

PARLIAMENT OF BARBADOS
Bridgetown



Report
of the
Joint Select Committee
on the
DATA PROTECTION BILL, 2019

**REPORT OF
JOINT SELECT COMMITTEE
ON THE
DATA PROTECTION BILL, 2019**

1. Pursuant to a Resolution of the Honourable the Senate on Friday, 31st May, 2019 and the concurrence of the Honourable the House of Assembly on Tuesday, 4th June, 2019, a Joint Select Committee (**hereafter referred to as “the Committee”**) was constituted to debate and report on:-

A Bill to:-

- (a) regulate the collection, keeping, processing, use and dissemination of personal data;
- (b) protect the privacy of individuals in relation to their personal data; and
- (c) provide for matters related to (a) and (b).

2. The following members were appointed to the Committee:-

Senator the Hon. Miss Kay S. McConney (Chairman)

Senator Damien R. Sands

Senator Rawdon J. H. Adams

Senator Miss Crystal N. Drakes

Senator Kevin J. Boyce

Senator Ms. Alpheia M. Wiggins

Hon. Dale D. Marshall, Q.C., M.P.

Bishop Joseph J. S. Atherley, J.P., M.P.

Hon. Dwight G. Sutherland, M.P.

Hon. Ms. C. Sandra V. Husbands, M.P.

Mr. Neil G. H. Rowe, M.P.

3. The Terms of Reference of the Committee were as follows:-

To inquire into and determine whether the Bill as drafted effectively fulfils the expressed objects of improving the protection of personal data.

To examine whether the Bill as drafted will upon effective implementation contribute to an ethos of compliance with data protection; thereby promoting transparency and accountability.

To make recommended changes, if deemed necessary, to the Bill as drafted for further consideration by the Chief Parliamentary Counsel.

4. The Committee has the honour to report as follows:-

The Committee scheduled meetings for the following dates:- Monday, 24th June, 2019, Wednesday, 26th June, 2019, Monday, 1st July, 2019 and Monday 8th July, 2019.

The Minutes of the meetings are appended hereto and marked “B”, “C”, “D” and “E” respectively and form part of this report.

Senator the Hon. Miss Kay S. McConney was elected Chairman of the Committee and chaired the meetings of the Committee.

The Committee at its first meeting settled on the procedure which governed its deliberations. It was determined that the deliberations of the second meeting as it related to the oral presentations would be streamed *via* Parliament’s website. Thereafter, as it related to the written submissions the meetings were closed to the public.

The agreed procedure that informed the Committee was for the Committee to receive the oral presentations at the second meeting during the morning session on Wednesday, 26th June, 2019. And in the afternoon, consideration was to be given to the written submissions. Each presenter would be allotted ten (10) minutes for their presentation

followed by a fifteen (15) to twenty (20) minutes question and answer segment. Subsequent written submissions were given consideration on Monday, 1st July, 2019.

The Committee determined that it would complete its work by Monday, 1st July, 2019 and be in a position to report to the Honourable the Senate and thereafter the Bill be submitted to the Honourable the House of Assembly.

The Committee by public advertisement *via* the Government Information Service requested oral or written submissions on the Bill to be received by Thursday, 20th June, 2019. The Committee however extended the deadline to Thursday, 27th June, 2019. The following persons made oral presentations:

1. Mr. Steve Clarke, Advisory Partner, Deloitte;
2. Mr. Chesterfield Coppin, E-Commerce Development Officer;
3. Ms. Cynthia Wiggins;
4. Mr. S. Antonio Hollingsworth – Bajan Digital Creations Inc.; and
5. Mr. Bartlett Morgan – Senior Associate, LEX Caribbean

Written submissions were received from the following persons/organisations:

1. Ms. Cynthia Wiggins;
2. Mr. S. Antonio Hollingsworth – Bajan Digital Creations Inc.;
3. Ms. Soledad González, Business Developer for Latin America – Quidgest;
4. Ms. Shireen Flann (Board Member) and Mr. Steven Williams (President) – Barbados ICT Professionals Association;
5. Mr. Shannon Clarke;
6. Mr. Grenville Phillips II, President – Solutions Barbados;
7. The Barbados Bankers Association Inc.;
8. The Barbados Bar Association; and
9. Mr. Devaron Bruce; and
10. Barbados Association of Medical Practitioners

These submissions are appended hereto and marked “F”, “G”, “H”, “I”, “J”, “K”, “L” “M”, “N” and “O”, and form part of this report.

In addition to the written submissions, the Committee through the Clerk of Parliament invited persons/organisations to make written submissions to the Committee. (See letters appended “P”, “Q” and “R” respectively)

The Barbados Bankers Association Inc. and the Barbados Bar Association accepted the invitation and submitted written submissions to the Committee for its consideration.

The reference in the Report to the amendments are to the old Bill at Appendix “A” and those changes are consequently reflected in the new Bill at Appendix “S”.

Having given due consideration to the various submissions, the Committee agreed to the following amendments to the Bill and reflected in the revised Bill:-

1. Amend the long title-“*provide for provide for matters*” should read “*provide for matters*”.
2. Amend clause 2 to delete the reference to “Credit Reference Agency”.
3. Amend clause 4(7) to clarify the words “*ensure the reliability*” in respect of employees.
4. The Committee agreed to amend clause 9(1)(a) and delete the words “written consent” and substitute for the words “explicit consent”. The Committee also agreed that a definition of “explicit consent” should be provided. **A definition of consent was included in clause 2 which will give clarity to use of the word “consent” throughout the Bill. The reference to “written consent” was deleted in clause 9(1)(a) and replaced with the word “consent”. “Consent” is defined in clause 2 of the Bill.**
5. Amend clause 15 and any other clause in the Bill to remove any reference to “*his or her*” and make any consequential amendment arising from such reference.
6. Amend clause 71 to empower the Commissioner to issue advice to data processors and data controllers upon request. **See clause 71 (m) where the words “or person” have been inserted which will include data controllers and data processors as well as other persons who may require advice.**

7. Amend clause 79(1)- “... *requiring the data controller to furnish him with ...*” should read “*requiring the data controller to furnish him with ...*”
8. References to the word “court” in the Bill should be clarified. See clause 2 definition of sensitive personal data, para. (k), clause 16(4), clause 17(2), clause 25(e), clause 38(1), clause 67(1)(a), clause 70(3), clause 73(2)(a), clause 82(1)(b),(2), clause 85(1), clause 88, clause 94(2)(a)(ii), clause 95(3),
9. Insert a clause on the liability of data controllers and data processors. **See clause 93.**
10. Insert a clause on the right of compensation. **See clause 93.**

2019/04/12

OBJECTS AND REASONS

This Bill would

- (a) regulate the collection, keeping, processing, use and dissemination of personal data;**
- (b) protect the privacy of individuals in relation to their personal data; and**
- (c) provide for matters related to (a) and (b).**

A

Arrangement of Sections

PART I

PRELIMINARY

1. Short title
2. Interpretation
3. Application of Act

PART II

DATA PROTECTION PRINCIPLES

4. Principles relating to processing of personal data
5. Fairness of processing
6. Lawfulness of processing
7. Conditions for consent
8. Conditions applicable to child's consent
9. Processing of sensitive personal data

PART III
RIGHTS OF A DATA SUBJECT

- 10. Right of access**
- 11. Right to rectification**
- 12. Right to erasure**
- 13. Right to restriction of processing**
- 14. Notification regarding rectification or erasure of personal data or restriction of processing of personal data**
- 15. Right to data portability**
- 16. Right to prevent processing likely to cause damage or distress**
- 17. Right to prevent processing for purposes of direct marketing**
- 18. Automated individual decision-making, including profiling**
- 19. Information to be provided where personal data is collected from the data subject**
- 20. Information to be provided where personal data has not been obtained from the data subject**
- 21. Transparent information, communication and modalities for the exercise of the rights of the data subject**

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

- 22. General principle for transfers**
- 23. Adequate level of protection**
- 24. Appropriate safeguards**
- 25. Binding corporate rules**
- 26. Derogations**
- 27. Non-compliance**
- 28. Substantial public interest**

PART V

EXEMPTIONS

- 29. References to subject information provisions and non-disclosure provisions**
- 30. National Security**
- 31. Crime and taxation**
- 32. Health, education and social work**
- 33. Regulatory activity**
- 34. Journalism, literature and art**

35. Research, history and statistics
36. Manual data held by public authorities
37. Information available to the public by or under enactment
38. Disclosures required by law or made in connection with legal proceedings
39. Parliamentary privilege
40. Legal professional privilege
41. Domestic purposes
42. Confidential references given by the data controller
43. Armed forces
44. Judicial appointments and honours
45. Appointments to public service
46. Corporate finance
47. Negotiations with data subject
48. Examinations
49. Powers to make further exemptions by Order

PART VI

DATA CONTROLLER AND DATA PROCESSOR

50. Data controllers must be registered

51. Register of Data Controllers
52. Notification of changes in respect of a data controller
53. Responsibility of the data controller
54. Data protection by design and by default
55. Data processors must be registered
56. Register of Data Processors
57. Notification of changes in respect of a data processor
58. Data Processor
59. Processing under the authority of the data controller or data processor
60. Records of processing activities
61. Cooperation with the Commissioner
62. Security of processing
63. Notification of a personal data breach to the Commissioner
64. Communication of a personal data breach to the data subject
65. Data protection impact assessment
66. Prior consultation
67. Designation of the data privacy officer
68. Position of the data privacy officer

- 69. Duties and functions of a data privacy officer

PART VII

DATA PROTECTION COMMISSIONER

- 70. Data Protection Commissioner
- 71. Functions of Commissioner
- 72. Staff
- 73. Confidential information
- 74. Indemnity
- 75. Report

PART VIII

ENFORCEMENT

- 76. Enforcement notice
- 77. Cancellation of enforcement notice
- 78. Request for assessment
- 79. Information notice
- 80. Special information notice
- 81. Determination by Commissioner as to the purposes of journalism or artistic or literary purposes

- 82. Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes**
- 83. Failure to comply with notice**
- 84. Service of notice by Commissioner**
- 85. Warrants**
- 86. Execution of warrants**
- 87. Matters exempt from inspection and seizure**
- 88. Return of warrants**
- 89. Obstruction of execution of a warrant**

PART IX

DATA PROTECTION TRIBUNAL

- 90. Establishment of the Data Protection Tribunal**
- 91. Right of appeal**
- 92. Determination of appeals**

PART X

MISCELLANEOUS

- 93. Unlawful obtaining of personal data**
- 94. Administrative penalty**

- 95. Disclosure of information
- 96. Act binds Crown
- 97. Amendment of *Schedule*
- 98. Regulations
- 99. Commencement

SCHEDULE
Data Protection Tribunal

BARBADOS

A Bill entitled

An Act to

- (a)* regulate the collection, keeping, processing, use and dissemination of personal data;
- (b)* protect the privacy of individuals in relation to their personal data; and
- (c)* provide for provide for matters related to *(a)* and *(b)*.

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Data Protection Act, 2019*.

Interpretation

2. In this Act

“accessible public record” means any record that is kept by a public authority and to which members of the public are given access;

“accessible record” means

- (a) a health record;
- (b) an educational record; or
- (c) an accessible public record;

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual;

“child” means a person who is under the age of 18 years;

“Commissioner” means the Data Protection Commissioner referred to in section 70;

“consent” in relation to a data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him;

“credit reference agency” means a person who carries on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose;

“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 such equipment;
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record; or
- (e) does not fall within paragraph (a), (b), (c) or (d) but is recorded information held by a public authority;

“data controller” means

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

“data privacy officer” means a person designated as such pursuant to section 67;

“data processor” means any person, other than an employee of a data controller, who processes personal data on behalf of the data controller;

“data subject” means an individual who is the subject of personal data;

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual;

“health care professional” includes a person who is registered under

- (a) the *Medical Professions Act* (Act 2011-1);
- (b) the *Dental Registration Act*, Cap. 367;
- (c) the *Nurses Act*, Cap. 372 or enrolled under that Act;
- (d) the *Pharmacy Act*, Cap. 372D; and
- (e) the *Paramedical Professions Act*, Cap. 372C;

“health record” means any record which

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

“personal data” means data which relates to an individual who can be identified

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

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

“process” in relation to information or data, means to obtain, record or hold the information or data or carry out any operation or set of operations on the information or data, including the

- (a) organization, adaptation or alteration of the information or data;
- (b) retrieval, consultation or use of the information or data;
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

“profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

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

“public authority” means a public office or a ministry, department, agency, unit or other authority of the Government including a statutory body;

“recipient” means a person, public authority, agency or another body, to which the personal data is disclosed but a public authority shall not be considered a recipient where the personal data is received pursuant to an obligation imposed by the any enactment;

“relevant filing system” means any set of information relating to individuals to the extent that although the information is not processed by means of equipment operating automatically in response to instructions given for that

purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that the specific information relating to a particular individual is readily accessible;

“representative” means a representative of the data controller or data processor who is not established in Barbados and is nominated pursuant to

- (a) section 50(3) in respect of a data controller; or
- (b) section 55(3) in respect of a data processor

and who represents that data controller or data processor with regard to their obligations under this Act;

“restriction of processing of personal data” means marking of stored personal data with the aim of limiting their processing in the future;

“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) membership of a political body;
- (e) membership of a trade union;
- (f) genetic data;
- (g) biometric data;
- (h) sexual orientation or sexual life;
- (i) financial record or position;
- (j) criminal record; or
- (k) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;

“trade union” has the meaning assigned to it by the *Trade Unions Act, Cap. 361*;

“Tribunal” means the Data Protection Tribunal established pursuant to section 90.

Application of Act

3.(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 Barbados;
- (b)* the processing of personal data of data subjects in Barbados by a data controller or a data processor not established in Barbados, where the processing activities are related to the offering of goods or services to data subjects in Barbados.

(2) For the purposes of subsection (1) “established in Barbados” means

- (a)* an individual who is ordinarily resident in Barbados;
- (b)* a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c)* a person who does not fall within paragraph *(a)* or *(b)* but maintains in Barbados an office, branch or agency through which he carries on any activity related to the processing of personal data.

PART II

DATA PROTECTION PRINCIPLES

Principles relating to processing of personal data

4.(1) Personal data shall be

- (a)* processed lawfully, fairly and in a transparent manner in relation to the data subject;
- (b)* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- (c)* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d)* accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (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;
- (f)* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) A data controller shall, in relation to all of the personal data he processes, comply with the requirements set out in subsection (1).

