the information contained in the sensitive personal of the data subject has been made public, as a result of steps taken by the data subject.

(7) The Minister may, upon the recommendation of the Commissioner, specify by order, other circumstances where sensitive personal data of the data subject may be processed.

36. Sensitive personal data relating to health.

(1) Sensitive personal data relating to the health of a data subject, may only be processed with the consent of data subject and processed —

(a) by or under the responsibility of a health care professional; or

(b) by a person subject to the obligation of professional secrecy under a written law.

(2) Notwithstanding subsection (1), sensitive personal data relating to the health of a data subject may be processed, where the processing is —

(a) necessary for reasons of public interest in the area of public health; or

(b) carried out by another person who in the circumstances owes a duty of confidentiality under a written law.

37. Consent required for direct marketing.

(1) A data controller shall not process personal data of the data subject for the purpose of direct marketing unless the data subject consents to the processing of his personal data for that purpose.

(2) A data controller shall request the consent of a data subject in the prescribed manner, and shall not approach a data subject more than once to request the consent of the data subject to receive direct marketing by means of a particular medium.

(3) A data controller may process the personal data of a data subject who is a customer of that data controller for the purpose of direct marketing —

(a) if the data controller has obtained the contact details of the data subject in the context of the sale of goods or services;

(b) of the data controller's own goods or services; and

(c) if the data subject has been given a reasonable opportunity to object, free of charge in the prescribed manner, to the use of the data subject's personal data —

(i) at the time the personal data was collected; and

(ii) on the occasion of each communication with the data subject for the purpose of direct marketing.

(4) A communication to a data subject for the purpose of direct marketing shall contain —

(a) the details of the identity of the sender or the person on whose behalf the communication has been sent; and

(b) an address or other contact details to which the data subject may send an objection to the use of his personal data for the purpose of direct marketing.

(5) In this section, **"direct marketing"** means to approach a data subject by any means of communication or otherwise, for the purpose of —

(a) promoting or offering to supply goods or services in the ordinary course of business; or

(b) requesting a donation from the data subject.

(6) A data controller may approach a data subject for the purpose of direct marketing by a communication that intentionally targets the data subject based on personal data relative to the data subject.

(7) A data controller may not approach a data subject for the purposes of direct marketing by general advertising not directed to any particular individual.

(8) This section does not apply to a marketing activity which takes place on a face to face basis, namely, marketing conducted at trade shows, temporary

public displays and other marketing activity conducted where both parties are present together in the same location.

PART V – DATA CONTROLLERS AND DATA PROCESSORS

38. Registration of data controllers and data processors.

(1) Subject to subsection (4), a data controller or data processor, shall submit an application of registration to the Office of the Data Protection Commissioner.

(2) Notwithstanding subsection (1), for the purposes of registration, a person who operates as a data controller or data processor and who is not established in The Bahamas, shall nominate a representative established in The Bahamas.

(3) The requirement to appoint a representative established in The Bahamas, shall not apply where the data controller or data processor engages in the processing of personal data which —

(a) is occasional;

(b) does not include large scale processing of —

(i) sensitive personal data; or

(ii) personal data relating to criminal conviction and offences; and

(iii) personal data that is unlikely to result in a risk to the fundamental rights and freedoms of an identifiable natural person,

taking into account the nature, context, scope and purpose of the processing.

(4) The requirement to appoint a representative established in The Bahamas shall not apply to a public body.

(5) The Minister, upon the recommendation by the Commissioner, shall by regulation, prescribe the categories of data controllers and data processors that are subject to, or exempt from, mandatory registration obligations under this Act.

(6) A person who operates as a data controller or data processor without being registered under this section commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or to a term of imprisonment not exceeding six months or to both.

39. Application for registration.

(1) A person who desires to operate as a data controller or data processor shall register at the Office of the Data Protection Commissioner in the prescribed manner and the prescribed form and pay the prescribed fee.

(2) An application for registration under subsection (1) shall provide for the following particulars —

(a) a description of the personal data to be processed by the data controller or data processor, along with a retention schedule;

(b) a description of the purpose for which the personal data is to be processed;

(c) the category of data subjects to which the personal data relates;

(d) contact details of the data controller or data processor;

(e) a general description of the technical and organizational measures adopted by the data controller and the data processor to ensure the security of the processing of the personal data;

(f) any measures to indemnify the data subject from unlawful use of data by the data controller or data processor; and

(g) other details as may be required by the Commissioner.

(3) A person who knowingly supplies false details on his application for registration as a data controller commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years or to both.

40. Registration certificate.

(1) The Commissioner shall issue a certificate of registration to a data controller or data processor who meets the requirements for registration under section 39.

(2) A registration certificate issued under this section, is valid for a period of one year from the date of issue.

(3) A data controller and data processor shall display the certificate of registration issued under this Act in a conspicuous place, at their principal place of business.

(4) A certified copy of the certificate of registration issued under subsection (2), shall be displayed at every subsidiary premises where the registered data controller or data processor carries on business.

41. Renewal of registration certificate.

(1) A data controller or data processor shall, upon expiry of his registration certificate, apply to the Office of the Data Protection Commissioner for

the renewal of the registration certificate in the prescribed manner and pay the prescribed fee.

(2) The Commissioner shall, within twenty-eight days of receiving an application for the renewal of a registration certificate, grant or reject the application.

(3) Where the Commissioner rejects an application submitted under subsection (1), he shall provide reasons for the rejection, to the applicant in writing.

(4) A person who knowingly supplies any false details on his application for the renewal of his registration as a data controller or data processor, commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years or to both.

42. Register of Data Controllers.

(1) The Commissioner shall maintain a register, to be called the Register of Data Controllers, in which he shall cause to be entered in relation to each data controller registered under this Act, the following particulars —

(a) the name, address and contact information of the data controller;

(b) the date of registration of the data controller; and

(c) the name, address and contact information of each registered data controller who is nominated as a representative for a data controller who is not established in The Bahamas.

(2) The data controller shall give written notice to the Commissioner, of any changes which may affect the particulars entered in the Register of Data Controllers as it relates to the data controller.

(3) The Register of Data Controllers shall be a public document and available for inspection at all reasonable times by a person upon payment of the prescribed fee.

(4) The Commissioner shall ensure that the Register of Data Controllers is kept accurate and up to date.

43. Register of Data Processors.

(1) The Commissioner shall maintain a register, to be called the Register of Data Processors, in which he shall cause to be entered in relation to each data processor registered under this Act, the following particulars —

(a) the name, address and other contact information of the data processor;

(b) the date of registration of the data processor; and

(c) the name, address and contact information of each registered data processor who is nominated as a representative for a data processor who is not established in The Bahamas.

(2) The data processor shall give written notice to the Commissioner of any changes which may affect the particulars entered in the Register of Data Processors as it relates to the data processor.

(3) The Register of Data Processors shall be a public document and available for inspection at all reasonable times by any person upon payment of the prescribed fee.

(4) The Commissioner shall ensure that the Register of Data Processors is kept accurate and up to date.

44. Data processing records.

(1) A data controller and where applicable, the data controller's representative shall keep and maintain, in writing or by electronic means, a record of data processing activities under its responsibility.

(2) A record maintained by a data controller under subsection (1) shall contain —

(a) the name and contact details of the data controller and the data controller's representative and the name and contact details of the data protection officer;

(b) the purposes of the processing of the personal data;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) a description of the categories of recipients to whom the personal data has been or will be disclosed;

(e) a description of the recipients in other countries or international organizations to whom the personal data has been or will be disclosed;

(f) information on the transfers of personal data by the data processor or by the data processor on behalf the data controller, to another country or an international organization;

(g) the identification of the country or international organization where the personal data was transferred by data processor under section 54;

(h) the documentation of the adequate level of protection of the fundamental rights and freedoms of data subjects in relation to the processing of personal data;

(i) the envisaged time limits for erasure of the different categories of personal data; and

(j) a general description of the technical and organizational measures referred to in section 53(2).

(3) A data controller shall, upon the request of the Commissioner, make data processing records available to the Commissioner.