(3) A data controller pursuant to subsection 1(b) may specify the purpose for which personal data is obtained

(a) in any notice given for the purposes of section 5(3)(a) by the data controller to the data subject; or

(b) in a notification given to the Commissioner pursuant to Part III.

(4) In determining whether any disclosure of personal data is compatible with the purpose for which the data is obtained in accordance with subsection 1(b), regard is to be had to the purpose for which the personal data is intended to be processed by any person to whom the data is disclosed.

(5) Subsection 1(d) shall not as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where

(a) having regard to the purpose for which the data was obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and

(b) the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicate that fact.

(6) Pursuant to subsection 1(f), having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to

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

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

(7) The data controller shall take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(8) Pursuant to subsection 1(*f*), where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall

(*a*) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and

(*b*) take reasonable steps to ensure compliance with those measures.

(9) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with subsection 1(*f*) unless

(*a*) the processing is carried out under a contract

(i) which is made or evidenced in writing; and

(ii) under which the data processor is to act only on instructions from the data controller; and

(*b*) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by subsection 1(*f*).

(10) A person who fails to comply with the requirements set out in subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Fairness of processing

5.(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 any 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

(*a*) authorised by or under any enactment to supply them; or

person within that period, the time when the data controller does become, or ought to become, so aware; or

(iii) in any other case, the end of that period.

Lawfulness of processing

6.(1) Processing shall be lawful where

- (a) the data subject has given consent to the processing of his personal data for one or more specific purposes; or
- (b) the processing is necessary
 - (i) for the performance of a contract to which the data subject is a party;
 - (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
 - (iii) for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
 - (iv) in order to protect the vital interests of the data subject;
 - (v) for the administration of justice;
 - (vi) for the exercise of any functions of either House of Parliament;
 - (vii) for the exercise of any functions conferred on any person by or under any enactment;
 - (viii) for the exercise of any functions of a public authority;
 - (ix) for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; or

(x) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(2) Subsection (1)(b)(x) shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for consent

7.(1) Where processing is based on consent, the data controller shall demonstrate that the data subject has consented to processing of his personal data.

(2) Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) A data subject has the right to withdraw his consent in respect of the processing of his personal data at any time and the data controller shall inform the data subject of his right to withdraw prior to him giving consent to the data controller to process his personal data.

(4) The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal.

(5) In determining whether consent is freely given, the data controller shall take into account whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Conditions applicable to child's consent

8.(1) The processing of a child's personal data shall be lawful only where and to the extent that consent is given or authorised by the parent or guardian of the child.

(2) The data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the parent or guardian of a child, taking into consideration available technology.

(3) Subsection (1) shall not effect contract law under any enactment in respect of the validity, formation or effect of a contract in relation to a child.

Processing of sensitive personal data

9.(1) Processing of sensitive personal data shall be prohibited unless

- (a) the data subject gives his written consent to the processing;
- (b) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- (c) the processing is necessary in order to protect the vital interests of the data subject or another person, in a case where
 - (i) consent cannot be given by or on behalf of the data subject; or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject;
- (d) the processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

- (e)* the processing
 - (i)* is carried out in the course of its legitimate activities by any body or association which
 - (A)* is not established or conducted for profit; and
 - (B)* exists for political, philosophical, religious or trade union purposes;
 - (ii)* is carried out with appropriate safeguards for the rights and freedoms of data subjects;
 - (iii)* relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
 - (iv)* does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (f)* the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- (g)* the processing is necessary
 - (i)* for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (ii)* for the purpose of obtaining legal advice; or
 - (iii)* otherwise for the purposes of establishing, exercising or defending legal rights;
- (h)* the processing is necessary for the administration of justice;
- (i)* the processing is necessary for the exercise of any functions of either House of Parliament;
- (j)* the processing is necessary for the exercise of any functions conferred on any person by or under an enactment;

- (k) the processing is necessary for the exercise of any functions of a public authority;
 - (l) the processing is necessary for medical purposes and is undertaken by

 - (i) a health care professional; or
 - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
 - (m) the processing

 - (i) is of sensitive personal data consisting of information as to racial or ethnic origin; and
 - (ii) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
 - (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- (2) The Minister may by Order specify circumstances other than those identified in subsection (1) where sensitive personal data may be processed.
- (3) An Order made pursuant to subsection (2) is subject to negative resolution.
- (4) For the purposes of subsection (1)(l) "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.

PART III

RIGHTS OF A DATA SUBJECT

Right of access

- 10.(1)** A data subject has the right
- (a) to be informed by a data controller whether personal data of that data subject is being processed by or on behalf of the data controller;
 - (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request from, and to be given by, the data controller, a description of
 - (i) the purposes of the processing;
 - (ii) the categories of personal data concerned;
 - (iii) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organisations;
 - (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (v) the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (vi) the right to lodge a complaint with the Commissioner;
 - (vii) any available information as to their source, where the personal data is not collected from the data subject;
 - (viii) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases,

meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- (2) Where personal data is transferred to another country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 24.
- (3) The data controller shall provide a copy of the personal data undergoing processing to the data subject and where requests more copies are requested by the data subject, the data controller may charge a reasonable fee based on administrative costs.
- (4) Where the data subject makes the request for personal data by electronic means, and unless otherwise requested by the data subject, the personal data shall be provided in electronic form.
- (5) The right of the data subject to obtain a copy of personal data referred to subsection (3) shall not adversely affect the rights and freedoms of other data subjects.

Right to rectification

- 11.(1) The data subject shall have the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning him.
- (2) Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed by the data controller, including by means of providing a supplementary statement.

Right to erasure

- 12.(1) The data subject shall have the right to obtain from the data controller the erasure of 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 on which the processing is based pursuant to section 6(1)(a) or section 9(1)(a), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to section 16 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 17;
- (d) the personal data has been unlawfully processed;
- (e) the personal data has to be erased in compliance with a legal obligation in Barbados to which the data controller is subject.

(3) Where the data controller has made the personal data public and is obliged pursuant to subsection (1) or (2) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers who are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, the personal data.

(4) Subsections (1), (2) and (3) shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by any enactment 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 official authority vested in the data controller;
- (c) for reasons of public interest in the area of public health;

- (d) for archiving for the purposes of research, history or statistics in accordance with section 35; or
- (e) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

13.(1) The data subject shall have the right to obtain from the data controller restriction of processing of personal data where one of the following applies:

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

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

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

(3) A data subject who has obtained restriction of processing of personal data pursuant to subsection (1) shall be informed by the data controller before the restriction of processing of personal data is removed pursuant to subsection (2).

Notification regarding rectification or erasure of personal data or restriction of processing of personal data

14.(1) The data controller shall communicate any

- (a)* rectification of personal data pursuant to section 11;
- (b)* erasure of personal data pursuant to section 12; or
- (c)* restriction of processing of personal data pursuant to section 13

to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The data controller shall inform the data subject about those recipients where the data subject requests such information.

Right to data portability

15.(1) The data subject has the right to receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format.

(2) The data subject has the right to transmit the personal data concerning him, which he has provided to a data controller to another data controller without hindrance where

- (a)* the processing is based on consent pursuant to section 6(1)(a) or section 9(1)(a) or on a contract pursuant to section 6(1)(b)(i); and
- (b)* the processing is carried out by automated means.

(3) In exercising his or her right to data portability pursuant to subsections (1) and (2), the data subject shall have the right to have his personal data transmitted directly from one data controller to another, where technically feasible.

(4) The exercise of the right referred to in subsection (1) shall be exercised without prejudice to section 12.

- (5) The exercise of the right referred to in subsection (1) shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- (6) The exercise of the right referred to in subsection (1) shall not adversely affect the rights and freedoms of other data subjects.

Right to prevent processing likely to cause damage or distress

16.(1) Subject to subsection (2), a data subject is entitled, by a written notice, to require the data controller at the end of a 21 day period to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that

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

(2) Subsection (1) does not apply

- (a) in a case where any of the conditions in section 6(1)(a) or (b)(i), (ii), (iii) or (iv) is satisfied; or
- (b) in such other cases as the Minister may prescribe by Order.

(3) The data controller shall, within 21 days of receiving a notice under subsection (1), give the data subject written notice stating

- (a) that he has complied or intends to comply with the data subject's notice;
- (b) the reasons for his refusal to comply with the data subject's notice; or
- (c) the reasons for complying with part of the data subject's notice and the extent of that compliance.

(4) Where a court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller in question has failed

to comply with the notice, the court may order the data controller to take such steps for complying with the notice as the court sees fit.

Right to prevent processing for purposes of direct marketing

17.(1) A person is entitled at any time, by a written notice to a data controller, to require the data controller at the end of a 21 day period to cease processing for the purposes of direct marketing, personal data in respect of which he is the data subject.

(2) Where a court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the court may order the data controller to take such steps for complying with the notice as the court sees fit.

(3) For the purposes of this section “direct marketing” means the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.

Automated individual decision-making, including profiling

18.(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or similarly significantly affects him.

(2) Subsection (1) shall not apply where the automated processing or profiling of personal data is

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

(3) In the cases referred to in subsection (2)(a) and (c), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the data controller, to express his opinion or object to the decision.

(4) Subsection (2) shall not apply to sensitive personal data unless it is in the public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Information to be provided where personal data is collected from the data subject

19.(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 the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;
- (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d) where the processing is done pursuant to 6(1)(b)(x), the legitimate interests pursued by the data controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the data controller intends to transfer personal data to another country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in sections 24 or 25 reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in subsection (1), the data controller shall at the time when personal data is obtained, provide the data

subject with the following further information necessary to ensure fair and transparent processing:

- (a)* the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (b)* the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
 - (c)* where the processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (d)* the right to lodge a complaint with the Commissioner;
 - (e)* whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - (f)* the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (3) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).
- (4) Subsections (1), (2) and (3) shall not apply where and insofar as the data subject already has the information.

Information to be provided where personal data has not been obtained from the data subject

20.(1) Where personal data has not been obtained from the data subject, the data controller shall provide the data subject with the following:

- (a)* the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b)* the contact details of the data privacy officer, where applicable;
- (c)* the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d)* the categories of personal data concerned;
- (e)* the recipients or categories of recipients of the personal data, if any;
- (f)* where applicable, that the data controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in section 24 or section 25, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in subsection (1), the data controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a)* the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b)* where the processing is done pursuant to section 6(1)(b)(x), the legitimate interests pursued by the data controller;
- (c)* the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing

concerning the data subject and to object to processing as well as the right to data portability;

- (d)* where processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (e)* the right to lodge a complaint with the Commissioner;
 - (f)* from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
 - (g)* the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (3) The data controller shall provide the information referred to in subsections (1) and (2)
- (a)* within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data is processed;
 - (b)* if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
 - (c)* if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.
- (4) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).

- (5) Subsections (1), (2), (3) and (4) shall not apply where and insofar as:
- (a) the data subject already has the information;
 - (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes pursuant to section 35;
 - (c) obtaining or disclosure is expressly laid down by any enactment to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
 - (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by any enactment.

Transparent information, communication and modalities for the exercise of the rights of the data subject

21.(1) The data controller shall take appropriate measures to provide any information referred to in section 19 and section 20 and any communication under sections 10 to 18 and section 63 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

(2) The information pursuant to subsection (1) shall be provided in writing, or by other means, including, where appropriate, by electronic means.

(3) When requested by the data subject, the data controller may provide the information, pursuant to his rights under sections 10 to 15 and 18 orally provided that the identity of the data subject is verified.

(4) The data controller shall facilitate the exercise of data subject rights under sections 10 to 15 and 18.

(5) The data controller shall provide information on action taken on a request under sections 10 to 15 and 18 to the data subject without undue delay and in any event within one month of receipt of the request.

(6) The period of time referred to in subsection (5) shall be extended by two months where necessary, taking into account the complexity and number of the requests under sections 10 to 15 and 18.

(7) The data controller shall inform the data subject of any extension granted pursuant to subsection (6) within one month of receipt of the request, together with the reasons for the delay.

(8) Where the data subject makes the request pursuant to his rights under sections 10 to 15 and 18 by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(9) Where the data controller does not take action on the request of the data subject under this section, the data controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Commissioner or appealing to the High Court.

(10) Information provided under section 18 and section 19 and any communication and any actions taken under sections 10 to 15 and 18 and section 63 shall be provided free of charge.

(11) Where requests referred to in this section from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the data controller may either

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

(12) The data subject may object to the decision of a data controller made pursuant to subsection (11) by lodging a complaint with the Commissioner or appealing to the Tribunal.

(13) For the purposes of subsection (12), the data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of a request referred to in subsection (11).

(14) Where a data controller has reasonable doubts concerning the identity of the individual making a request pursuant to sections 10 to 18, the data controller may request the provision of additional information necessary to confirm the identity of the data subject.

(15) The information to be provided to data subjects pursuant to section 19 and section 20 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing and where the icons are presented electronically they shall be machine-readable.

(16) The Minister in consultation with the Commissioner, may make regulations for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

General principle for transfers

22. Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for

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

Adequate level of protection

23. For the purposes of section 22, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the data is intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and
- (h) any security measures taken in respect of the data in that country or territory.

Appropriate safeguards

24. For the purposes of section 22, appropriate safeguards may be provided for by

- (a) a legally binding and enforceable instrument between public authorities;
- (b) binding corporate rules in accordance with section 25;
- (c) standard data protection clauses prescribed by the Commissioner with the approval of the Minister;

- (d) contractual clauses authorised by the Commissioner between the data controller or data processor and the data controller, data processor or the recipient of the personal data; or
- (e) provisions, authorised by the Commissioner, to be inserted into administrative arrangements between public authorities which include enforceable and effective data subject rights.

Binding corporate rules

25.(1) Data controllers and data processors shall develop binding corporate rules which shall specify

- (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- (c) their legally binding nature, both in and outside of Barbados;
- (d) the application of principles regarding purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of sensitive personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with this Act, the right to lodge a complaint with the competent supervisory authority or Commissioner and the courts and

to obtain any other available form of redress and, where appropriate, compensation for a breach of the binding corporate rules;

- (f)* the acceptance by the data controller or data processor of liability for any breaches of the binding corporate rules;
- (g)* that the data controller or the data processor shall be exempt from the liability referred to in paragraph (f), in whole or in part, only where it is proven that the data controller or data processor is not responsible for the event giving rise to the damage;
- (h)* how the information on the binding corporate rules is provided to the data subjects;
- (i)* the complaint procedures;
- (j)* the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules;
- (k)* the mechanisms for reporting and recording changes to the binding corporate rules and reporting those changes to the supervisory authority;
- (l)* the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority or Commissioner the results of verifications of the measures specified in paragraph (j);
- (m)* the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n)* the appropriate data protection training to personnel having permanent or regular access to personal data.