(4) A data processor and where applicable, the data processor's representative shall maintain, in writing or by electronic means, a record of all categories of processing activities carried out on behalf of a data controller, which shall contain —

(a) the name and contact details of the data processor and each data controller on behalf of whom the data processor is acting, and where applicable, the name and contact details of the representative of the data controller or the data processor and the name and contact details of the data protection officer;

(b) the categories of processing of personal data carried out on behalf of each data controller;

(c) information on transfers of personal data to another country or an international organization under section 54;

(d) the documentation of the adequate level of protection for the fundamental rights and freedoms of data subjects in relation to the processing of personal data; and

(e) a general description of the technical and organizational measures referred to in section 53(2).

(5) The obligations referred to in subsections (1) and (4) above, shall not apply to an enterprise or an organization employing fewer than one hundred and fifty persons, unless the processing of personal data it carries out is likely to result in a risk to the rights and freedoms of a data subject.

(6) The Minister may, after consultation with the Commissioner, make regulations prescribing categories of data controllers or data processors that are small-sized or medium-sized businesses which may be exempted, whether wholly or in part, from the requirements of subsections (2) and (4), where the exemption is necessary and proportionate to reduce administrative burdens, having regard to the scale, nature and context of the processing carried out by those businesses.

45. Auditing of data controllers and data processors.

(1) The Commissioner may annually audit the policies of a data controller and data processor and the conduct of the processing of personal data.

(2) Where a data controller or data processor has been authorized to transfer data on a server or data centre located outside of The Bahamas, the cost of reviewing or auditing the server of the data controller or data processor shall be borne by the data controller and the data processor.

46. Appointment of a data protection officer.

(1) A data controller and the data processor shall appoint a person as the data protection officer on the terms and conditions as the data controller and data processor may determine, where —

(a) the processing of personal data is carried out by a public body or private body;

(b) the core activities of the data controller or the data processor consist of processing operations which, by its nature, scope, or purposes, require regular and systematic monitoring of data subjects; or

(c) the core activities of the data controller consist of the processing of sensitive personal data.

(2) A data controller and data processor shall —

(a) appoint a person as a data protection officer if that person has relevant academic or professional qualifications and knowledge and technical skills in matters relating to data protection; and

(b) support the data protection officer by providing the resources necessary to —

(i) maintain the data protection officer's expert knowledge; and

(ii) enable the data protection officer to carry out the functions provided in subsection (3).

(3) The functions of a data protection officer include —

(a) informing and advising the data controller or the data processor and of their obligations under this Act;

(b) informing and advising the employees of the data controller or the data processor, who carry out the processing of personal data, of their obligations under this Act;

(c) monitoring compliance with this Act and with the policies of the data controller or data processor in relation to the protection of personal data;

(d) monitoring the assignment of responsibilities, awareness-raising and training of staff involved in the processing of personal data and related audits;

(e) advising the data controller and his employees on data processing requirements that are contained in this Act or in another written law;

(f) facilitating capacity building of staff involved in the processing of personal data;

(g) providing advice on the preparation of the data protection impact assessment under section 51;

(h) acting as the contact point for the Commissioner on issues relating to the processing of personal data;

(i) acting as the contact point during consultations with the Commissioner as specified in section 51(6) to (8); and

(j) cooperating with the Commissioner on matters relating to data protection.

(4) A data protection officer shall —

(a) not be dismissed or penalized by the data controller or data processor for performing the functions provided in subsection (3); and

(b) keep confidential all matters concerning the performance of his duties and functions referred to in subsection (3).

(5) The Minister may, after consultation with the Commissioner, make regulations prescribing categories of data controllers or data processors that are small-sized or medium-sized businesses which may be exempted, whether wholly or in part, from the requirements of this section, where the exemption is necessary and proportionate to reduce administrative burdens, having regard to the scale, nature and context of the processing carried out by those businesses.

(6) A person may be appointed as a data protection officer by more than one data controller or data processor on the condition that the data protection officer is accessible to each data controller or data processor.

(7) A data protection officer may be appointed for one public body or two or more public bodies.

(8) A data controller and a data processor shall publish the contact details of the data protection officer on its official website and provide the contact details to the Commissioner.

47. Non-disclosure of personal data.

(1) Except as provided in this Act, a person shall not disclose to another person or allow another person to have access to the content or nature of the personal data of the data subject, in his possession.

(2) A data controller shall not disclose the personal data of a data subject without first obtaining the consent of the data subject under this Act, unless the disclosure of the personal data is necessary to —

(a) prevent a reasonable threat to national security, defence, public safety or public order; or

(b) investigate or prosecute a cognizable offence.

(3) A data controller who is required to disclose the personal data of a data subject shall, prior to disclosing the personal data, inform the data subject of —

(a) when and to whom the personal data shall be disclosed;

(b) the purpose of the disclosure of the personal data;

(c) the security practices, privacy policies and other policies, that protect the personal data of the data subject; and

(d) the procedure for recourse in case of a grievance in relation to the disclosure of the personal data.

(4) A person who contravenes this section commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years or to both.

48. Notification of breach of personal data.

(1) A data controller shall notify the Commissioner, within seventy-two hours of becoming aware of a personal data breach, where the breach is likely to result in a risk to the fundamental rights and freedoms, reputation, or other legitimate interests of an identifiable natural person, or involves the unauthorized disclosure of sensitive personal data.

(2) For the purposes of subsection (1), without limiting other relevant factors, a data breach shall automatically be deemed likely to result in a risk where it —

(a) involves sensitive categories of personal data;

(b) could cause humiliation, harm, distress, reputational damage, or economic loss to a data subject; or

(c) exposes personal data to unauthorized access, use, or disclosure.

(3) Where the notification referred to in subsection (1) is not made by the data controller to the Commissioner within seventy-two hours, the data controller shall provide reasons for the delay to the Commissioner.

(4) A data processor shall notify the data controller within seventy-two hours, after having become aware of a breach of personal data.

(5) The notification of the breach of personal data referred to in subsections (1) and (4) shall —

(a) describe the nature of the breach;

(b) specify the categories of the breach;

(c) specify, or provide an estimate of, the number of data subjects affected by the breach;

(d) specify the categories and number of personal data records affected by the breach;

(e) specify the name and contact details of the data protection officer or other contact point where more information can be obtained;

(f) describe the consequences of the breach;

(g) describe the measures taken or measures proposed to be taken to address the breach; and

(h) outline the measures to mitigate the adverse effects of the breach.

(6) Where it is not possible to provide all the information required under subsection (5) at the same time, the information may be provided in phases within seven working days or within a extended time as prescribed.

(7) The data controller shall record every breach of personal data and shall describe in the record —

(a) the facts relating to the breach;

(b) the effects of the breach; and

(c) the remedial action taken in order to facilitate the assessment by the Commissioner of the compliance of this section by the data controller.

49. Communication of breach of personal data to a data subject.

(1) Where a breach of personal data is likely to result in the violation of the fundamental rights and freedoms of a data subject or the unauthorized disclosure of an identifiable natural person's sensitive personal data, the data controller shall communicate the breach of personal data to the data subject within seventy-two hours after having become aware of the breach.

(2) The communication of the breach of personal data specified in subsection (1) shall describe in clear and plain language the nature of the breach and contain the information specified in section 48(4).

(3) The communication of the breach of personal data to the data subject referred to in subsection (1), is not required where the following conditions are satisfied that —

(a) the data controller has implemented technical and organizational measures which when applied to the personal data affected by the breach, renders the personal data unintelligible to a person who is not authorized to access it;

(b) the data controller has taken subsequent measures which ensure that the violation of the fundamental rights and freedoms of a data subject is no longer likely to materialize; or

(c) the notification of the breach would involve a disproportionate effort due to the number of data subjects affected, and a public communication or similar measure by which affected data subjects

are informed of the breach, would be an effective method of notification of the breach to the affected data subjects.

50. Automated data processing.

(1) Subject to this section, no data subject shall be subject to a decision based solely on automated data processing or profiling, which produces legal effects concerning the data subject or similarly affects the data subject.

(2) Subsection (1) does not apply where the decision is —

(a) necessary for entering into, or performing a contract between the data subject and a data controller;

(b) authorized by a written law to which the data controller is subject, and which also specifies suitable measures to safeguard the fundamental rights and freedoms of the data subject; or

(c) based on the consent of data subject for automated data processing or profiling.

(3) In cases referred to in subsection (2)(a) and (c), the data controller shall implement suitable measures to safeguard a data subject's fundamental rights and freedoms.

(4) Subsection (2) shall not apply to sensitive personal data of the data subject unless —

(a) the use of automated data processing or profiling is in the public interest; and

(b) suitable measures to safeguard the data subject's fundamental rights and freedoms, are implemented and enforced.

51. Data protection impact assessment.

(1) The Minister may, on the recommendation of the Commissioner, make regulations prescribing the classes or categories of data controllers and data processors that are required to conduct data protection impact assessments, and setting out the form, content, and procedures for data protection impact assessment assessments, having regard to the nature, scope, and risks of the processing.

(2) Until regulations are made under this section, the Commissioner may direct that a data protection impact assessment be conducted in relation to any processing operation that, in the opinion of the Commissioner, is likely to result in a high risk to the fundamental rights and freedoms, or legitimate interests of data subjects.

52. Data processing by data processors.

(1) Where processing is to be carried out by a data processor, the data controller shall —

(a) only use data processors that provide sufficient guarantees to implement technical and organizational measures referred to in this section; and

(b) enter into a written contract with the data processor in a manner that provides for —

(i) the subject matter and duration of the processing;

(ii) the nature and purpose of the processing;

(iii) the type of personal data and categories of data subjects;

(iv) the obligations and rights of the data controller.

(2) The contract prepared under subsection (1)(b) shall also stipulate that the data processor shall —

(a) process the personal data only on written instructions from the data controller, including with regard to transfers of personal data to countries outside of The Bahamas or an international organization, unless required to do so by a written law and in either of these cases, the data processor shall inform the data controller of that legal requirement before processing, unless the written law prohibits information to be shared on important grounds of public interest;

(b) ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) take the technical and organizational measures required under section 53;

(d) comply with the provisions of subsections (3) and (5) for engaging another data processor;

(e) take into account the nature of the processing, assist the data controller by technical and organizational measures, so far as possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights under Part IV;

(f) assist the data controller in ensuring compliance with the obligations under sections 48, 49, 51 and 53;

(g) on the determination of the data controller, delete or return all the personal data to the data controller after the end of the provision of services relating to processing, and delete existing copies unless an enactment requires the storage of the personal data; and

(h) make available to the data controller all information necessary to demonstrate compliance with the obligations set out in this section and allow for and contribute to audits, and inspections, conducted by the data controller or another auditor mandated by the data controller.

(3) The data processor shall not engage another data processor without prior specific or general written authorization of the data controller.

(4) Where there is a general written authorization under subsection (3), the data processor shall inform the data controller of any intended changes concerning the addition or replacement of other data processors and the data controller shall be given the opportunity to object to the intended changes.

(5) Where a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller in accordance with subsection (3) —

(a) the same obligations set out in the contract between the data controller and the data processor referred to in subsection (2) shall be imposed on that other data processor, in particular providing sufficient guarantees to implement technical and organizational measures in a manner that the processing shall meet the requirements of this Act; and

(b) the initial data processor shall, where the other data processor fails to fulfil its data protection obligations, remain fully liable to the data controller for the performance of the other data processor's obligations.

(6) The Commissioner shall publish on the official website of the Office of the Data Protection Commission standard contractual clauses for the matters referred to in subsections (2) and (5)(a).

(7) The data processor and a person acting under the authority of the data controller or the data processor who has access to personal data shall not process the personal data except on instructions from the data controller, unless required to do so by a written law.

(8) A person who contravenes subsection (7) commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or to a term of imprisonment of six months, or to both.

53. Security of processing.

(1) Every data controller and data processor shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

(2) Every data controller shall, having regard to the nature, scope and purpose of processing, and the likelihood and severity of the harm that may result from such processing, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and the relative cost of implementing technical and organizational measures, including —

(a) maintaining the integrity of personal data using methods of pseudonymization and encryption;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

(3) Every data controller shall inform data subjects of the technical and organizational measures utilised to protect the personal data associated with the processing of that data subject's data and ensure strict adherence to the technical and organizational measures.

(4) Every data controller shall, in accordance with guidelines issued by the Commissioner undertake periodic review of technical and organizational measures implemented under subsection (2).

(5) Every data controller and data processor shall periodically review the technical and organizational measures implemented under this section, in accordance with any guidelines issued by the Commissioner.

(6) The Minister may, on the recommendation of the Commissioner, make regulations prescribing exemptions or modifications from the application of this section for specified categories of data controllers or data processors, having regard to the nature and scale of the processing activities of the data controllers or data processors and the risk to data subjects.

PART VI – TRANSFER OF PERSONAL DATA OUTSIDE THE BAHAMAS

54. General principle for transfer outside The Bahamas.

(1) Personal data shall not be transferred to a country, territory or international organization unless that country, territory or international organization ensures an adequate level of protection for the fundamental

rights and freedoms of data subjects in relation to the processing of personal data.

(2) A person who transfers data to a country or territory outside of The Bahamas in contravention of this section, commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years, or to both.

(3) In this section —

"adequate level of protection" means protection that is adequate in all the circumstances of the case, having regard in particular to —

(a) the nature of the personal data;

(b) the country, territory or international organization from which the information contained in the personal data originated;

(c) the country, territory or international organization of final destination of information contained in the personal data;

(d) the purposes for which and period during which the personal data are intended to be processed;

(e) the applicable laws in the country, territory or international organization in question;

(f) the international obligations of that country, territory or international organization;

(g) any relevant codes of conduct or other rules that are enforceable in that country, territory or international organization, whether generally or by arrangement in particular cases; and

(h) any security measures taken in respect of the personal data in that country, territory or international organization.

55. Conditions for transfer outside of The Bahamas.

Personal data may be transferred outside of The Bahamas where —

(a) the data subject consents to the transfer;

(b) the transfer is necessary —

(i) for the performance of a contract between the data subject and the data controller or implementation of pre-contractual measures taken at the request of the data subject;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another person;

(iii) for a matter of public interest as specified by the Minister by order;

(iv) for the establishment, exercise or defence of a legal claim;

(v) where the data subject is physically or legally incapable of giving consent, in order to protect the fundamental rights and freedoms of the data subject or of other persons; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller which are not overridden by the legitimate interests, fundamental rights and freedoms of the data subjects;

(c) the transfer of personal data is part of the personal data on the public register and any conditions subject to which the public register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer.

56. Requirement of data controller to review.

(1) Within one year after the commencement of this Act, every data controller shall review any existing arrangements for —

(a) the storage or processing of personal data by third parties, whether within or outside The Bahamas; and

(b) the contracts or other mechanisms governing the cross-border transfer or storage of personal data,

to ensure compliance with the requirements for the transfer of personal data under this Part.

(2) The extent and manner of the review required under subsection (1) shall be proportionate to the nature, scope, and volume of the personal data processed, and the risks posed to the fundamental rights and freedoms of data subjects.

(3) The Minister may, on the recommendation of the Commissioner, make regulations providing for exemptions for certain categories of data controllers or data processors from —

(a) the principles for transfer of personal data outside The Bahamas under section 54;

(b) the conditions for transfer of personal data outside The Bahamas under section 55; and

(c) the annual review of arrangements by the data controller under section 56.

PART VII – EXEMPTIONS TO DATA PROTECTION STANDARDS OR TO DISCLOSURE OF DATA SUBJECT REQUIREMENTS

57. National security.

Parts II, IV, V and VI and section 77, do not apply where the processing of the personal data is required for the purpose of safeguarding national security.