(2) The binding corporate rules referred to in subsection (1) shall be submitted to the Commissioner for authorisation.

(3) The Commissioner may specify the format and procedures for the exchange of information between data controllers, data processors and supervisory authorities for binding corporate rules.

(4) For the purposes of this section,

“binding corporate rules” means personal data protection policies which are adhered to by a data controller or data processor for transfers or a set of transfers of personal data to a data controller or a data processor in one or more countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

“enterprise” means a person engaged in an economic activity;

“group of undertakings” means a controlling undertaking and its controlled undertakings;

“supervisory authority” means an independent public authority which is established by in a country or territory outside of Barbados.

Derogations

26. Section 22, 23 and 24 shall not apply where

- (a) the data subject has given his consent to the transfer of personal data;
- (b) the transfer of personal data is necessary for
 - (i) the performance of a contract between the data subject and the data controller;
 - (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (iii) the conclusion of a contract between the data controller and a person other than the data subject which
 - (A) is entered into at the request of the data subject; or

- (B) is in the interest of the data subject;
- (iv) the performance of a contract described in sub-paragraph (iii);
- (v) reasons of substantial public interest;
- (vi) the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- (vii) the purpose of obtaining legal advice;
- (viii) the purposes of establishing, exercising or defending legal rights; or
- (ix) the protection of the vital interests of the data subject;
- (c) the transfer of personal data is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer;
- (d) the transfer of personal data is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer of personal data has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

Non-compliance

27. A person who contravenes sections 22, 23 or 24 is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Substantial public interest

28.(1) The Minister may by Order specify the

- (a)* circumstances in which a transfer of the personal data of data subjects outside of Barbados is to be considered to be necessary for reasons of substantial public interest; and
- (b)* circumstances in which a transfer of the personal data of data subjects outside of Barbados, which is not required by or under an enactment, is not to be considered necessary for reasons of substantial public interest.

(2) An Order made pursuant to subsection (1) shall be subject to negative resolution.

PART V

EXEMPTIONS

References to subject information provisions and non-disclosure provisions

29.(1) In this Part

- (a)* “the subject information provisions” refers to
 - (i)* section 4(1)(a) to the extent to which it requires compliance with section 5(2); and
 - (ii)* section 10;
- (b)* “the non-disclosure provisions” refers to the following provisions to the extent to which they are inconsistent with the disclosure in question:
 - (i)* section 4(1)(a), except to the extent to which it requires compliance with the conditions in 6 and 9;

- (ii) section 4(1) (b), (c), (d), (e); and
- (iii) sections 11 to 18.

(2) Except as provided for by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding of information.

National Security

30. Parts II, III, IV, VI and section 79 do not apply where the processing of the personal data is required for the purpose of safeguarding national security.

Crime and taxation

31.(1) Personal data processed for

- (a) the prevention or detection of crime;
- (b) the apprehension or prosecution of offenders; or
- (c) the assessment or collection of any tax, duty or other imposition of a similar nature,

are exempt from section 4(1)(a) (except to the extent to which it requires compliance with the conditions in section 6 and 9) and from section 10 in any case to the extent to which the application of those provisions to the data is likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Personal data which

- (a) is processed for the purpose of discharging statutory functions; and
- (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1)(a) to (c)

is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in subsection (1)(a) to (c).

- (3) Personal data is exempt from the non-disclosure provisions where
- (a) the disclosure is for any of the purposes mentioned in subsection (1)(a) to (c); and
 - (b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned in subsection (1)(a) to (c).
- (4) Personal data in respect of which the data controller is a public authority and which
- (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 authority for any of the following purposes:
 - (i) the assessment or collection of any 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 of, or an unlawful application of, public funds; and
 - (b) is processed for either of those purposes

is exempt from section 10 to the extent to which the exemption is required in the interests of the operation of the system.

Health, education and social work

32.(1) The Minister may by Order exempt from the subject information provisions, or modify those provisions in relation to, personal data

- (a) consisting of information as to the physical or mental health or condition of a data subject;
- (b) in respect of which the data controller is an educational institution and which consist of information relating to persons who are or have been pupils at the educational institution;

- (c) in respect of which the data controller is a tertiary institution and which consist of information relating to persons who are or have been students at the tertiary institution;
- (d) of such other descriptions as may be specified in the Order, being information processed
 - (i) by public authorities, charities or other entities designated by or under the Order; and
 - (ii) in the course of, or for the purposes of, carrying out social work in relation to the data subject or other individuals.

(2) Notwithstanding subsection (1)(d), Minister shall not confer any exemption or make any modification under subsection (1)(d) except so far as he considers that the application to the data of those provisions (or of those provisions without modification) is likely to prejudice the carrying out of social work.

(3) In subsection (1)

“educational institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41;

“tertiary institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41.

Regulatory activity

33.(1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed for the purpose of

- (a) protecting members of the public against
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;
 - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity;
- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;
- (c) protecting the property of charities from loss or misapplication;
- (d) the recovery of the property of charities;
- (e) securing the health, safety and welfare of persons at work; or
- (f) protecting persons other than persons at work against risk to health or safety arising out of, or in connection with, the actions of persons at work.

(3) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

- (a) maladministration by public authorities;
- (b) failures in services provided by public authorities; or
- (c) a failure of a public authority to provide a service which it is a function of the authority to provide

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

(4) Personal data processed for the purpose of discharging any function which is designed for

- (a) protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;
- (b) regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
- (c) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market

is exempt from the subject information provisions to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

(5) For the purposes of subsection (2) “relevant function” means

- (a) any function conferred on any person by or under any enactment;
- (b) any function of a public authority; or
- (c) any other function which is of a public nature and is exercised in the public interest.

Journalism, literature and art

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

- (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;

- (b)* the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
 - (c)* the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the purpose of journalism or artistic or literary purposes.
- (2) In considering for the purposes of subsection (1)(b) 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 his compliance with any code of practice which is relevant to the publication in question and is designated by the Minister by Order for the purposes of this subsection.
- (4) In any proceedings against a data controller where the data controller claims, or it appears that any personal data to which the proceedings relate are being processed
 - (a)* only for the purposes of journalism or for artistic or literary purposes; and
 - (b)* with a view to the publication by any person of any journalistic, literary or artistic material which, at the time 24 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 (5) is met.
- (5) The conditions referred to in subsection (4) 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.
- (6) For the purposes of this section “publication”, in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

Research, history and statistics

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

(2) Personal data which is processed only for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from section 10 where

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

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

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

(a) to any 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; or

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

(5) In this section

“research purposes” includes statistical or historical purposes;

“the relevant conditions”, in relation to processing of personal data, means the conditions that the data

- (a) is not processed to support measures or decisions with respect to particular individuals; and
- (b) is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Manual data held by public authorities

36. Personal data which fall within paragraph (e) of the definition of “data” in section 2 is exempt from Parts II, III, IV and VI.

Information available to the public by or under enactment

37. Personal data is exempt from Parts II, III, IV and VI where the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

Disclosures required by law or made in connection with legal proceedings

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

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

- (a) for the purpose of, or in connection with, any legal proceedings including prospective 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.

Parliamentary privilege

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

Legal professional privilege

40. 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.

Domestic purposes

41. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs including recreational purposes is exempt from Parts II, III, IV and VI.

Confidential references given by the data controller

42. Personal data is exempt from section 10 where it consists 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 any office; or
- (c) the provision, or prospective provision, by the data subject of any service.

Armed forces

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

Judicial appointments and honours

- 44.** Personal data processed for the purposes of
- (a) assessing any person's suitability for judicial office or the office of Queen's Counsel; or
 - (b) the conferring by the Crown of any honour or dignity,
- is exempt from the subject information provisions.

Appointments to public service

- 45.** The Minister may by Order exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for
- (a) employment in the Public Service; or
 - (b) any office to which appointments are made by the Governor-General or by a Minister.

Corporate finance

- 46.(1)** Where personal data is processed for the purposes of, or in connection with, a corporate finance service
- (a) the data is exempt from the subject information provisions to the extent to which either
 - (i) the application of those provisions to the data could affect the price of any instrument which is already in existence or is to be or may be created; or
 - (ii) the data controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and

- (b) to the extent that the data is not exempt from the subject information provisions by virtue of paragraph (a), the data is exempt from those provisions where the exemption is required for the purpose of safeguarding an important economic or financial interest of Barbados.
- (2) For the purposes of subsection (1)(b) the Minister may by Order specify
- (a) matters to be taken into account in determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of Barbados; or
 - (b) circumstances in which exemption from those provisions is, or is not, to be taken to be required for that purpose.
- (3) In this section
- “corporate finance service” means a service consisting of
- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
 - (b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
 - (c) services relating to such underwriting as is mentioned in paragraph (a);

“price” includes value.

Negotiations with data subject

47. Personal data which consist 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 in any case to the extent to which the application of those provisions would be likely to prejudice those negotiations.

Examinations

48.(1) The results of an examination are exempt from section 10.

(2) Personal data consisting of information recorded by candidates during an academic, professional or other examination is exempt from section 10.

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

Powers to make further exemptions by Order

49.(1) The Minister may by Order exempt from the subject information provisions personal data consisting of information the disclosure of which is prohibited or restricted by or under any enactment where and to the extent that he considers it necessary for the safeguarding of

(a) the interests of the data subject; or

(b) the rights and freedoms of any other individual,

that the prohibition or restriction ought to prevail over those provisions.

(2) The Minister may by Order exempt from the non-disclosure provisions any disclosures of personal data made in circumstances specified in the Order, where he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other person.

(3) An Order made under this section shall be subject to negative resolution.

PART VI

DATA CONTROLLER AND DATA PROCESSOR

Data controllers must be registered

50.(1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers.

(2) A person who desires to operate as a data controller may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data controller that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data controller who is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Controllers

51.(1) The Commissioner shall keep 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 pursuant to section 50, the following particulars:

- (a)* the name and address and other contact information of the data controller;
- (b)* the date of registration;
- (c)* a description of the personal data processed by or on behalf of the data controller and of the categories of data subject to which they relate;
- (d)* a description of the purposes for which the data is processed;
- (e)* a description of any recipients to whom the data controller intends or may wish to disclose the data;
- (f)* the names, or a description of, any countries outside Barbados to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and
- (g)* where the data controller is not established in Barbados within the meaning of section 50(6), the name, address and other contact information of the representative nominated pursuant to section 50(3).

(2) The Register of Data Controllers shall be open to inspection at the office of the Commissioner.

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

Notification of changes in respect of a data controller

52.(1) 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 in relation to him.

(2) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register of Data Controllers as are necessary.

Responsibility of the data controller

53.(1) The data controller shall implement the appropriate technical and organisational measures to ensure that processing is performed in accordance with this Act taking into consideration the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals.

(2) Where proportionate in relation to processing activities, the measures referred to in subsection (1) shall include the implementation of appropriate data protection policies by the data controller.

Data protection by design and by default

54.(1) The data controller shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement the principles set out in section 4 in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects, taking into consideration the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

(2) The data controller shall implement the appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing is processed.

(3) Subsection (2) applies to the amount of personal data collected, the extent of processing of the personal data, the period of storage of the personal data and the accessibility to the personal data.

(4) The technical and organisational measures referred to in subsection (1) shall ensure that personal data is not, by default, made accessible without the individual's intervention to an indefinite number of individuals.

Data processors must be registered

55.(1) A person shall not operate as a data processor unless he is registered in the Register of Data Processors.

(2) A person who desires to operate as a data processor may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data processor that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data processor that is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Processors

56.(1) The Commissioner shall keep a register, to be called the Register of Data Processors, in which he shall cause to be entered in relation to each data processor, the following particulars:

- (a)* the name and address and other contact information of the data processor;
 - (b)* the date of registration;
 - (c)* a description of the personal data processed by or on behalf of the data processor and of the categories of data subject to which they relate;
 - (d)* a description of the purposes for which the data is processed;
 - (e)* a description of any recipients to whom the data processor intends or may wish to disclose the data;
 - (f)* the names, or a description of, any countries or territories outside Barbados to which the data processor directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and
 - (g)* where the data processor is not established in Barbados within the meaning of section 55(6), the name, address and other contact information of the representative nominated pursuant to section 55(3).
- (2) The Register of Data Processors shall be open to inspection at the office of the Commissioner.
- (3) The Commissioner shall ensure that the Register of Data Processors is kept accurate and up to date.

Notification of changes in respect of a data processor

57.(1) 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 in relation to him.

(2) On receiving notification of the data processor under subsection (1) the Commissioner shall make such amendments to the Register of Data Processors as are necessary.

Data Processor

58.(1) Where processing is to be carried out on behalf of a data controller, the data controller shall only use data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Act and ensure the protection of the rights of the data subject.

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

(3) Where there is general written authorisation pursuant to subsection (2), 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 such changes.

(4) Processing by a data processor shall be governed by a written contract between the data processor and the data controller which sets out the following:

- (a) the subject-matter and duration of the processing;
- (b) the nature and purpose of the processing;
- (c) the type of personal data and categories of data subjects;
- (d) the obligations and rights of the data controller.

(5) The contract prepared pursuant to subsection (4) shall also stipulate that the data processor

- (a) processes the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to countries outside of Barbados or an international organisation, unless required to do so by any enactment and in such a case, the data

processor shall inform the data controller of that legal requirement before processing, unless the enactment prohibits such information to be shared on important grounds of public interest;

- (b)* ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c)* takes all measures required pursuant to section 62.
 - (d)* respects the conditions referred to in subsections (2) and (7) for engaging another data processor;
 - (e)* taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights under Part III;
 - (f)* assists the data controller in ensuring compliance with the obligations pursuant to sections 62 to 66 taking into account the nature of processing and the information available to the data processor;
 - (g)* on the determination of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless the enactment requires storage of the personal data;
 - (h)* makes 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, including inspections, conducted by the data controller or another auditor mandated by the data controller.
- (6) Where in relation to subsection (5)(h) an instruction from the data controller to the data processor infringes this Act, the data processor shall immediately inform the data controller.

(7) Where a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller in accordance with subsection (2), the same obligations as set out in the contract between the data controller and the data processor as referred to subsections (5) and (6) shall be imposed on that other data processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Act.

(8) Where that other data processor mentioned in subsection (7) fails to fulfil its data protection obligations, the initial data processor referred to in subsection (7) shall remain fully liable to the data controller for the performance of that other data processor's obligations.

(9) The Commissioner with the approval of the Minister may prescribe standard contractual clauses for the matters referred to in subsections (5) and (7).

(10) Where data processor contravenes this Act determining the purposes and means of processing, the data processor shall be considered to be a data controller in respect of that processing.

Processing under the authority of the data controller or data processor

59.(1) The data processor and any person acting under the authority of the data controller or of the data processor, who has access to personal data, shall not process those data except on instructions from the data controller, unless required to do so by any enactment.

(2) A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

Records of processing activities

60.(1) A data controller and, where applicable, the data controller's representative, shall maintain a record of processing activities under its responsibility and that record shall contain all of the following:

- (a)* the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative and the data privacy officer;
- (b)* the purposes of the processing;
- (c)* a description of the categories of data subjects and of the categories of personal data;
- (d)* the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;
- (e)* where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
- (f)* where possible, the envisaged time limits for erasure of the different categories of data;
- (g)* where possible, a general description of the technical and organisational security measures referred to in section 62(1).

(2) A data processor and, where applicable, the data processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a data controller, which contains:

- (a)* the name and contact details of the data processor or data processors and of each data controller on behalf of whom the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the data privacy officer;

- (b) the categories of processing carried out on behalf of each data controller;
- (c) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
- (d) where possible, a general description of the technical and organisational security measures referred to in section 62(1).

Cooperation with the Commissioner

61. A data controller and the data processor and, where applicable, their representatives, shall cooperate, on request, with the Commissioner in the performance of his tasks.

Security of processing

62.(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the data controller and the data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- (a) the pseudonymisation and encryption of personal data;
- (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;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

(3) The data controller and data processor shall take steps to ensure that any individual acting under the authority of the data controller or the data processor who has access to personal data does not process the personal data except on instructions from the data controller, unless he is required to do so by any enactment.

Notification of a personal data breach to the Commissioner

63.(1) Where there is a personal data breach the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

(2) Where the notification of the personal data breach to the Commissioner is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

(3) The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

(4) The notification of the personal data breach to the Commissioner referred to in subsection (1) shall

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data privacy officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;

- (d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- (5) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- (6) The data controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in order to facilitate the Commissioner in his assessment of the data controller's compliance with this section.

Communication of a personal data breach to the data subject

- 64.(1)** Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.
- (2) The communication to the data subject referred to in subsection (1) shall describe in clear and plain language the nature of the personal data breach and contain the information referred to in paragraphs (b), (c) and (d) of section 63(4).
 - (3) The communication to the data subject referred to in subsection (1) shall not be required where any of the following conditions are met:
 - (a) the data controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
 - (b) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise;

- (c) it would involve disproportionate effort and in such a case, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Data protection impact assessment

65.(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A single assessment pursuant to subsection (1) may address a set of similar processing operations that present similar high risks.

(3) The data controller shall seek the advice of the data privacy officer, where designated, when carrying out a data protection impact assessment.

(4) A data protection impact assessment referred to in subsection (1) shall in particular be required in the case of:

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

(5) The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to subsection (1) and the Commissioner shall publish that list in the *Official Gazette*.

(6) The Commissioner shall establish and make public a list of the kind of processing operations no data protection impact assessment is required and the Commissioner shall publish that list in the *Official Gazette*.

(7) A data protection impact assessment referred to in subsection (1) shall contain

- (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in subsection (1); and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account the rights and legitimate interests of data subjects and other persons concerned.

(8) Where appropriate, the data controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(9) Where necessary, the data controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Prior consultation

66.(1) The data controller shall consult the Commissioner prior to processing where a data protection impact assessment under section 65 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

- (2) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe this Act, in particular where the data controller has insufficiently identified or mitigated the risk, the Commissioner shall, within a period of up to 8 weeks of receipt of the request for consultation, provide written advice to the data controller and, where applicable to the data processor.
- (3) The period mentioned in subsection (2) may be extended by 6 weeks, taking into account the complexity of the intended processing.
- (4) The Commissioner shall inform the data controller and, where applicable, the data processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay.
- (5) The period mentioned in subsection (2) may be suspended until the Commissioner has obtained information he has requested for the purposes of the consultation.
- (6) When consulting the Commissioner pursuant to subsection (1), the data controller shall provide the Commissioner with:
- (a) where applicable, the respective responsibilities of the data controller and data processors involved in the processing, in particular for processing within a group of undertakings;
 - (b) the purposes and means of the intended processing;
 - (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Act;
 - (d) where applicable, the contact details of the data privacy officer;
 - (e) the data protection impact assessment provided for in section 65;
 - (f) any other information requested by the Commissioner.

Designation of the data privacy officer

67.(1) The data controller and the data processor shall designate a data privacy officer in any case where:

- (a)* the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b)* the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c)* the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.
- (2) A group of undertakings may appoint a single data privacy officer provided that a data privacy officer is easily accessible from each establishment.
- (3) Where a data controller or the data processor is a public authority or body, a single data privacy officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
- (4) In cases other than those referred to in subsection (1), the data controller or data processor or associations and other bodies representing categories of data controllers or data processors may designate a data privacy officer.
- (5) The data privacy officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions referred to in section 69.
- (6) The data privacy officer may be a staff member of the data controller or data processor, or fulfil the tasks on the basis of a service contract.
- (7) The data controller or the data processor shall communicate the contact details of the data privacy officer to the Commissioner.

Position of the data privacy officer

68.(1) The data controller and the data processor shall ensure that the data privacy officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 69 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.

(3) The data controller and data processor shall ensure that the data privacy officer does not receive any instructions regarding the exercise of the duties and functions referred to in section 69.

(4) A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69.

(5) A data privacy officer shall report directly to highest management level of a data controller or a data processor.

(6) Data subjects may contact the data privacy officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.

(7) A data privacy officer is required to keep confidential all matters concerning the performance of his duties and functions referred to in section 69.

Duties and functions of a data privacy officer

69.(1) A data privacy officer shall

- (a) inform and advise the data controller or the data processor and the employees who carry out processing of their obligations pursuant to this Act;

- (b) monitor compliance with this Act and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 65;
 - (d) cooperate with the Commissioner;
 - (e) act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in section 66, and to consult, where appropriate, with regard to any other matter.
- (2) A data privacy officer shall in the performance of his duties and functions under this section have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

PART VII

DATA PROTECTION COMMISSIONER

Data Protection Commissioner

70.(1) There shall be a public officer, to be called the Data Protection Commissioner, who shall be responsible for the general administration of this Act.

(2) A person is qualified to hold or to act in the post of Data Protection Commissioner, where that person is qualified to practise as an attorney-at-law and has so practised for a period of not less than 7 years, or for periods amounting in the aggregate to not less than 7 years.

(3) In this section “practise as an attorney-at-law” includes any period during which a person served as an attorney-at-law, advocate, barrister-at-law, solicitor, parliamentary counsel, magistrate or registrar of a court in some part of the Commonwealth, or as a professor or teacher of law at the University of the West Indies or at a school for legal education approved by the Judicial and Legal Service Commission.

Functions of Commissioner

71. Without prejudice to the generality of the functions set out in this Act, 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) organise activities addressed specifically to children to educate them about the risks, rules, safeguards and rights in relation to processing;
- (e) conduct, at his own discretion or where requested to do so by any person, an audit of the personal data processed by the person, for the purpose of ascertaining whether or not the data is processed in accordance with this Act;
- (f) upon request, provide information to any data subject concerning the exercise of their rights under this Act;
- (g) monitor the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data, and
 - (i) report to the Minister on the results of that monitoring; and
 - (ii) where appropriate, make recommendations on the need for, or desirability of, taking legislative, administrative or other action to

give protection or better protection, to the privacy of persons in respect of their personal data;

- (h)* examine any proposed legislation or proposed policy of the Government that
 - (i)* the Commissioner considers may affect the privacy of persons in respect of their personal data; or
 - (ii)* provides for the collection of personal data by any public authority or the disclosure of personal data by one public authority to another public authority,

and report to the Minister the results of that examination;

- (i)* conduct investigations on the application of this Act, including on the basis of information received from a public authority;
- (j)* receive and invite representations from members of the public on any matter affecting the privacy of persons in respect of their personal data;
- (k)* consult and cooperate with other persons concerned with the privacy of persons in respect of their personal data;
- (l)* make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interest of the privacy of persons in respect of their personal data;
- (m)* provide, at his own discretion or where requested to do so, advice to any Minister or public authority on any matter relevant to the operation of this Act;
- (n)* inquire generally into any matter, including any law, practice or procedure, whether governmental or non-governmental, or any technical development, where it appears to the Commissioner that the privacy of persons in respect of their personal data is being or may be infringed thereby;

- (o) undertake research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons in respect of their personal data is minimised, and report to the Minister the results of such research and monitoring;
- (p) report to the Minister on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of persons in respect of their personal data;
- (q) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- (r) prepare appropriate codes of practice for the guidance of persons processing personal data;
- (s) recommend the adoption and development of standard contractual clauses and standard data protection clauses pursuant to this Act;
- (t) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to section 65(5) and (6);
- (u) investigate complaints from persons concerning abuses in the processing of personal data;
- (v) approve binding corporate rules pursuant to section 25;
- (w) keep internal records of contraventions of this Act and of measures taken to address those contravention;
- (x) do anything incidental or conducive to the performance of any of the preceding functions; and
- (y) exercise such other functions as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

Staff

72.(1) There shall be appointed to assist the Commissioner in the discharge of his functions such number of public officers as may be required.

(2) A person appointed pursuant to subsection (1) section is subject to the Commissioner's direction and control in the performance of functions under this Act.

Confidential information

73.(1) The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.

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

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

(b) a duty or obligation imposed by any enactment; or

(c) an international agreement to which Barbados is a party.

(3) A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both.

(4) In this section, "confidential information" means information of any kind and in any form that relates to one or more persons and that is obtained by or on behalf of the Commissioner for the purpose of administering or enforcing this Act or any enactment that the Commissioner has jurisdiction to administer or enforce, or that is prepared from such information, but does not include information that does not directly or indirectly reveal the identity of the person to whom it relates.

Indemnity

74. The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act.

Report

75.(1) The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct.

(2) A copy of the report of the Commissioner referred to in subsection (1) shall be printed and laid before both Houses of Parliament and published in the Official Gazette not later than 3 months from the date of receipt thereof by the Minister.

PART VIII

ENFORCEMENT

Enforcement notice

76.(1) Where the Commissioner is satisfied that a data controller or a data processor has contravened or is contravening this Act, the Commissioner may serve him with a notice, to be referred to as an “enforcement notice” requiring him, to do either or both of the following:

- (a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified; or

- (b) to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing the personal data for a purpose so specified or in a manner so specified, after such time as may be so specified.
- (2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.
- (3) An enforcement notice shall contain
 - (a) a statement of the provision of the Act which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion; and
 - (b) particulars of the right of appeal conferred by section 91.
- (4) Subject to subsections (5) and (6), an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the notice need not be complied with 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 notice a statement to that effect and a statement of his reasons for reaching that conclusion.
- (6) Where subsection (5) applies, the notice shall not require the provisions of the notice to be complied with before the end of the period of 7 days beginning with the day on which the notice is served.

Cancellation of enforcement notice

77.(1) Where the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with this Act, he may cancel or vary the enforcement notice by written notice to the person on whom it was served.

(2) 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 notice on the ground that, by reason of a change of circumstances, all or any of the provisions of the notice need not be complied with in order to ensure compliance with the provisions of this Act to which the notice relates.

Request for assessment

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

(2) On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate, unless he is not supplied with such information as he may reasonably require 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 him to raise a matter of substance;
- (b) any undue delay in making the request; and
- (c) whether or not the person making the request is entitled to make an application under section 10 in respect of the personal data in question.

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

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

- (b) to the extent that he considers appropriate, having regard in particular to any exemption from section 10 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

Information notice

79.(1) Where the Commissioner

- (a) has received a request under section 78 in respect of any processing of personal data; or
- (b) reasonably requires any information for the purpose of determining whether a data controller has complied or is complying with the data protection principles,

he may serve the data controller with a notice, to be referred to as an “information notice”, requiring the data controller to furnish him with specified information relating to the request or to compliance with the provisions of this Act.

(2) An information notice shall contain

- (a) in a case falling within
 - (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
 - (ii) 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
- (b) particulars of the right of appeal conferred by section 91.

(3) The Commissioner may specify in an information notice

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

- (b) the period within which, or the time and place at which, the information must be furnished.
- (4) Subject to subsection (5), a period specified in an information notice under subsection (3)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the information need not be furnished 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, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event subsection (4) shall not apply, but the notice shall not require the information to be furnished before the end of the period of 7 days beginning with the day on which the notice is served.
- (6) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of

 - (a) any communication between a professional legal adviser 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
 - (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any 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 such proceedings.
- (7) In subsection (6) references to the client of a professional legal adviser includes references to any person representing such a client.
- (8) A person shall not be required by virtue of this section to furnish the Commissioner with any information where the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence of perjury, expose that person to proceedings for that offence.

(9) Any 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, other than an offence under section 83, unless in the proceedings

- (a) in giving evidence the person provides information that is inconsistent with it; and
- (b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(10) The Commissioner may cancel an information notice by written notice to the person on whom it was served.

(11) This section has effect subject to section 82(3).

(12) In subsection (1) "specified information" means information

- (a) specified or described in the information notice; or
- (b) falling within a category which is specified or described in the information notice.

(13) In subsection (9), "relevant statement", in relation to a requirement under this section, means

- (a) an oral statement; or
- (b) a written statement made for the purposes of the requirement.

Special information notice

80.(1) Where the Commissioner

- (a) receives a request under section 78 in respect of any processing of personal data; or

- (b) has reasonable grounds for suspecting that, in a case in which proceedings have been stayed under section 34, the personal data to which the proceedings relate
 - (i) is not being processed only for the purposes of journalism or for artistic or literary purposes; or
 - (ii) is not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may serve the data controller with a notice, referred to as a “special information notice”, requiring the data controller to furnish him with specified information for the purpose specified in subsection (2).