58. Law enforcement and taxation.

(1) Personal data processed for —

(a) the prevention, detection, or investigation of crime;

(b) the apprehension or prosecution of offenders; or

(c) the assessment or collection of a tax or duty or of an imposition of a similar nature,

is exempt from section 5(1)(a), except to the extent to which it requires compliance with the conditions in sections 6, 7, 8, 24 and 35 to the extent to which the application of those provisions to the personal data is likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Personal data is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in subsection (1) if it —

(a) is processed for the purpose of discharging statutory functions; and

(b) consist of information obtained from a person who had the information in his possession for the purposes mentioned in subsection (1).

(3) Personal data is exempt from the non-disclosure provisions where —

(a) the disclosure is for any of the purposes mentioned in subsection (1); and

(b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned in subsection (1).

(4) Personal data is exempt from section 24 to the extent to which the exemption is required in the interests of the operation of a system described in paragraph (a), if the data controller of the personal data is a public authority and the personal data —

(a) consist of a classification applied to the data subject as a part of a system of risk assessment which is operated by the public body for —

(i) the assessment or collection of tax, duty or other imposition of a similar nature; or

(ii) the prevention or detection of crime or the apprehension or prosecution of offenders, where the offence concerned involves an unlawful claim for payment out, or an unlawful application of, public funds; and

(b) is processed for either purpose in paragraph (a)(i) or (ii).

59. Regulatory activities.

(1) Personal data processed by a regulatory body or other person for the purposes of discharging any function under this Act or power under a written law are exempt from disclosure of the data subject requirements to the subject information provisions to the extent to which the application of those provisions in any case is likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to function which is —

(a) conferred on a person by or under a written law;

(b) public in nature, and exercised in the public interest and is connected with —

(i) public safety;

(ii) breaches of codes of ethics for a regulated profession; or

(iii) important national economic or financial interests monetary, budgetary or taxation matters;

(c) designed for protecting members of the public against —

(i) maladministration by public bodies;

(ii) the failure of a public body to provide a service for which it is a function of that public body to provide; or

(iii) conduct by persons carrying on trade or business, which may adversely affect the public interest;

(d) designed for regulating —

(i) agreement or conduct which has as its object or effect, the prevention, restriction or distortion of competition, in connection with commercial activity; or

(ii) conduct, on the part of one or more undertakings, which amounts to the abuse of a dominant market position.

(3) In subsection (2)(b)(ii), **"regulated profession"** means a profession subject to regulation by a body established in a written law.

60. Processing of personal data for journalism, artistic or literary purposes.

(1) Personal data which is processed only for the purposes of journalism or for artistic or literary purposes is exempt from a provision to which this subsection relates where —

(a) the processing of personal data is undertaken with a view to the publication of the personal data by a person for journalism, artistic or literary purposes;

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, the publication would be in the public interest; and

(c) the data controller reasonably believes that, in all the circumstances, compliance with the publication of personal data in the public interest would be incompatible with the journalism, artistic or literary purposes.

(2) For the purposes of considering whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to a data controller's compliance with a Code of Practice for the processing of personal data for journalism, artistic or literary purposes and issued by the Commissioner.

(3) In roceedings against a data controller where the data controller claims or it appears that personal data to which the proceedings relate are being processed —

(a) only for journalism, artistic or literary purposes; and

(b) with a view to the publication by a person of a journalistic, artistic or literary material which, at the time twenty-four hours immediately before the relevant time, had not previously been published by the data controller,

the proceedings shall be stayed until either of the conditions in subsection (4) is met.

(4) The conditions referred to in subsection (3) are —

(a) that a determination of the Commissioner with respect to the data in question takes effect; or

(b) in a case where the proceedings were stayed, on the making of a claim, that the claim is withdrawn.

(5) For the purposes of this section, **"publication"** means to make available to the public.

61. Processing of personal data for research purposes.

(1) The processing of personal data only for research purposes in compliance with the relevant conditions, shall not to be regarded as incompatible with the purposes for which it was obtained.

(2) Personal data that is processed only for research purposes is exempt from section 24 if —

(a) the personal data is processed in compliance with the relevant conditions; and

(b) the results of the research or resulting statistics are not made available in a form which identifies the data subjects.

(3) Personal data that is processed only for research purposes may be kept indefinitely if the relevant conditions are met.

(4) For the purposes of subsections (1) to (3), personal data is not to be treated as processed otherwise than for research purposes only because the personal data is disclosed —

(a) to a person, for research purposes only;

(b) to the data subject or a person acting on his behalf;

(c) at the request, or with the consent, of the data subject or a person acting on his behalf;

(d) in circumstances in which the person making the disclosure, has reasonable grounds for believing that the disclosure falls within paragraphs (a), (b) or (c).

(5) In this section —

"research purposes" include historical research purposes, scientific research purposes and statistical purposes;

"the relevant conditions", in relation to processing of personal data, means the conditions that the personal data —

(a) is not processed to support measures or decisions with respect to particular identifiable natural persons; and

(b) is not processed in a way that substantial damage or substantial distress is, or is likely to be, caused to a data subject.

62. Information available to public by law.

(1) Personal data is exempt from Parts II, IV, V and VI where the personal data consist of information which the data controller is obliged by a written law to make available to the public, whether by publishing it, by making it available for inspection, or otherwise.

(2) Personal data may be available to the public for inspection on the payment of a prescribed fee.

63. Disclosures required by law or made for the purpose of legal proceedings.

(1) Personal data is exempt from the non-disclosure provisions where the disclosure is required or authorized under a written law, under any rule of law, or by an order of a court of competent jurisdiction.

(2) Personal data is exempt from the non-disclosure provisions where the disclosure is necessary —

(a) for the purpose of legal proceedings; or

(b) for the purpose of obtaining legal advice,

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

64. Parliamentary privilege.

Personal data is exempt from Parts II, IV, V and VI, where the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

65. Legal professional privilege.

Personal data is exempt from the subject information provisions where the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

66. Personal data processed for personal, family or household affairs and recreational purposes.

Personal data processed for by an identifiable natural person for the purposes of the personal, family or household affairs, and recreational purposes of the identifiable natural person is exempt from Parts II, IV, V and VI.

67. Confidential references given by a data controller.

Personal data is exempt from section 24 if the data consist of a reference given or to be given in confidence by the data controller for the purposes of —

(a) the education, training or employment, or prospective education, training or employment of the data subject;

(b) the appointment, or prospective appointment, of the data subject to an office; or

(c) the provision, or prospective provision, by the data subject of a service.

68. Judicial appointments and honours.

Personal data processed for the purposes of —

(a) assessing a person's suitability for —

(i) judicial office; or

(ii) the office of King's Counsel; or

(b) the conferring of an honour or award under the National Honours Act (*Ch. 391A*),

is exempt from the subject information provisions.

69. Armed forces.

Personal data is exempt from the subject information provisions to the extent to which the application of those requirements would be likely to prejudice the combat effectiveness of the armed forces of the Crown.

70. Correctional services.

Personal data consisting of a report on an inmate of a correctional facility are exempt from section 24 if the disclosure could reasonably be expected to reveal information supplied in confidence.

71. Appointments to the public service.

The Minister may by order, exempt from the subject information provisions personal data processed for the purposes of assessing a person's suitability for —

(a) employment to an office of emolument in the public service as defined by *Article 137* of the Constitution; or

(b) any office to which appointments are made by the Governor-General or by a Minister.

72. Negotiations with the data subject.

Personal data which consists of records of the intentions of the data controller in relation to any negotiations with the data subject is exempt from the subject information provisions where the application of those provisions would be likely to prejudice those negotiations.

73. Examinations.

(1) The results of an examination are exempt from section 24.

(2) Personal data consisting of information recorded by candidates during an academic or professional examination or other examination is exempt from section 24.

(3) In this section, **"examination"** includes a process for determining the knowledge, intelligence, skill or ability of a candidate by reference to his performance in a test, work or other activity.