(2) The purpose referred to in subsection (1) is the purpose of ascertaining whether personal data is being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; or
- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.

(3) A special information notice must contain

- (a) particulars of the right of appeal conferred by section 91; and
- (b) in a case falling within
 - (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
 - (ii) subsection (1)(b), a statement of the Commissioner’s grounds for suspecting that the personal data is not being processed as mentioned in that paragraph.

- (4) The Commissioner may also specify in the special information notice
- (a) the form in which the information must be furnished; and
 - (b) the period within which, or the time and place at which, the information must be furnished.
- (5) Subject to subsection (6), a period specified in a special information notice under subsection (4)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.
- (6) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event subsection (5) shall not apply, but the notice shall not require the information to be furnished before the end of the period of 7 days beginning with the day on which the notice is served.
- (7) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of
- (a) any communication between a professional legal adviser 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
 - (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any 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 such proceedings.
- (8) In subsection (7) a reference to the client of a professional legal adviser include a reference to any person representing such a client.
- (9) A person shall not be required by virtue of this section to furnish the Commissioner with any information where the furnishing of that information

would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence of perjury, expose him to proceedings for that offence.

(10) Any 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 any offence under this Act, other than an offence under section 83, unless in the proceedings

- (a) in giving evidence the person provides information inconsistent with it; and
- (b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(11) In subsection (10)“relevant statement”, in relation to a requirement under this section, means

- (a) an oral statement; or
- (b) a written statement made for the purposes of the requirement.

(12) The Commissioner may cancel a special information notice by written notice to the person on whom it was served.

(13) In subsection (1)“specified information”means information

- (a) specified, or described, in the special information notice; or
- (b) falling within a category which is specified, or described, in the special information notice.

Determination by Commissioner as to the purposes of journalism or artistic or literary purposes

81.(1) Where at any time it appears to the Commissioner, whether as a result of the service of a special information notice or otherwise, that any personal data is not being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; or
- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may make a determination in writing to that effect.

(2) Notice of the determination shall be given to the data controller; and the notice must contain particulars of the right of appeal conferred by section 91.

(3) A determination under subsection (1) shall not take effect until the end of the period within which an appeal can be brought and, where an appeal is brought, shall not take effect pending the determination or withdrawal of the appeal.

Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes

82.(1) The Commissioner may not serve an enforcement notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless

- (a) a determination under section 81(1) with respect to those 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

- (a) that the Commissioner has reason to suspect a contravention of the data protection principles which is of substantial public importance; and
- (b) except where the case is one of urgency, that the data controller has been given notice, in accordance with rules of court, of the application for leave.

(3) The Commissioner may not serve an information notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless a determination under section 81(1) with respect to those data has taken effect.

Failure to comply with notice

83.(1) A person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence and is liable on summary conviction to a fine of \$15 000 or to a term of imprisonment of 6 months.

- (2) A person who, in purported compliance with an information notice
- (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,

is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

(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.

Service of notice by Commissioner

84.(1) Any notice authorised or required by this Act to be served on or given to any person by the Commissioner may where the person is

- (a) an individual, be served on him by
 - (i) delivering it to him;
 - (ii) sending it to him by post addressed to him at his usual or last known place of residence or business; or
 - (iii) leaving it for him at that place; or
- (b) a body corporate or partnership, be served on it by
 - (i) sending it by post to the proper officer of the company at its principal office; or
 - (ii) addressing it to the proper officer of the partnership and leaving it at the office of the proper officer.

(2) This section is without prejudice to any other lawful method of serving or giving a notice.

(3) Nothing in subsections (1) and (2) precludes the service of a notice by electronic means.

Warrants

85.(1) Where a judge is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting that

- (a) a data controller or a data processor has contravened or is contravening Parts II, III or IV; 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 any premises specified by the Commissioner,

the Judge may issue a warrant.

(2) A warrant issued, under subsection (1), shall authorise a police officer accompanied by the Commissioner, staff or such other person skilled in information technology as the police officer may deem necessary for the purpose, within 7 days of the date of the warrant, to

- (a) enter the premises;
- (b) search the premises;
- (c) inspect, examine, operate and test any 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 any person on the premises to provide
 - (i) an explanation of any document or other material found on the premises;
 - (ii) such other information as may reasonably be required for the purpose of determining whether the data controller has contravened or is contravening Parts II, III or IV.

(3) A judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect.

Execution of warrants

86.(1) A police officer executing a warrant may use such reasonable force as may be necessary.

(2) Where the person who occupies the premises in respect of which a warrant is issued is present when the warrant is executed, he shall be shown the warrant

and supplied with a copy of it and where the person is not present, a copy of the warrant shall be left in a prominent place on the premises.

(3) A police officer seizing anything in pursuance of a warrant shall make a list of any items seized with the date and time of the seizure and shall give the list to

- (a) the data controller; or
- (b) the occupier of the premises.

Matters exempt from inspection and seizure

87.(1) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of personal data which, by virtue of section 30, is exempt from any of the provisions of this Act.

(2) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of any communication between

- (a) a professional legal adviser 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
- (b) a professional legal adviser and his client, or between such an adviser or his client and any 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 those proceedings.

Return of warrants

88. A warrant shall be returned to the court from which it was issued

- (a) after being executed; or
- (b) where not executed within the time authorised for its execution;

and the police officer by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him under the warrant.

Obstruction of execution of a warrant

89. Any person who

- (a) intentionally obstructs a person in the execution of a warrant;
- (b) fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant;
- (c) makes a statement in response to a requirement under section 85(2)(e) which that person knows to be false in a material respect; or
- (d) recklessly makes a statement in response to a requirement under section 85(2)(e) which is false in a material respect,

is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 2 years or to both.

PART IX

DATA PROTECTION TRIBUNAL

Establishment of the Data Protection Tribunal

- 90.(1)** There is established a tribunal called the Data Protection Tribunal.
- (2) The *Schedule* has the effect as to the constitution of Tribunal and otherwise in relation to the Tribunal.

Right of appeal

91.(1) A person on whom an enforcement notice, an information notice or a special information notice has been served may appeal to the Tribunal against the notice.

(2) A person on whom an enforcement notice has been served may appeal to the Tribunal against the refusal of an application under 77(2) for cancellation or variation of the notice.

(3) Where an enforcement notice, an information notice or a special information notice contains a statement by the Commissioner in accordance with section 76(3), section 79(5) or 80(6) then, whether or not the person appeals against the notice, he may appeal against

- (a) the Commissioner's decision to include the statement in the notice; or
- (b) the effect of the inclusion of the statement in respect of any part of the notice.

(4) A data controller in respect of whom a determination has been made under section 81 may appeal to the Tribunal against the determination.

(5) A person on whom an order has been made pursuant to under section 94 may appeal to the Tribunal against that order.

Determination of appeals

92.(1) Where on an appeal under section 91(1) the Tribunal considers

- (a) that the notice against which the appeal is brought is not in accordance with this Act or any regulations made thereunder; or
- (b) to the extent that the notice involved an exercise of discretion by the Commissioner, and it is determined that the Commissioner ought to have exercised his discretion differently,

the Tribunal shall allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner and in any other case the Tribunal shall dismiss the appeal.

(2) Upon appeal pursuant to subsection (1), the Tribunal may review any determination of fact on which the notice in question was based.

(3) Where on an appeal under 91(2) the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal shall cancel or vary the notice.

(4) On an appeal under 91(3) the Tribunal may direct

(a) that the notice in question shall have effect as if it did not contain any such statement as is mentioned in that subsection; or

(b) that the inclusion of the statement in accordance with section 76(3), section 79(5) or 80(6) shall not have effect in relation to any part of the notice, and may make such modifications in the notice as may be required for giving effect to the direction.

(5) On an appeal under section 91(4), the Tribunal may cancel the determination of the Commissioner.

(6) Any party to an appeal to the Tribunal under section 91 may appeal from the decision of the Tribunal on a point of law to the High Court.

PART X

MISCELLANEOUS

Unlawful obtaining of personal data

93.(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 shows that

- (a)* the obtaining, disclosing or procuring
 - (i)* was necessary for the purpose of preventing or detecting crime; or
 - (ii)* was required or authorised by or under any enactment, by any rule of law or by the order of a court;
- (b)* he acted in the reasonable belief that he had in law, the right to obtain or disclose the data or information or, as the case may be, 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), is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 6 months or to both.

(4) A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

(5) A person who offers to sell personal data is guilty of an offence where

(a) he has obtained the data in contravention of subsection (1); or

(b) he subsequently obtains the data in contravention of subsection (1)

and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

Administrative penalty

94.(1) Where the Commissioner after a hearing determines that a person has contravened section 52(1), section 57(1) and sections 60 to 67 and the Commissioner considers it to be in the public interest to make an order, the Commissioner may order the person to pay to the Crown a penalty of an amount not exceeding \$50 000.

(2) In addition to the public interest, where the Commissioner seeks to make an order pursuant to subsection (1), he shall have due regard to the following:

(a) the nature, gravity and duration of the contravention taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the contravention;

(c) any action taken by the data controller or data processor to mitigate the damage suffered by data subjects;

(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, in particular whether, and if so to what extent, the data controller or data processor notified the contravention; and
 - (h) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.
- (3) Where the Commissioner makes an order under subsection (1) the Commissioner shall file in the registry of the Court a copy of the order certified by the Commissioner, and on being filed the order shall have the same force and effect, and all proceedings may be taken on it, as if it were a judgment of the court, unless an appeal has been filed pursuant to section 91.
- (4) A penalty imposed by the Commissioner in the exercise of his powers under this Act shall be payable into the general revenue and may be recovered by the Crown as a civil debt and for the purposes of the proof of such debt a certificate under the hand of the Commissioner shall be receivable in evidence as sufficient proof of such debt.
- (5) A person aggrieved by an order made by the Commissioner pursuant to subsection (1) may appeal to the Tribunal within 28 days of the date of the order.

Disclosure of information

95. No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the Tribunal with any information necessary for the discharge of their functions under this Act.

Act binds Crown

96. This Act binds the Crown.

Amendment of *Schedule*

97. The Minister may by Order amend the *Schedule*.

Regulations

98. The Minister may make Regulations generally for the purposes of giving effect to this Act.

Commencement

99. This Act comes into operation on a date to be fixed by proclamation.

SCHEDULE

(Section 90)

Data Protection Tribunal

Constitution

Members of the Tribunal

1.(1) The members of the Tribunal shall be appointed by the Minister by instrument in writing from among persons who appear to him to be qualified as having had experience of, and shown capacity in, matters relating to data protection and privacy or such other related discipline.

(2) The Tribunal shall comprise 5 members who shall be appointed by the Minister.

(3) At least one of the members of the Tribunal shall be an attorney-at-law of at least 10 years standing, and he shall be the Chairman of the Tribunal.

(4) The members of the Tribunal shall hold office for such period not exceeding 3 years as the Minister may specify in the instrument of appointment.

(5) The Minister shall appoint a person appearing to him to have the qualifications necessary for appointment under paragraph 1(3) to act temporarily in the place of the Chairman where the Chairman is absent or unable to perform his functions.

Resignation

2. A member of the Tribunal may at any time resign his office by instrument in writing addressed to the Minister and such resignation shall take effect from the date of the receipt by the Minister of that instrument.

Revocation of appointments

3. The Minister shall revoke the appointment of any member of the Tribunal where that member

- (a) fails to carry out any of the functions conferred or imposed on him under this Act;
- (b) becomes of unsound mind or becomes permanently unable to perform his functions by reason of ill health;
- (c) becomes bankrupt or compounds with, or suspends payment to, his creditors;
- (d) is convicted and sentenced to a term of imprisonment or to death; or
- (e) is convicted of any offence involving dishonesty.

Gazetting appointments

4. The appointment, removal or resignation of a member of the Tribunal shall be recorded in the *Official Gazette*.

Protection of the members of the Tribunal

5. No action, suit, prosecution or other proceedings shall be brought or instituted personally against a member of the Tribunal in respect of any act done in good faith in pursuance of their functions under this Act.

Remuneration of the members of the Tribunal

6. There shall be paid to the members of the Tribunal such remuneration and other such allowances as the Minister may determine.

Read three times and passed the House of Assembly this
day of _____, 2019.

Speaker

Read three times and passed the Senate this _____ day of
, 2019.

President

**PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2018 – 2023)**

**JOINT SELECT COMMITTEE
ON THE
DATA PROTECTION BILL, 2019**

Minutes of the First Meeting of the Joint Select Committee on the Data Protection Bill, 2019 held in the Senate Chamber, Parliament Buildings, Bridgetown on Monday, June 24th, 2019 at 2:00 p.m.

PRESENT WERE:

Senator the Hon. Miss Kay S. McConney (Chairman)

Hon. Dale D. Marshall, Q.C, M.P.

Hon. Dwight G. Sutherland, M.P

Mr. Neil G. H. Rowe, M.P.

Senator Damien R. Sands

Senator Rawdon J. H. Adams

Senator Miss Crystal N. Drakes

Senator Kevin J. Boyce

Senator Ms. Alpheia M. Wiggins

ABSENT WERE:

Hon. Ms. C. Sandra V. Husbands, M.P.

Bishop Joseph J. S Atherley, J.P., M.P.



IN ATTENDANCE WERE:

Hon. Miss Cynthia Y. Forde, J.P., M.P.

Mr. Pedro Eastmond, Clerk of Parliament

Mr. Nigel Jones, Deputy Clerk of Parliament

Ms. Beverley S. Gibbons, Deputy Clerk of Parliament

Miss Suzanne Hamblin, (Library Assistant) Procedural Officer to the Committee (Ag.)

Ms. Shawn Belle, Senior Parliamentary Counsel, Chief Parliamentary Counsel Office

Item 1: Appointment of Chairman

The Clerk called the meeting to order at 2:25 p.m. and apologised for the late start. He stated that the first order of business would be to appoint a Chairman.

On the motion of Hon. Dale D. Marshall, seconded by Senator Rawdon J. H. Adams, Senator the Hon. Miss Kay S. McConney was appointed Chairman.

Senator the Hon. Miss Kay S. McConney assumed the Chair.

Item 2: Welcome

On the motion of Senator Ms. Alpheia M. Wiggins, seconded by Hon. Dale D. Marshall the amended Agenda was adopted.