PART VIII – ENFORCEMENT

74. Enforcement notice.

(1) Where the Commissioner is satisfied that a data controller has contravened this Act, the Commissioner may serve the data controller with a notice in writing (an **"enforcement notice"**), which requires the data controller to —

(a) take, within the time specified in the notice, or refrain from taking, after the time specified in the notice, those steps that are specified in the notice; or

(b) refrain from processing personal data or personal data of a description specified in the notice, or to refrain from processing the personal data for a purpose or in the manner specified, within a time period specified in the notice.

(2) The Commissioner shall, when deciding to serve an enforcement notice, consider whether the contravention has caused or is likely to cause a person damage or distress.

(3) An enforcement notice shall contain —

(a) a statement of the section of the Act that to the satisfaction of the Commissioner has been or is being contravened and the Commissioner's reasons for arriving at that conclusion; and

(b) particulars of the right of appeal conferred by section 88.

(4) Subject to subsections (5) and (6), no enforcement notice shall require the provisions of the enforcement notice to be complied with before the end of the period within which an appeal can be brought against the enforcement notice and, where an appeal is brought, the person upon whom the enforcement notice is served is not required to comply with the enforcement notice pending the determination or withdrawal of the appeal.

(5) Where, by reason of special circumstances, the Commissioner considers that an enforcement notice should be complied with as a matter of urgency, he may include in the enforcement notice a statement to that effect together with his reasons for the urgency.

(6) Notwithstanding subsection (5), no enforcement notice shall require the provisions of the enforcement notice to be complied with before the end

of the period of seven days, beginning with the day on which the enforcement notice is served.

75. Cancellation of enforcement notice.

(1) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that enforcement notice, apply in writing to the Commissioner for the cancellation or variation of the enforcement notice on the ground that, by reason of a change of circumstances, all or any of the provisions of the enforcement notice need not be complied with in order to ensure compliance with the provisions of this Act to which the enforcement notice relates.

(2) The Commissioner may cancel or vary an enforcement notice if the Commissioner considers that all or any of the provisions of the enforcement notice need not be complied with in order to ensure compliance with this Act.

76. Request for assessment.

(1) A person who is, or believes himself to be, directly affected by the processing of personal data may, in writing, request an assessment to be undertaken by the Commissioner as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with this Act.

(2) Under subsection (3), the Commissioner shall, on receiving a request, make an assessment in a manner as appears to him to be appropriate, unless the Commissioner is not supplied with the information necessary to —

(a) satisfy himself as to the identity of the person making the request; and

(b) enable him to identify the processing in question.

(3) The matters to which the Commissioner may have regard in determining in what manner it is appropriate to make an assessment include —

(a) the extent to which the request appears to the Commissioner to raise a matter of substance;

(b) an undue delay in making the request; and

(c) whether or not the identifiable natural person making the request has the right to access the personal data in question as specified in section 24.

(4) Where the Commissioner has received a request under this section, he shall notify the person who made the request of —

(a) whether he has made an assessment as a result of the request; and

(b) any view formed or action taken as a result of the request, having regard in particular to an exemption from section 24 applying in relation to the personal data concerned.

77. Information notice.

(1) The Commissioner may serve a data controller or data processor with an information notice that requires that person to provide the Commissioner with the specified information relating to the request or to comply with the provisions of this Act where the Commissioner —

(a) has received a request for an assessment under section 76; or

(b) reasonably requires any information for the purpose of determining whether a data controller or data processor has complied with or is complying with the data protection principles in Part II.

(2) An information notice shall contain —

(a) in the instance of subsection (1)(a), a statement that the Commissioner has received a request under section 76 in relation to the specified processing;

(b) in the instance of subsection (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller or the data processor has complied or is complying with the provisions of this Act and his reasons for regarding it as relevant for that purpose; and

(c) particulars of the right of appeal conferred by section 88.

(3) The Commissioner may specify in an information notice —

(a) the form in which the information must be provided; and

(b) the period within which, or the time and place at which the information must be provided.

(4) Subject to subsection (5), a period or time specified in an information notice under subsection (3)(b) must not end or fall before the conclusion of the period within which an appeal can be brought against the information notice and, where an appeal is brought, no information shall be provided pending the determination or withdrawal of the appeal.

(5) Where, by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency —

(a) the Commissioner may include in the information notice a statement to that effect and a statement of his reasons for the urgency;

(b) subsection (4) shall not apply; and

(c) the information notice shall not require the information to be provided before the end of the period of seven days beginning with the day on which the information notice is served.

(6) This section does not require a person to provide the Commissioner with information —

(a) where the information would, by revealing evidence of the commission of an offence, other than an offence under this Act or an offence of perjury, expose that person to the proceedings for that offence;

(b) in respect of a communication between —

(i) a counsel and attorney and his client in connection with the giving of legal advice to the client concerning his obligations, liabilities, or rights under this Act; or

(ii) a counsel and attorney and his client, or between the counsel and attorney or his client and other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before the Tribunal, and for the purposes of the proceedings.

(7) A relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for an offence under this Act except an offence under section 80, unless in the proceedings —

(a) in giving evidence, the person provides information that is inconsistent with it; and

(b) evidence related to it is adduced or a question is asked relating to it, by that person or on that person's behalf.

(8) In this section —

"specified information" means information —

(a) described in the information notice;

(b) falling within a category that is specified or described in the information notice; or

(c) about the processing of personal data and the documentation of personal data, as well as information relating to the security and confidentiality of the processing and documentation;

"relevant statement" means an oral statement or a written statement.

78. Commissioner to determine processing for journalism, artistic or literary purposes.

(1) The Commissioner may make a determination in writing where it appears to him, whether as a result of the service of an information notice or otherwise, that any personal data is not being processed —

(a) only for the purposes of journalism, artistic or literary purposes; or

(b) with a view to the publication by any person of a journalistic, artistic or literary material which has not previously been published by the data controller.

(2) The Commissioner shall give notice of his determination made under subsection (1) to the data controller.

(3) A determination under this section shall not take effect —

(a) until the end of the period within which an appeal can be brought; or

(b) pending the determination or withdrawal of an appeal.

79. Restriction on enforcement in processing for journalism, artistic or literary purposes.

(1) The Commissioner shall not serve an enforcement notice on a data controller with respect to the processing of personal data for journalism, artistic or literary purposes unless —

(a) a determination under section 78 with respect to personal data has taken effect; and

(b) the court has granted leave for the notice to be served.

(2) The court shall not grant leave for the purposes of subsection (1)(b) unless it is satisfied that —

(a) the Commissioner has reason to suspect a contravention of the data protection principles that substantially affect the public; and

(b) except for in urgent circumstances, the data controller has been given notice of the application for leave in accordance with the Supreme Court Civil Procedure Rules, 2022 (*S. I. No. 76 of 2022*).

(3) The Commissioner shall not serve an information notice on a data controller with respect to the processing of personal data for journalism, artistic or literary purposes unless a determination under section 78 with respect to the personal data has taken effect.

80. Failure to comply with notice.

(1) A person commits an offence where he fails to comply with an —

(a) enforcement notice;

(b) information notice; or

(c) request for assessment.

(2) A person commits an offence if, in purported compliance with an information notice or request for assessment, he —

(a) makes a statement which he knows to be false in a material respect; or

(b) recklessly makes a statement which is false in a material respect.

(3) It is a defence for a person charged with an offence under subsection (1) to prove that he exercised all due diligence to comply with the notice in question.

(4) A person who commits an offence under subsections (1) or (2) is liable upon summary conviction to a fine of fifty thousand dollars or to a term of imprisonment of three years, or to both.

81. Issue of warrants.

(1) A Justice of the Supreme Court may issue a warrant if he is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting that —

(a) a data controller has contravened or is contravening Part II, sections 24 to 32, or Part VI of this Act; or

(b) an offence under this Act has been or is being committed, and that evidence of the contravention or of the commission of the offence is to be found on a premises specified by the Commissioner.