Madam Chairman welcomed everyone and informed the Committee that the Data Protection Bill, 2019 was designed to regulate the collection, keeping, processing, use and dissemination of personal data. She cited the terms of reference:

1. To inquire into and determine whether the Bill as drafted effectively fulfils the expressed objects of improving the protection of personal data;
2. To examine whether the Bill as drafted would upon effective implementation contribute to an ethos of compliance with data protection; thereby promoting transparency and accountability; and
3. To make recommended changes, if deemed necessary, to the Bill as drafted for further consideration by the Chief Parliamentary Counsel.

Item 3: Quorum

The Chair recommended that five (5) persons constitute a quorum for meetings of the Joint Select Committee.

There was no objection, and on the motion of Senator Damien R. Sands, seconded by Senator Miss Crystal N. Drakes the quorum was set at five (5).

Item 4: Technical Support

Madam Chairman informed the meeting that the technical support would be provided by Ms. Shawn Belle, Senior Parliamentary Counsel, Chief Parliamentary Counsel Office.

Item 5: Procedure

Madam Chairman proposed that the Committee conclude its work, and report to the Honourable the Senate by Wednesday, July 10th, 2019 and further that the Bill be submitted to the Honourable the House of Assembly by Tuesday, July 23rd, 2019. She noted that the deadline for the submissions to the Committee was Thursday, June 20th, 2019 and so far Parliament had received five (5). There was an additional request from Ms. Anne Reid to submit a written submission.

On the motion of Senator Ms. Alpheia M. Wiggins, seconded by Senator Kevin J. Boyce the deadline was extended to Thursday, June 27th, 2019.

It was agreed that the oral presentations would begin at the next scheduled meeting on Wednesday, June 26th, 2019 at 10:00 am. After lunch, consideration would be given to the written submissions.

Madam Chairman proposed that the Committee meet again on Monday, July 1st, 2019 to consider the subsequent submissions received by the new deadline. It was agreed that the proceedings would be streamed.

Madam Chairman stated that each presentation would be ten (10) minutes long and followed up with a fifteen (15) to twenty (20) minutes question and answer segment.

It was agreed that the Clerk of Parliament would invite the Barbados Bankers' Association Inc., The Barbados Association of Medical Practitioners and the Barbados Bar Association to submit submissions.

Ms. Shawn Belle informed the Committee that comments were received from the Barbados ICT Professionals Association (BIPA), the Barbados Chapter of Information Systems Security Association (BISSA) and ISOC Barbados -- the Barbados Chapter of the Internet Society.

On the motion of Senator Damien R. Sands, seconded by Senator Kevin J. Boyce the procedures were adopted.

Item 6: Presentations

Madam Chairman outlined the three (3) presentations:-

1. "An overview of the Data Protection Bill, 2019" by Mr. Chesterfield Coppin, E-Commerce Development Officer;
2. "Provisions of the Data Protection Bill, 2019" by Ms. Shawn Belle, Senior Parliamentary Counsel; and

3. "Best Practices in Data Protection" by Mr. Steve Clarke, Advisory Partner, Deloitte.

Madam Chairman invited the presenters to join the meeting and introduced Mr. Charlie Browne, Permanent Secretary, Ministry of Innovation, Science and Smart Technology to the Committee.

It was agreed by the Committee to switch the order of the presentations so that the order of appearance would be Ms. Shawn Belle, Mr. Steve Clarke and then Mr. Chesterfield Coppin.

Ms. Shawn Belle, Senior Parliamentary Counsel presented on the "Provisions of the Data Protection Bill, 2019" (Transcript follows).

Senator Rawdon J. H. Adams queried the adjustment made in the General Data Protection Regulations (GDPR) between the powers that sit with the Controller and the Processor. Ms. Belle stated that the Data Processor was regulated a bit more in terms of registration and it was felt in the GDPR that they should be regulated a bit more.

Mr. Steve Clarke presented on the "Best Practices in Data Protection" (Transcript follows).

Senator Rawdon J. H. Adams queried whether there was a split in the capacity of firms to respect the legislation as a function of their size, whether they were small, medium or large? Mr. Clarke answered in the affirmative but stated that the smaller entities seemed to be experiencing a problem as they tend to outsource the DPO but believed that persons were missing the regulations from a GDPR perspective.

Senator Rawdon J. H. Adams followed up by querying whether there was any sort of data around as to how financially onerous the legislation has proven, for example, as a percentage of total operating costs?

Mr. Steve Clarke responded that the breaches and penalties which have occurred have been by extremely large organisations such as Facebook and

Amazon. Even though the penalties were onerous and quite large they looked to see if they were actively doing something to mitigate the breaches.

Mr. Chesterfield Coppin presented on "An overview of the Data Protection Bill, 2019" (Transcript follows).

Item 7: **ADJOURNMENT**

On the motion of Hon. Dale D. Marshall, seconded by Senator Rawdon J. H. Adams the meeting was adjourned to Wednesday, June 26th, 2019 at 10:00 a.m.

There being no other business Madam Chairman adjourned the meeting accordingly at 4:00 p.m.


Beverley S. Gibbons
Deputy Clerk of Parliament

Confirmed this 1st day of July 2019.


Chairman

C

**PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2018 – 2023)**

**JOINT SELECT COMMITTEE
ON THE
DATA PROTECTION BILL, 2019**

Minutes of the Second Meeting of the Joint Select Committee on the Data Protection Bill, 2019 held in the Senate Chamber, Parliament Buildings, Bridgetown on Wednesday, June 26th, 2019 at 10:00am.

PRESENT WERE:

Senator the Hon. Miss Kay S. McConney (Chairman)

Hon. Dale D. Marshall, Q.C, M.P.

Bishop Joseph J. S. Atherley, J.P., M.P

Hon. Ms. C. Sandra V. Husbands, M.P.

Hon. Dwight G. Sutherland, M.P.

Senator Rawdon J. H. Adams

Senator Miss Alpheia M. Wiggins

Senator Kevin J. Boyce

Senator Miss Crystal. N. Drakes

Senator Damien R. Sands

ABSENT WERE:

Mr. Neil G. H. Rowe, M.P

IN ATTENDANCE WERE:

Mr. Pedro E. Eastmond, Clerk of Parliament

Mr. Nigel R. Jones, Deputy Clerk of Parliament

Ms. Beverley S. Gibbons, Deputy Clerk of Parliament

Miss Shawn Belle, Senior Parliamentary Counsel, Chief Parliamentary Counsel

Mr. Chesterfield Coppin, E-Commerce Development Officer, Ministry of Small Business, Entrepreneurship and Commerce

Miss Suzanne Hamblin, (Library Assistant) Procedural Officer to the Committee (Ag.)

Item 1: Welcome

Madam Chairman called the meeting to order at 10:32 a.m. and welcomed those present. She recognised that there were five (5) members present which constituted a quorum.

Item 2: Minutes

On the motion of Senator Kevin J. Boyce, seconded by Miss C.N. Drakes, the Minutes of the Meeting held on Monday, June 24th, 2019 at 2:00 p.m. were deferred.

Item 3: Matters Arising

There were no matters arising since the Minutes were deferred.

Item 4: Oral Submissions

Madam Chairman expressed that there were five (5) requests for oral presentations for this session. However, one presenter was absent and as such they would be four (4).

Madam Chairman reiterated the agreed procedures set at the First Meeting of the Committee for the oral presentations and asked the Committee to permit Mr. Chesterfield Coppin to sit as a technical resource person as part of the Committee. The Committee unanimously agreed.

Madam Chairman stated that the Parliamentary team had reached out to the Barbados Bar Association and the Barbados Bankers' Association Inc. and would consider their written submissions on Monday, July 1st, 2019.

Madam Chairman acknowledged the presence of the presenters, informed them of the presentation procedures, and that the meeting was being streamed live.

1. Miss Cynthia Wiggins

Ms. Cynthia Wiggins identified herself as a small business owner (transcript follows).

On conclusion, Ms. Wiggins said that she would provide the Committee with the written submissions through the Clerk of Parliament.

2. **Mr. Antonio Hollingsworth – Bajan Digital Creation Inc.** (transcript follows).
3. **Mr. Bartlett Morgan – Senior Associate, Lex Caribbean** (transcript follows)

On conclusion, Mr. Morgan promised to submit the written submission to the Committee by Thursday, June 27th, 2019.

Madam Chairman informed the Committee that the fourth presenter was no longer presenting.

SUSPENSION

On the motion of Senator Kevin J. Boyce, seconded by Senator Miss Crystal N. Drakes the meeting was suspended for fifteen (15) minutes.

At 11:50 a.m. Madam Chairman suspended the meeting.

RESUMPTION

Madam Chairman resumed the Chair and called the meeting back to order at 12:05 p.m.

Item 5: Consideration of Written Submissions

Madam Chairman proposed to the Committee to proceed by examining critical recommendations, then conducting discussions on such recommendations to determine whether they would impact the Bill. The Committee agreed to this proposal.

1. Soledad González, Business Developer for Latin America – Quidgest

Madam Chairman stated that this submission was to be deferred or disregarded as it was not in accordance with the Terms of Reference of the Committee.

On the motion of Hon. Ms. C. Sandra V. Husbands, M.P., seconded by Senator Rawdon J. H. Adams, the submission was disregarded.

2. Mr. S. Antonio Hollingsworth, Bajan Digital Creations Inc.

Madam Chairman proceeded to point number 2, page 4. The recommendation was to reduce the requirements of the Data Controller to fall within the established Article VI of the Electronic Transaction Act. The Committee agreed that there would be no adjustments to the requirement for the Data Controller as it had no impact on the Bill. However, there would be a proclamation to get the Data Protection Commissioner and the regulatory

framework in place ahead of time for guidance. Also, consideration should be given to the treatment regarding small businesses.

Madam Chairman examined point number 3, page 5. The recommendation was that the registration and certification of the data controller be phased over a period of three years from enactment. The Committee agreed that there was no need to address this as it had no impact on the Bill.

Madam Chairman moved on to point number 4, page 5. The recommendation was to clarify the term "*in writing*" as it relates to the Electronic Filing Act. The Committee agreed that this recommendation was irrelevant to the Bill as it was not considered as part of the Terms of Reference.

Madam Chairman examined point number 5, page 5. The recommendation was that the definition of "*profiling*" is not in sync with current technology trends. The Committee agreed that since the definition was informed from Article IV, 4 of the General Data Protection Regulations (GDPR), there was no need to make any adjustments.

Madam Chairman proceeded to point number 6, page 5. The recommendation was that there is no pressing justification for sensitive data as defined by this Bill to be legitimately processed by political, religious or philosophical bodies, given that the Bill itself gives the data subject the right to migrate their data from one data controller to another. Also, that sensitive data should only be processed by persons who fall under implied or explicit

confidentiality. Ms. Shawn Belle informed the Committee that its construction was informed by the GDPR and as such the Committee agreed that “*Clause 9*” would not change.

Madam Chairman moved on to point number 7, page 6. The recommendation was that the term “*Automated decision*” be clearly defined. It was agreed by the Committee that the definition was informed by reference to the GDPR and should not change.

Madam Chairman made reference to point number 1, page 4. The recommendation was to clarify in this Bill how [it] relates to or supersedes Article VI of the Electronic Transaction Act. Ms. Shawn Belle informed the Committee that the Electronic Transactions Act and the Electronic Filing Act were two (2) separate Acts. The Committee agreed that this recommendation had not impact on the Bill.

Madam Chairman concluded that the recommendations particularly with respect to public education would be taken on board for some consideration. Additionally, the models identified by Mr. Chesterfield Coppin previously to treat to the micro, small and medium enterprises would be considered as well as.

SUSPENSION

On the motion of Senator Kevin J. Boyce, seconded by Senator Miss Crystal N. Drakes the meeting was suspended for lunch until 2:30 p.m.

At 1:20 p.m. Madam Chairman suspended the meeting.

RESUMPTION

Madam Chairman resumed the Chair and called the meeting back to order at 2:30 p.m.

3. The Barbados International Business Association (BIPA)

Madam Chairman outlined the three (3) major recommendations which were put forward for consideration.

1. Reference: Part I, Clause 2, page 13: *“data processor” means any person, other than an employee of a data controller, who processes personal data on behalf of the “data controller”*. The recommendation was that consideration be given to the incorporation and recognition of cognitive technologies. Ms. Shawn Belle informed the meeting that the definition of *“data processor”* was informed by Article IV of the GDPR. The Committee agreed that they would allow the definition to stand as it is without the incorporation of the cognitive technologies.

2. Reference: PART VI, Clause 50(2), page 59: *“A person who desires to operate as a data controller may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose”*. It was recommended that a local agency be set up

to provide shared services to micro, small and medium enterprises to implement data protection requirement. Madam Chairman stated that there was no need for it to be placed in the legislation at this point in time and therefore it should be a consideration but not to be incorporated into the legislation.

However, the Committee was informed by Mr. Chesterfield Coppin that there was representation by the Small Business community and all the stakeholders with regards to the drafting of the legislation.

Madam Chairman pointed out going forward that the constituted Committee, once they had made the decision, stakeholder groups would be engaged as they start moving towards implementation. She stated that there was a need to encourage the private sector to take it up as a business opportunity, rather than Government do it all at this stage.

3. Reference: PART IV, Clause 59(2) page 66: *“A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both”*. The recommendation was that to use a percentage of income versus a fixed sum as it related to penalties. Madam Chairman suggested to the Committee that this recommendation be taken under further consideration and returned to the Committee at the next meeting before the Report is concluded.

4. Mr. Shannon Clarke

Madam Chairman directed the meeting to the heading *“Suggestions for improving the Bill”*.

1. The requirements for compliance for businesses should match the level of access that company has to customer’s private information such that a company that deals with sensitive information.” The Committee agreed that this suggestion did not impact the Bill.

2. The fines should be adjusted to be a percentage of the gross revenue of the company in order to address the fact that large service providers have the most access to private data and would not be deterred by a BBD\$500 000 fine. However, a small business may indeed be crippled by such. The Committee agreed that they would stand by the original decision made with regard to the fines.

3. The enactment of the Data Protection Bill needs to be delayed or an interim period established until the measures of the enforcement have been adequately clarified prior to the enforcement. Madam Chairman reiterated that the Bill could be proclaimed at any time and it was agreed that this suggestion had no impact on the Bill.

4. A public education campaign is necessary in order to sensitise the public of their data privacy rights. The Committee agreed that this suggestion did not relate to the Terms of Reference but consideration would be given to it. However, it had no further impact on the Bill.

5. Business training sessions are necessary to educate and prepare the small and medium-sized businesses who are highly at risk of non-compliance. As per the GDPR, businesses should be required to adhere to established Codes of Conduct. The Bill should refer to the establishment of Codes of Conduct *via* consultation with the local business sector. The Committee agreed that this suggestion does not relate to the Terms of Reference but consideration would be given to it. However, it had no further impact on the Bill.

5. Solutions Barbados

1. **Preamble (Page 11):** Grammatical errors are common throughout the document. While a common-sense read of the Bill appears to allow it to be understood as intended, the errors should be cleaned up in the final version. We have identified some of the most glaring errors. *“provide for provide for matters”* should read *“provide for matters”*. Madam Chairman believed that these basic errors would be corrected.

2. **Clause 9.1(e)(iii) (Page 25):** The non-consent processing of sensitive information by political parties, trade unions, or other groups is allowed, once the data belongs to their members. They proposed that this should not be allowed. The Committee agreed that the Attorney-General had provided clarification on this previously and as such it had no impact on the Bill.

3. **Clause 10.3 (Page 28):** *“The data controller shall provide a copy of the personal data undergoing processing to the data subject”*. Madam Chairman mentioned that their concern was that when it got to the point where the data controller had reasonable doubts. She stated that Clause 21 suggested that they

may request the provision of additional information necessary to confirm the identity of the subject. Her understanding was that this provision was put to give the controller flexibility in terms of confirming identity. The Committee agreed that that flexibility should remain for the data controller and therefore this recommendation had no impact on the Bill.

4. **Clause 15.3 (Page 31):** *“In exercising his or her right to data portability”*. They proposed that the gender references should be consistent. Madam Chairman stated that their concern was that there were gender references – one part of the Bill dealt with *“his”* and some said *“hers”*. The Committee agreed that there should be consistency and would seek to have that consistency throughout the Bill.

5. **Clause 22 (Page 40):** *“Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.”* Madam Chairman stated that they were asking for a further definition of *“adequate”* and *“appropriate safeguards”*. They further proposed that for the avoidance of doubt, a schedule containing an approved list of countries, or a negative list of countries, should be part of the legislation. The Committee was in consensus that these recommendations had no impact on the Bill as drafted.

6. **Clause 50.4 (Page 59):** *“A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.”* They raised the question that a data controller is anyone who is responsible for processing data, which can include every employer and educational institution and this needs clarification. Ms. Shawn Belle clarified to the meeting that *“a person”* applied to legal and natural persons and also applicable to every employer. The Committee agreed that was an inclusive Bill and should not change.

7. **Clause 55.1 (Page 62):** *“A person shall not operate as a data processor unless he is registered in the Register of Data Processors”.* They raised the question that if there is no separate Registration Act for the new profession, should it then be included in the Profession, Trade and Business Registration Act (Cap. 373), like other professions? Madam Chairman informed the meeting that a new profession was not being created and that was not the intention of the Bill. Ms. Shawn Belle clarified that the nature of the person’s activities would dictate whether they are a processor or a controller which would justify their registration requirements under the Bill. Therefore, there would be no need to refer to or go under the Profession Trade and Business Registration Act.

8. **Clause 55.4 (Page 62):** *“A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.”* The Profession, Trade and Business Registration Act specifies a

penalty of \$500 and no imprisonment for this offence. The Committee agreed that this was null and void because no professions were created and that it was not relevant to the Bill.

9. **Clause 68(3) and (4) (Page 75):** *“The data controller and data processor shall ensure that the data privacy officer does not receive any instructions regarding the exercise of the duties and functions referred to in section 69.” and “A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69.”*

Madam Chairman disagreed with the concern that it was making the data privacy officer the Commissioner’s spy but paid for and maintained by a company. She stated that the data controller would designate their own privacy officers and that they would facilitate core operations in the data subject’s interest. The Committee agreed that this comment re Clause 68(3) did not have any impact on the Bill.

10. **Clause 73.1 (Page 80):** *“The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.”* Their contention was that the last sentence appears to be a glaring loophole for mischief. If the Commissioner instructs his employee to release someone’s personal information to one of their competitors, then while it is clearly unethical,

this clause appears to make it legal. Ms. Shawn Belle explained that this was a very common provision as it relates to functionaries. The Commissioner has to take everything into account and he if does not he can be challenged and disciplined under the Public Service Act because he is a public officer. The Committee agreed that this submission had no impact on the Bill as drafted.

11. **Clause 73.3 (Page 80):** *"A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both."* They suggested that for releasing someone's personal information to one of their competitors, the fine should be a minimum of \$500 000. The Committee agreed that the law does not allow for a minimum penalty and that this recommendation had no impact on the Bill.

12. **Clause 74 (Page 81):** *"The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act."* They suggested that this loophole seems to excuse professional negligence. Madam Chairman explained that the idea of *"in good faith"* is the measuring stick and where that officer would act outside of good faith then they would be subject to the Public Service Act. The Committee agreed that this recommendation had no impact on the Bill as drafted.

13. **Clause 75.1 (Page 81):** *"The Commissioner shall, not later than 3 months after the end of each financial year submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct."* They queried whether there was any penalty for not submitting the report within 3 months? Madam Chairman reiterated that the Commissioner would be subject to the Public Service Act with regard to not executing their duties. The Committee agreed that this recommendation had no impact on the Bill.

14. **Clause 79.1 (Page 84):** Grammatical error. *"... requiring the data controller to furnishhim with ..."* should read: *"requiring the data controller to furnish him with ..."* Madam Chairman stated that this was a typo and typos would be fixed in the final Bill.

15. **Clause 85.2(d) (Page 93):** *"inspect and seize any documents or other material found on the premises;"* Their contention was that copies of documents may be seized, but the person should be allowed to make copies if the material seized is unrelated to the charge, and is part of his business, but belonging to another client. Madam Chairman stated that this recommendation was taken within the context of a warrant having been issued by a Judge. The Committee agreed that this recommendation had no impact on the Bill as drafted.

16. **Clause 85.3 (Page 93):** *"A judge shall not issue a warrant in respect of any personal data processed for the purpose of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect."* They queried what about educational

institutions processing student records? Ms. Shawn Belle explained that this provision would not apply to educational purposes. The Committee agreed that this recommendation had no impact on the Bill.

17. **Clause 89(b) (Page 95):** *“Any person who fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant; is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or a term of imprisonment of 2 years or to both.”* Their concern was that if the person fails to help a police officer with a ladder, while that officer wants to search an elevated part of the property, is the person guilty of obstruction? Committee agreed that this query was not a consideration for the Terms of Reference of the Bill.

18. **Clause 93.3 (Page 98):** *“A person who, contravenes subsection (1), is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 6 months or to both.”;*

19. **Clause 93.4:** *“A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both”; and*

20: **Clause 93.5:** *“A person who offers to sell personal data is guilty of an offence where he has obtained the data in contravention of subsection (1); or he subsequently obtains the data in contravention of subsection (1) and is liable on*

summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both. The Committee agreed that they would keep the existing levels within the Bill and then revisit at a later stage.

Madam Chairman informed the meeting that The Barbados Bankers' Association Inc. had submitted their written submissions. The Parliamentary team were awaiting a response from the Barbados Bar Association and the Barbados Association of Medical Practitioners. The general consensus was that the Committee would meet again on Monday, July 1st, 2019 at 11:00 a.m. to consider these subsequent written submissions but if there was a need to invite the person or organisations to make an oral submission for clarification it would be done off the record.

Item 6: Any Other Business

There was none.

Item 7: Adjournment

On the motion of Senator Ms. Alpheia M. Wiggins, seconded by Senator Miss Crystal N. Drakes, the meeting was adjourned to Monday, July 1st, 2019 at 11:00 a.m.

There being no other business Madam Chairman adjourned the meeting accordingly at 4:10 p.m.

B. Gibbons

Beverley S. Gibbons
Deputy Clerk of Parliament

Confirmed this 8th day of July 2019.

[Handwritten signature]
Chairman

**PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2018 – 2023)**

**JOINT SELECT COMMITTEE
ON THE
DATA PROTECTION BILL, 2019**

Minutes of the Third Meeting of the Joint Select Committee on the Data Protection Bill, 2019 held in the Senate Chamber, Parliament Buildings, Bridgetown on Monday, July 1st, 2019 at 11:00 a.m.

PRESENT WERE:

Senator the Hon. Miss Kay S. McConney (Chairman)

Senator Rawdon J. H. Adams

Senator Damien R. Sands

Senator Ms. Althea M. Wiggins

Hon. Dwight G. Sutherland, M.P.

Hon. Ms. C. Sandra V. Husbands, M.P.

Senator Miss Crystal N. Drakes

Mr. Neil G. H. Rowe, M.P.

ABSENT WERE:

Hon. Dale. D. Marshall, Q.C, M.P.


Bishop Joseph J. S. Atherley, J.P., M.P

Senator Kevin J. Boyce

IN ATTENDANCE WERE:

Mr. Nigel Jones, Deputy Clerk of Parliament

Ms. Beverley S. Gibbons, Deputy Clerk of Parliament

Ms. Shawn Belle, Senior Parliamentary Counsel, Chief Parliamentary Counsel Office

Mr. Chesterfield Coppin, E-Commerce Development Officer, E-Commerce Development Officer, Ministry of Small Business, Entrepreneurship and Commerce

Miss Suzanne Hamblin, (Library Assistant) Procedural Officer to the Committee (Ag.)

Item 1: Welcome

Madam Chairman called the meeting to order at 11:30 a.m.

Madam Chairman informed the Committee of the presence of Miss Charlin Skeete, student of the Kent University, England, who was on a work/study attachment to Parliament. There were no objections to her observing the meeting.

Item 2: Minutes

The Minutes of the Meeting held on Monday, 24th June, 2019 were taken as read.

On the motion of Senator Rawdon J. H. Adams, seconded by Senator Ms. Alpheia M. Wiggins, the minutes were approved and confirmed.

Item 3: Matters Arising

Madam Chairman raised the issue of streaming the proceedings and informed the Committee that the meeting would not be streamed live for the public as previously agreed.

Item 4: Consideration of Written Submissions

Madam Chairman proposed that the Committee only consider the recommendations that were deemed as absolutely necessary.

1. The Barbados Bankers Association Inc.

1. Financial records as “sensitive personal data” (Clause 2)

The recommendation was that “*financial record or position*” not be included in the list of personal data deemed to be sensitive personal data in keeping with the EU General Data Protection Regulations (GDPR). The Committee agreed that the definition of “*sensitive personal data*” should remain as it falls under Clause 9.(1)(j) of the Bill.

2. Credit Reference Agency (Clause 2)

Although a definition for “*Credit Reference Agency*” has been included in the Bill, this term is not used anywhere in the Bill. The Committee agreed that the definition should be removed as it does no harm to the Bill.

3. Ensuring the reliability of employees that can access data (Clause 4(7))

The Bill requires a data controller to take reasonable steps to “*ensure the reliability*” of any employees who have access to the personal data. This is vague and should be deleted or clarified. The Committee agreed with the recommendation that clarification should be made to the term “*ensure the reliability*”.

4. Existing contracts with Data Processors (Clause 4(9))

Data can only be processed by a data processor under a written contract with a data controller. The recommendation was that a transition period for the implementation of the Bill would facilitate the need to implement new contracts and renegotiate existing contracts with vendors who process data on their behalf. The Committee agreed that the recommendation for a transition period was not a matter to be considered at this time, as it could be addressed privately.

5. Lawfulness of Processing (Clause 6)

Processing of data is deemed to be lawful only in certain circumstances, one of which is where it is necessary for compliance with a legal obligation. Clause 6.(1)(iii), however exempts obligations imposed by contract. The recommendation is that the exemption be deleted as it is unnecessary. It is a basic principle in law that persons cannot contract outside of the law. The Committee disagreed with the recommendation to delete Clause 6.(1)(ii) and decided that it should remain as it was a reiteration of the law.

6. Children (Clauses 2 and 8)

It is recommended that *“child”* should be categorised as someone younger than 16 rather than 18 years old. It is noted that under the GDPR, member states may define a *“child” to be a person as young as 13 years old*. The Committee agreed that the word *“child”* should be categorised as a person under the age of eighteen and not a person under the age of sixteen as recommended.

7. Processing of sensitive personal data (Clause 9)

Under Clause 9.(1)(a), *“written consent”* is one of the grounds on which sensitive personal data (which is defined to include financial data), may be processed. The recommendation was that *“explicit consent”* be used instead of *“written consent”*, as was done in the EU under the GDPR, which is a wider term. The Committee agreed to the recommendation and that a definition for *“explicit consent”* to be included in Clause 2.

8. Right to Erasure (Clause 12)

Madam Chairman stated that the point here is that when the data is stored, erasure of all physical and electronic databases is done by the data controller and such processors could be difficult given that the data of a large multi-national bank would be in varying formats in databases in different countries and on multiple system platforms. This would be administratively challenging, and may not be possible for some computer systems which are not designed to erase information. The Committee acknowledged that it could be hard and expensive and agreed that the recommendation with regard to Clause 12 had no impact on the Bill as drafted and therefore there would be no change.

9. Right to data portability (Clause 15)

Under Clause 15.(1) of the Bill, data subjects will be entitled to receive the personal data they have provided to data collectors in a *“structured, commonly used and machine-readable format.”* In addition, Clause 15.(2) allows data subjects to have such information transmitted directly to another data controller, but only where the processing of the data is carried out by automated means. In such a case, the data supplied would already be held in a machine-readable format. It is recommended that in the GDPR the right to data portability, to receive it in machine readable format, data portability only exists where the processing of data is carried out by automated means. The Committee recommended that the *“structured, commonly used and machine-readable format”* remain a part of the definition and not change. In speaking to portability that exist where

the processing of the data is carried out by automated means, the Committee agreed that the Clause should remain as it is and would seek to make accommodation if they could in a transition period.

10. Transfer of personal data outside of Barbados (Clauses 22 to 25)

Personal data may be not transferred to a country outside of Barbados unless (a) the country provides for an adequate level of protection for the rights of data subjects; (b) there are appropriate safeguards and legal remedies; and (c) data controllers and data processors develop very detailed binding corporate rules. Where a data subject has given his consent to the transfer, and in other specified cases, (a) and (b) do not apply but binding corporate rules are still required.