(2) A warrant issued under subsection (1) shall authorize a police officer accompanied by the Commissioner, his staff, or another person skilled in information and communications technology as the police officer may deem necessary to —

(a) enter the premises;

(b) search the premises;

(c) inspect, examine, operate, and test an equipment found on the premises which is used or intended to be used for the processing of personal data;

(d) inspect and seize any documents or other material found on the premises;

(e) require a person on the premises to provide —

(i) an explanation of a document or other material found on the premises;

(ii) other information as may reasonably be required for the purpose of determining whether the data controller has contravened Part II, sections 24 to 32, Part VI of this Act.

(3) A Justice of the Supreme Court shall not issue a warrant in respect of personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination has been made by the Commissioner, in accordance with section 78.

82. Execution of warrants.

(1) Where a person who occupies the premises in respect of which a warrant is issued is present when the warrant is executed, that person shall be shown the warrant and provided with a copy of it, and in the absence of that person a copy of the warrant shall be left on a prominent place on the premises.

(2) A police officer who executes a warrant in accordance with this section shall make a list of any items seized, including the date and time of the seizure and shall give the list to —

(a) the data controller; or

(b) the occupier of the premises.

83. Matters exempt from inspection and seizure.

The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of —

(a) personal data, which by virtue of section 57, is exempt from the provisions of this Act;

(b) any communication between —

(i) a counsel and attorney and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities, or rights under this Act; or

(ii) a counsel and attorney and his client, or between the counsel and attorney or his client and another person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before the Tribunal and for the purposes of those proceedings.

84. Return of warrants.

(1) A warrant issued under this Act shall be returned to the Supreme Court —

(a) upon the execution of the warrant; or

(b) if the time authorized for the execution of the warrant has passed.

(2) The police officer that executes a warrant shall make an endorsement on it stating the powers exercised under the warrant.

85. Forfeiture.

(1) Subject to subsection (2), the Supreme Court may order that a document or other material be forfeited where it is used in connection with the processing of personal data and appears to the Supreme Court to be connected with the commission of an offence under this Act.

(2) The Supreme Court shall not make an order under subsection (2) in relation to material where a person, other than the offender —

(a) claims to be the owner of the material or otherwise has an interest in the material; and

(b) applies to the Supreme Court to be heard and upon being given an opportunity to be heard, shows cause as to why the order should not be made.

(3) Where the Supreme Court makes an order for the forfeiture of a document or other material in accordance with this section, the Supreme Court may also order the document or material to be destroyed or erased.

86. Offences.

(1) A person commits an offence if he —

(a) intentionally obstructs a person in the execution of a warrant issued under this Act;

(b) fails without reasonable excuse to give a police officer executing a warrant issued under this Act the assistance as he may reasonably require for the execution of the warrant;

(c) makes a statement in response to a requirement under section 80(2)(e) which that person knows to be false in a material respect; or

(d) recklessly makes a statement which is false in a material respect as it relates to a requirement under section 81(2)(e).

(2) A person who commits an offence under this section is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years or to both.

PART IX – DATA PROTECTION APPEAL TRIBUNAL

87. Establishment of Data Protection Appeal Tribunal.

(1) There is established a tribunal to be known as the Data Protection Appeal Tribunal.

(2) The provisions of the *First Schedule* shall have effect, in respect of the constitution and functions of the Tribunal.

88. Right of appeal.

(1) A person on whom an enforcement notice or an information notice has been served may appeal to the Tribunal against the enforcement notice or information notice.

(2) A person on whom an enforcement notice has been served may appeal to the Tribunal against the refusal of an application by the Commissioner under section 75(1) for cancellation or variation of the enforcement notice.

(3) Where an enforcement notice or an information notice contains a statement by the Commissioner in accordance with sections 74(3) or 77(2) then, whether or not the person appeals against the enforcement notice or information notice, he may appeal against —

(a) the Commissioner's decision to include the statement in the enforcement notice or information notice; or

(b) the effect of the inclusion of the statement in respect of any part of the enforcement notice or information notice.

(4) A data controller in respect of whom a determination has been made under section 78 may appeal to the Tribunal against the determination.

(5) A person to whom a penalty notice has been issued under section 90, may appeal to the Tribunal against the penalty notice.

89. Determination of appeals.

(1) Upon hearing an appeal, the Tribunal may —

(a) dismiss the appeal; or

(b) allow the appeal in whole or in part, and direct the appropriate person or body to take an action or make a decision which could have been taken or made by that person or body regarding the matter in respect of which the appeal is allowed.

(2) A party to an appeal to the Tribunal under section 87 may appeal the decision of the Tribunal on a point of law to the Supreme Court.

90. Penalty notices.

(1) Where the Commissioner is satisfied that a person has failed or is failing to comply with sections 42(2), 43(2), 44, 46, 48, 49, 51, or 53, the Commissioner, may issue a penalty notice where he considers it to be in the public interest, requiring the person to pay to the Office of the Data

Protection Commissioner, an amount not exceeding ten thousand dollars as specified in the penalty notice.

(2) Where the Commissioner issues a penalty notice under subsection (1), the Commissioner shall, have, in addition to the public interst, due regard to —

(a) the nature, gravity and duration of the contravention taking into account —

(i) the nature, scope or purpose of the processing concerned;

(ii) the number of data subjects affected; and

(iii) the level of damage suffered by those a data subjects;

(b) the intentional or negligent character of the contravention;

(c) any action taken by the data controller to mitigate the damage suffered by a data subject;

(d) any relevant previous contraventions by the data controller or data processor;

(e) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the contravention;

(f) the categories of personal data affected by the contravention;

(g) the manner in which the contravention became known to the Commissioner and, in particular whether, and to what extent, the data controller gave notice of the contravention to the Commissioner; and

(h) any other aggravating or mitigating factor applicable to the circumstances of the case, namely, the financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

(3) Where the Commissioner issues a penalty notice under subsection (1), the Commissioner shall file in the registry of the Supreme Court, a copy of the penalty notice certified by the Commissioner.

(4) A penalty notice issued under subsection (1), shall have the same force and effect as if the penalty notice was a judgment of the Supreme Court.

(5) A penalty imposed by the Commissioner in the exercise of his powers under this Act shall be payable into the Consolidated Fund and may be recovered by the Crown as a civil debt and for the purposes of the proof of a civil debt, a certificate certified by the Commissioner, shall be admissible in evidence as sufficient proof of the debt.

(6) A person aggrieved by a penalty notice issued by the Commissioner under subsection (1) may appeal to the Tribunal within twenty-eight days of the date of the order.

PART X – DATA PROTECTION OVERSIGHT COMMITTEE

91. Establishment of Data Protection Oversight Committee.

(1) There is established a Data Protection Oversight Committee (**"the "Committee"**).

(2) The objective of the Committee is to hold the Commissioner accountable to the public in the performance of the Commissioner's functions under this Act.

(3) The *Second Schedule* has effect with respect to the constitution of the Committee.

92. Functions of the Committee.

The functions of the Committee are to —

(a) monitor and review the performance of the functions of the Commissioner;

(b) report to both Houses of Parliament on any matter relating to the performance of the functions of the Commissioner;

(c) review the annual report required to be prepared under section 21 and make the recommendations to the annual report before the annual report is laid before Parliament; and

(d) perform other functions as may be necessary for promoting the objective of the Committee under section 91(2).

93. Powers of the Committee.

(1) The Committee shall have the power as may be requisite or incidental for or in connection with the performance of its functions.

(2) Without prejudice to the generality of subsection (1), the Committee —

(a) may investigate any aspect of the operations of the Commissioner, or the conduct of the Commissioner in relation to the functions of the Commissioner;

(b) may investigate the conduct of staff of the Office of the Data Protection Commissioner;

(c) shall take copies of document in relation to any matter under investigation by the Committee;

(d) may require the Commissioner to supply information or provide documents in respect of any matter relating to the operations of the Office of the Data Protection Commissioner in relation to the functions of the Commissioner under the Act; and

(e) may require the Commissioner to supply information or provide documents in respect of the conduct of any employee, of the Office of the Data Protection Commissioner.

(3) The Committee shall not be liable to any action, suit or proceedings or for any matter or thing done in the due execution or carrying out of the investigation under paragraph (a).

(4) A person appearing or summoned by the Committee shall be entitled to the same immunities and privileges as are parties, witnesses and representatives in civil proceedings before the Supreme Court.

PART XI – GENERAL

94. Prosecutions.

Proceedings for an offence under this Act, shall not be instituted except by —

(a) the Director of Public Prosecutions; or

(b) the Commissioner, with consent of the Director of Public Prosecutions.

95. Offences by officers of a body corporate.

(1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of a person, being a director, manager, secretary or other officer of the body corporate, or a person who was purporting to act in the capacity as a director, manager, secretary or other officer of the body corporate, that person and the body corporate is guilty of an offence and is liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director or manager of the body corporate.

96. Unlawful access, use, or disclosure of personal data.

(1) A person shall not knowingly or recklessly, without the consent of the data controller —

(a) obtain or disclose personal data or the information contained in personal data; or

(b) procure the disclosure to another person of the information contained in personal data.

(2) Subsection (1) does not apply to a person who demonstrates that —

(a) the personal data obtained, disclosed or procured was —

(i) necessary for the purpose of preventing or detecting crime; or

(ii) required or authorized by or under any written law, any rule of law or by the order of a court of competent jurisdiction;

(b) he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or to procure the disclosure of the information to the other person;

(c) he acted in the reasonable belief that he would have had the consent of the data controller, if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; or

(d) in the particular circumstances, the obtaining disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars or to a term of imprisonment not exceeding three years, or to both.

(4) A person who sells, rents or offers to sell personal data, commits an offence if he obtained the personal data in contravention of subsection (1) and is liable on summary conviction to a fine not exceeding one hundred thousand dollars or a term of imprisonment not exceeding five years, or to both.

(5) For the purposes of subsection (4) an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

97. Regulations.

(1) The Minister may, upon the recommendation of the Commissioner, make regulations —

(a) for the purpose of giving effect to the provisions of this Act;

(b) specifying additional conditions for the purposes of the *First* or *Second Schedule*.

(2) Regulations made under this section may —

(a) provide for the forms of exempting small-sized or medium-sized businesses from complying with the requirements section 7(5);

(b) provide for the creation and maintenance of a public register under section 15(v);

(c) provide for the form of the request in writing and the fee under section 24(4);

(d) provide for the time period and the fee under section 24(6);

(e) provide for the cases exempted under section 30(2)(b);

(f) provide the form, format and technical standards for the exercise of the right by the data subject, to receive and transfer personal data under section 31(1);

(g) provide the form of consent under section 37(2);

(h) provide for the forms of exemptions or modifications from the application of any provision of this Act, in relation to specified categories of data controllers or data processors, having regard to—

(i) the size and nature of the organization;

(ii) the volume and sensitivity of personal data processed;

(iii) the nature, scope, context, and purposes of the processing; and

(iv) the risk of harm to the fundamental rights and freedoms of data subjects;

(i) provide for the form of objection under section 37(3)(c);

(j) provide for the registration form and the fee under section 39(1);

(k) provide for the form for the renewal of the registration certificate and the fee under section 41(1);

(l) to provide the the fee to be paid to inspect the Register of Data Controllers under section 42(3);

(m) to provide the fee to be paid to inspect the Register of Data Processors under section 43(3);

(n) provide the extended time period in which the Commissioner is notified of the breach of personal data under section 48(5);

(o) provide the classes or categories of data controllers and data processors required to conduct data protection impact assessment under section 51;

(p) providing for exemptions for certain categories of data controllers or data processors from —

(i) the principles for transfer of personal data outside The Bahamas under section 54;

(ii) the conditions for transfer of personal data outside The Bahamas under section 55; and

(iii) the annual review of arrangements by the data controller under section 56.

(q) provide for the fee to be paid for the inspection of the personal data made available to the public under section 62;

(r) provide for the form of the penalty notice issued under section 90(1);

(s) provide for the electronic creation of a sandbox, similar to that which is electronically operational in the United Kingdom;

(t) provide additional safeguards in relation to sensitive personal data;

(u) prescribe retention periods for personal data to be observed by data controllers and data processors;

(v) prescribe the fees which may be imposed under this Act;

(w) prescribe the methods by which personal data may be disposed;

(x) provide for the establishment and maintenance of a public register for processing operations and the manner of notifications to the Commissioner;

(y) provide for the third-party data storage and cross-border data storage contract of a data controller.

98. Transitional.

(1) On the date that this Act comes into operation —

(a) all real and personal property and every right and interest in the property that, immediately before that date, was vested in the Data Protection Commissioner under the repealed Act, shall vest in the Office of the Data Protection Commissioner without conveyance or assignment and shall be used for a like purpose;

(b) all rights accruing or accrued to the Data Protection Commissioner under the repealed Act in respect of property vested in the Office of Data Protection Commissioner by virtue of this section are vested in the Office of the Data Protection Commissioner and may be enforced against the Office of the Data Protection Commissioner;

(c) all liabilities of the Data Protection Commissioner under the repealed Act shall vest in the Office of the Data Protection Commissioner without further assurance and the Office of Data Protection Commissioner shall have all powers necessary to satisfy those liabilities;

(d) all contracts, agreements, leases and undertakings made, and all securities lawfully given to or by the Data Protection Commissioner under the repealed Act which, before the date on which this Act comes into operation, are in force shall have effect as contracts, agreements, leases and undertakings by and with the Office of the Data Protection Commissioner, established under this Act and may be enforced by the Office of the Data Protection Commissioner accordingly;

(e) all debts due and moneys payable to the Data Protection Commissioner and all claims liquidated or unliquidated, or recoverable against the Data Protection Commissioner under the

repealed Act shall be debts due and moneys payable by and claims recoverable against the Office of Data Protection Commissioner accordingly;

(f) all actions, proceedings and causes of action to which the Data Protection Commissioner was a party under the repealed Act shall be continued as if the Office of Data Protection Commissioner was a party to those proceedings.

99. Savings.

(1) The person who, immediately before the coming into operation of this Act, was appointed Data Protection Commissioner under the repealed Act shall continue under the title of Data Protection Commissioner under this Act as if he had been appointed under this Act on the same terms and conditions for a term expiring on the day on which the appointment under the repealed Act would expire.

(2) An officer or employee appointed or employed by the Data Protection Commissioner under the repealed Act shall continue in office or employment with the Office of Data Protection Commissioner under this Act, on the same terms and conditions as existed before the coming into operation of this Act.

(3) Any provision of the repealed Act that is necessary to ensure the continued validity, enforcement, or completion of any registration, consent, authorization, investigation, or legal proceeding commenced under that Act, shall continue in operation until the corresponding provisions of this Act come into operation.

100. Act binds Crown.

This Act binds the Crown.

101. Repeal of *No. 3 of 2003*.

The Data Protection (Privacy of Personal Information) Act (*Ch. 324A*), is repealed.

FIRST SCHEDULE

(section 87(2))

DATA PROTECTION APPEAL TRIBUNAL

1. Composition of Tribunal.

(1) The Tribunal shall consist of five members appointed by the Governor-General upon the recommendation of the Prime Minister after consultation with the Leader of the Opposition.

(2) The membership of the Tribunal described in subparagraph (1) includes the Chairperson appointed in accordance with paragraph 2.

(3) With the exception of the Chairperson, the members of the Tribunal shall be persons having expertise in the field of data protection or privacy rights in order to be eligible for appointment.

(4) No member of the Tribunal shall be the holder of a public office within the meaning of *Article 137* of the Constitution of The Bahamas.

(5) The members of the Tribunal shall, subject to the provisions of this Schedule, hold office for a period of three years and shall be eligible for reappointment for one further period of three years.

(6) If a vacancy occurs in the membership of the Tribunal that vacancy shall be filled by the appointment of another member.

2. Appointment of Chairperson.

The Governor-General shall appoint a retired Justice of the Supreme Court or Court of Appeal to be the Chairperson of the Tribunal.

3. Acting appointments.

The Governor-General may appoint —

(a) in the case of the absence or inability to act of the Chairperson, another retired Justice of the Supreme Court or Court of Appeal to act in the place of the Chairperson; or

(b) in the case of the absence or inability to act of another member of the Tribunal, a person who possesses the qualifications described in subparagraph (3) of paragraph 1, to act in the place of that member.

4. Resignation.

(1) A member of the Tribunal, other than the Chairperson, may at any time resign the office by instrument in writing addressed to the Governor-General and delivered through the Chairperson, and that member shall

cease to be a member of the Tribunal from the date that the Governor-General receives the written instrument.

(2) The Chairperson may at any time resign the office by instrument in writing addressed to the Governor-General, and the resignation shall take effect from the date that the Governor-General receives the written instrument.

5. Revocation of appointment.

The Governor-General, upon recommendation of the Prime Minister after consultation with the Leader of Opposition, may terminate the appointment of any member of the Tribunal who —

(a) becomes of unsound mind or becomes permanently unable to perform his functions by reason of ill health;

(b) becomes bankrupt;

(c) is convicted and sentenced to a term of imprisonment;

(d) is convicted of any offence involving dishonesty; or

(e) fails to carry out the functions conferred or imposed on the member by this Act.

6. Publication of membership.

The Governor-General shall cause the names of every member of the Tribunal as first constituted, and any change in membership thereafter, to be published in the *Gazette.*

7. Proceedings of Tribunal.

(1) Subject to the provisions of this Act, the Tribunal shall regulate its own proceedings.

(2) The quorum of meetings of the Tribunal shall be three members.

(3) The decisions of the Tribunal shall be by a majority of votes of the members, and in addition to an original vote, the Chairperson shall have a casting vote in any case in which the voting is equal.

(4) Proper records of all proceedings of the Tribunal shall be kept.

8. Remuneration.

There shall be paid to the Chairperson and other members of the Tribunal, in respect of each appeal, the salary, honorarium and allowances as may be determined by the Minister responsible for Public Service.

9. Conflict of interest.

A member of the Tribunal who has any interest, directly or indirectly, in any matter before the Tribunal shall —

(a) as soon as possible when the relevant facts have come to the knowledge of that member, disclose the nature of the interest; and

(b) be absent during the deliberations of the matter and not take any part in the Tribunal's decision.

10. Confidentiality.

(1) A member of the Tribunal who obtains information in the course of exercising a power or carrying out a duty related to the administration of this Act or the regulations, shall preserve secrecy with respect to the information and shall not communicate the information to any person except —

(a) as may be required in connection with a proceeding under this Act or in connection with the administration of this Act or the regulations;

(b) to a ministry, department or agency of a government engaged in the administration of legislation similar to this Act or legislation that protects consumers or to any other entity to which the administration of legislation similar to this Act or legislation that protects consumers has been assigned;

(c) to a prescribed entity or organization if the purpose for the communication is consumer protection;

(d) to a law enforcement agency;

(e) to counsel of the person communicating the information; or

(f) with the consent of the person to whom the matter relates.

(2) Except in a proceeding under this Act, a member of the Tribunal shall not be required to give testimony in a civil proceeding with regard to information obtained in the course of exercising a power or carrying out a duty related to the administration of this Act or the regulations.

11. Indemnity.

No action, suit, prosecution, or other proceedings shall be brought or instituted personally against any member of the Tribunal in respect of any act done or omission made *bona fide* in accordance with this Act.

SECOND SCHEDULE

(section 91(3))

DATA PROTECTION OVERSIGHT COMMITTEE

1. Composition of Committee.

(1) The Committee shall consist of the members described in subparagraph (2), who shall be appointed by the Governor-General upon the recommendation of the Prime Minister after consultation with the Leader of the Opposition.

(2) The Committee members shall comprise —

(a) a retired Justice of the Supreme Court or Court of Appeal;

(b) a counsel and attorney having expertise in the area of data protection or privacy rights;

(c) a person representing the interests of data subjects;

(d) a person representing the interests of data controllers;

(e) three other persons having expertise in any one or more of the following areas —

(i) information and communications technology;

(ii) finance;

(iii) governance and public administration.

(3) The following persons shall not be eligible for appointment as members of the Committee —

(a) a member of either House of Parliament;

(b) a person who is bankrupt;

(c) a person who has been convicted of an offence involving dishonesty.

(4) A person appointed as a member of the Committee shall serve as a member for a period of three years and is eligible to be reappointed for one further period of three years.

(5) A person shall not be eligible for re-appointment if any circumstance in subparagraph (3) exists which would prohibit him from being appointed as a member.

2. Election of Chairperson.

(1) The members of the Committee shall elect one member, to be the Chairperson of the Committee.

(2) The Chairperson or any member elected by the Committee to act temporarily as Chairperson shall preside at a meeting of the Committee.

3. Appointment of secretary.

The Committee shall appoint a secretary whose duties shall be to —

(a) attend the meetings of the Committee;

(b) record minutes of the proceedings of the Committee and keep the minutes in proper form; and

(c) perform other duties connected with the work of the Committee as the Committee may require.

4. Revocation of appointment.

The Governor-General shall, upon the recommendation of the Prime Minister after consultation with the Leader of the Opposition, terminate the appointment of any member of the Committee if that member —

(a) is absent, without reasonable excuse, from three consecutive meetings of the Committee without the leave of —

(i) the Governor-General, in the case of the Chairperson; or

(ii) the Chairperson, in the case of any member other than the Chairperson;

(b) is convicted and sentenced to a term of imprisonment;

(c) is convicted of any offence involving dishonesty;

(d) becomes bankrupt; or

(e) fails to carry out the functions imposed on the member by this Act.

5. Resignation of members.

A member of the Committee may resign office by giving written notice of the resignation to —

(a) the Governor-General, in the case of the Chairperson; or

(b) the Chairperson, in the case of any member other than the Chairperson.

6. Publication of members.

The Governor-General shall cause the names of the members of the Committee as first constituted, and any change in membership thereafter to be published in the *Gazette*.

7. Proceedings of Committee.

(1) The Committee shall meet as often as it considers necessary for the proper conduct of its affairs but shall in any event meet not less than once per month.

(2) Any member of the Committee may attend a meeting virtually.

(3) The quorum of meetings of the Committee shall be four members.

(4) Decisions of the Committee shall be by a majority of votes of the members, and the Chairperson shall have a casting vote in addition to an original vote in any case where the voting is equal.

(5) Proper records of all proceedings of the Committee shall be kept.

8. Remuneration.

There shall be paid to the Chairperson and other members of the Committee, the salary, honorarium, and allowances as may be determined by the Minister responsible for public service.

9. Conflict of interest.

A member of the Committee who has any interest, directly or indirectly, in any matter before the Committee shall —

(a) as soon as possible when the relevant facts have come to the knowledge of that member, disclose the nature of the interest at a meeting of the Committee; and

(b) be absent during the deliberations of the Committee and not take any part in the decision.

10. Confidentiality.

(1) A member of the Committee who obtains information in the course of exercising a power or carrying out a duty related to the administration of this Act or the regulations, shall preserve secrecy with respect to the information and shall not communicate the information to any person except —

(a) as may be required in connection with a proceeding under this Act or in connection with the administration of this Act or the regulations;

(b) to a ministry, department or agency of a government engaged in the administration of legislation similar to this Act or legislation that protects consumers or to any other entity to which the administration of legislation similar to this Act or legislation that protects consumers has been assigned;

(c) to a prescribed entity or organization if the purpose for the communication is consumer protection;

(d) to a law enforcement agency;

(e) to counsel of the person communicating the information; or

(f) with the consent of the person to whom the matter relates.

(2) Except in a proceeding under this Act, a member of the Committee shall not be required to give testimony in a civil proceeding with regard to information obtained in the course of exercising a power or carrying out a duty related to the administration of this Act or the regulations.

11. Indemnity.

No action, suit, prosecution, or other proceedings shall be brought or instituted personally against any member of the Committee in respect of any act done or omission made *bona fide* in accordance with this Act.