Under the EU GDPR, data may be transferred to a country that has an adequate level of protection, as determined by an authority. This approach should be adopted. It is recommended that the data protection commissioner would have a list of countries deemed to have an adequate level of protection and this would prevent the individual companies, the data controllers and processors from doing their own research on the laws and to demonstrate that there are appropriate safeguards in place. The Committee agreed that the Bill would not be impacted by the recommendation and that Clauses 22 to 25 would remain as they were.

11. Binding Corporate Rules (Clause 25)

At Clause 25.(1)(c) data controllers and data processors are required to develop binding corporate rule which specify that they are legally binding both in and outside of Barbados. The reference to "*outside of Barbados*" should be removed as an entity cannot specify the legal effect of its rules in other countries. The Committee agreed that the Clause should remain as the recommendation for the removal of the requirements for binding rules "*outside of Barbados*" had no impact on the Bill.

12. Legal Professional Privilege (Clause 40)

This exemption should be widened to include information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser. The Committee agreed that there was no need for the widening of the exemption and that the recommendation had no impact on the Bill.

13. Registration as a Data Controller and a Data Processor (Clauses 50 and 51)

It is recommended that persons who process personal data solely for a reason set out in PART V, titled "*Exemptions*", should not be required as a data processor or data controller.

Persons who only process personal data as part of staff administration should also be exempt from registration.

The Committee agreed that the recommendation had no impact on the Bill.

14. Appropriate Technical and Organisational Measures (Clauses 53, 58 and 62)

It is recommended that the Data Protection Commissioner be required to issue codes of conduct and that these sections provide that adherence to such codes of conduct be capable of demonstrating compliance with the above-mentioned obligations. This will give far greater certainty of compliance.

Ms. Shawn Belle stated that Clause 71 (r) provides for the Data Protection Commissioner to prepare appropriate codes of practice for the guidance of persons processing personal data. The Committee agreed that the provision under Clause 71(r) satisfies and therefore the recommendation had no impact on the Bill.

15. Data Privacy Officer (Clause 68)

The data privacy officer must have expert knowledge of data protection law and practices and must report directly to the highest management level. Accordingly, banks may need to contract data privacy consultants and hire or identify and train data privacy officers, to facilitate implementation of the provision of the Bill.

It should be made clear that the data privacy officer may be assigned other tasks and duties which do not pertain to the Bill, so long as there is no conflict of duty. This will allow banks to assign those tasks to an existing position without being forced to hire additional personnel.

A transition period of at least two years is necessary to facilitate the implementation.

The Committee agreed that the recommendation was an internal matter which could be dealt with the Banks and therefore it had no impact on the Bill.

16. Functions of Commissioner (Clause 71)

The functions of the Data Commissioner should include the issue of model codes of conduct and approving same.

The Commissioner should also be empowered to issue advice to data processors and data controllers upon request.

The Committee agreed that the recommendation had already been dealt with and had no impact on the Bill.

17. Warrants (Clause 85)

A warrant can require any person on the premises to provide an explanation of any document found on the premises. This is not feasible or practicable. The person asked to explain the document should be duly authorised in writing. The Committee agreed that the recommendation had no impact on the Bill.

18. Administrative Penalty (Clause 94)

It is recommended that the Bill clarify that if a data controller or data processor, for the same or linked processing, breaches several provisions of the Act, the total penalty should not exceed \$50,000.00.

It is also recommended that where the Commissioner makes an order for an administrative penalty that notice of the order should be served on the relevant person and the 28 day deadline for appealing to the Tribunal should run from delivery, rather than the date of the order.

The Committee agreed that it would keep the penalties the way they were and there would be no further adjustment. The recommendation had no impact on the Bill.

The Bill has no “grandfathering provision” for personal data collected without consent that meets the newly implemented standards.

It is recommended that the legislation be applicable to information obtained on a go-forward basis and notice to existing customers suffice as consent.

On the explanation of Ms. Shawn Belle, Madam Chairman understood that one can have a retroactive benefit but not a retroactive penalty or liability. The Committee agreed that this recommendation had no impact on the Bill.

20. Employee Data

Businesses that do not process large amounts of customer or vendor personal data are still likely to process the sensitive personal data of their employees. Those businesses will have to register as data processors/controllers and meet the requirements of the Bill.

Given the likelihood of business disruption and increased costs, persons who only process personal data as part of staff administration should also be exempt from registration.

If all employers are required to register and comply with the Bill, clear guideline, training and education should be provided to all business, trade unions and members of the public to assist with their understanding of the Bill.

A generous transition period is required to facilitate the above.

The Committee agreed that the recommendation had no impact on the Bill.

21. Liability of Data Controllers and Data Processors

It is recommended that the Bill specify whether the data controller and or the data processor is liable for the damage caused by processing which infringes the Act. The Act should also explicitly provide that data controllers and data processors are exempt from liability if they are not in any way responsible for the event giving rise to the damage.

The Committee agreed that a provision would be included so that it will have an impact on the Bill as drafted.

22. Transition Period

A transition period of at least two years is vital for the legislation to have the desired effect and for businesses to grow during the implementation process.

The Committee agreed that when the Bill is proclaimed this would be addressed. The recommendation had no impact on the Bill.

23. Costs

The administrative costs will have to be borne by the data controllers and data processors, as data subjects are not required to pay any fees to

enforce the rights given to them under the Bill. It is possible, however, that the costs or part thereof may be passed on to the customer for businesses to remain viable.

The provisions of the Bill should also take into consideration the costs that will be incurred by the office of the Data Protection Commissioner in the exercise of its functions.

The Committee agreed that the recommendation had no impact on the Bill.

SUSPENSION

On the motion of the Hon. Ms. C. Sandra V. Husbands, M.P, seconded by Senator Ms. Alpheia M. Wiggins the meeting was suspended for lunch until 2:15 p.m.

At 1:25 p.m. Madam Chairman suspended the meeting.

RESUMPTION

Madam Chairman resumed the Chair and called the meeting back to order at 2:30 p.m.

2. The Barbados Bar Association

1. Regulations Provisions

It is important to include the draft regulations, otherwise there will be a lacuna between proclamation and implementation. It is always useful to hold consultation and discussions on the regulations in tandem with discussions on the Bill.

The Committee agreed that the Regulations had no immediate impact on the Bill but consideration would be given to having consultations on the regulations. It is not directly relevant to the Bill but would be noted for consideration.

2. Enforcement provisions generally

Penalties for breach or failure to comply occur throughout the Bill.

It is submitted that this Bill should either impose civil liability alone or dual civil or criminal liability for more serious breaches.

The Committee agreed that there was no consideration for the recommendation within the Bill.

PART I – Preliminary

3. Definition of “Court”

The Committee agreed that Miss Shawn Belle, Senior Parliamentary Counsel, Chief Parliamentary Counsel Office would re-examine and make the necessary corrections to word “*Court*” in the Bill.

PART III – Rights of a Data Subject (Clauses 10-21)

4. “Right to Privacy”

The Committee agreed that ensuring the “*right to privacy*” was a useful submission and would be taken into consideration but it had no immediate impact on the Bill as it is making an amendment to a different kind of legislation, namely the Constitution.

5. Right to Compensation

The recommendation is that in PART III there is no specific right to compensation for the data subject. In the absence of a right to compensation for damage suffered arising whether in respect of material and non-material damage, then it places a burden to show and prove pecuniary or other loss. In the realm of data and privacy, infringements can be difficult to quantify. The question is whether data subjects would indeed pursue recourse under the Act against data processors who have infringed their rights. The Committee agreed that a Clause should be inserted by CPC that would speak to compensation for the data subjects.

PART IV – Transfers of Personal Data Outside of Barbados (Clauses 22-28)

6. Data Transfers

It was clear that the intention of the legislature and an important facet of this Bill to hold foreign governments and foreign corporations/businesses liable for processing of data of Barbadians as is evidenced by PART IV, Clauses 22-28 of the Bill.

Section 22 of the Bill speaks to a general principle for data transfers and this section states that the country or territory where data is transferred to must provide an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their data and appropriate safeguards for the processing of that data which include legal remedies for data subjects.

Based on Section 23 of the Bill, which speaks to what will constitute as adequate protection as stated in Section 22, enforcement of the protection of the data of Barbadians is dependent on whether the foreign Country has adequate legislation, the laws enforced in the country or territory in question and international obligations of that Country”.

Madam Chairman stated the recommendation called for supporting legislation to hold foreign governments and private companies accountable. The Committee agreed that the recommendation would not be included in the legislation as there was no scope and had no impact on the Bill but would be kept for further consideration.

PART VI – Data Controller and Data Processor (Clauses 50 and 51)

7. Data Controllers must be registered

Clause 50 and 51 require data processors or data controllers to register and imposes fines and criminal sanctions on organisations who fail to do so.

Where the offending party is a corporation, it is submitted that civil liability through the imposition of fines and penalties would be a more efficient means of enforcement.

It is submitted that these provisions alone or a flat fine will not incentivise large foreign corporations with annual revenue earnings of billions of dollars to implement data protection policies in order to be in compliance with this Bill. It is recommended that penalties may be imposed on the basis of percentages of income or turnover, so that there is proportionality in the imposition of a fine.

The Committee agreed that the fines should be kept but with the view to reviewing at some stage to determine whether there is need to adjust the way the fines were assessed. They also agreed that the decision made on Wednesday, June 26th, 2019, would remain. There was no need to make adjustments to the Clauses.

9. Territorial Scope

The territorial scope of the Data Protection Bill is largely underpinned by other foreign actors performing certain actions (adequate legislation, international agreements, registering as data processors/data controllers) in order for the rights of Barbadian citizens to be enforced.

The recommendation is to consider whether we can shift the burden of compliance for processing data.

The Committee agreed that the recommendation to consider shifting the burden of compliance for processing the data had no impact on the Bill.

10. Data Protection Commissioner (PART VII – Clauses 70-75)

The Bill establishes the post of Data Protection Commissioner who is charged with the responsibility of general administration of the Act and is in fact the regulator.

The recommendation is to review the provisions with a view to establishing greater independence as a supervisory authority. The Committee agreed that the recommendation to establish greater independent supervisory authority had no impact on the Bill.

PART X – Miscellaneous

11. Commencement (Clause 99)

It is highly recommended that upon the passing of this Bill, a suggested grace period of at least 6 months to 1 year be inserted for the enforcement and commencement date of this Act.

Madam Chairman recommended that the matters raised with regard to the commencement should be dealt with in the Proclamation of the Act

when it became law. The Committee agreed that there was no need to make any further adjustment to the provisions for commencement.

At 3:10 p.m. Madam Chairman called for a five (5) minutes break.

Madam Chairman resumed the meeting at 3:15 p.m.

3. Mr. Devaron Bruce, MPhil Candidate

The Chair requested that Miss Shawn Belle examine and present to the Committee the salient points within Mr. Bruce's submission. She highlighted *"Main concern"*, *"Mitigating threats to data-privacy and sensitive data manipulation"* (re Clause 9), *"Disclosure requirements for companies that process sensitive social media data"*, *"Enhancing user's control over data"*, and *"Further considerations to improve data protection"*.

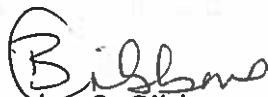
The Committee agreed that the submission was helpful and beneficial and there was a need to look at greater regulation of Social Media. However, the consensus was that the recommendations had no impact on the Bill.

4. Ms. Cynthia Wiggins

Item 6: **Adjournment**

On the motion of Mr. Neil G. H. Rowe, M.P., seconded by Senator Rawdon J. H. Adams, the meeting was adjourned until a date for the next meeting would be announced.

There being no other business, Madam Chairman adjourned the meeting accordingly at 3:35 p.m.



Beverley S. Gibbons
Deputy Clerk of Parliament

Confirmed this 8th day of July 2019.



Chairman

The Committee agreed that the written submission from Ms. Cynthia Wiggins would not be given further consideration as it mirrored her oral presentation made on Wednesday, 26th June, 2019.

At 3:25 p.m. Madam Chairman called for a five (5) minutes break.

At 3:30 p.m. Madam Chairman resumed the meeting.

Madam Chairman proposed that the Committee consider any further amendments to be made to the Bill.

PART I was called and it was agreed that nothing further than the amendments already made would apply. PART II was called and the Committee agreed that PART II should not change in anyway other than what was already agreed. PARTS III to X were called and passed. The Schedule was called and passed.

The Committee agreed that there should be no further amendments than what would have already been agreed to the respective Parts.

Item 5: Any Other Business

There was none.

**PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2018-2023)**

**JOINT SELECT COMMITTEE
ON THE
DATA PROTECTION BILL, 2019**

Minutes of the Fourth Meeting of the Joint Select Committee on the Data Protection Bill, 2019 held in the Senate Chamber, Parliament Buildings, Bridgetown on Monday, 8th July, 2019 at 2:00 p.m.

PRESENT WERE:

Senator the Hon. Miss Kay S. McConney (Chairman)

Senator Damien Sands

Senator Ms. Alpheia M. Wiggins

Hon. Dale D. Marshall, Q.C., M.P.

Hon. Dwight G. Sutherland

Senator Miss Crystal N. Drakes

Mr. Neil G. H. Rowe, M.P.

ABSENT WERE:

Senator Rawdon J. H. Adams

Hon. C. Sandra V. Husbands, M.P.

Bishop Joseph J. S. Atherley, J.P., M.P.

Senator Kevin J. Boyce

IN ATTENDANCE WERE:

Mr. Nigel R. Jones, *Deputy Clerk of Parliament*

Ms. Shawn Belle, *Senior Parliamentary Counsel, Chief Parliamentary Counsel Office*

Mr. Chesterfield Coppin, *E-Commerce Development Officer, Ministry of Small Business, Entrepreneurship and Commerce*

Miss Suzanne Hamblin, *(Library Assistant) Procedural Officer to the Committee (Ag.)*

Item 1: Welcome

Madame Chairman called the meeting to order at 2:25 p.m.

Item 2: Minutes

Minutes of 26th June, 2019

Minutes of 1st July, 2019

The aforementioned minutes were confirmed with amendments by the correction of the name Althea Wiggins to Alpeha Wiggins on the motion of Senator Damien R. Sands seconded by Senator Ms Alpeha M. Wiggins.

Item 3: Matters Arising

There were no matters arising.

Item 4: Consideration of the Draft Report

Amended Bill

Clause 1. – Long Title

The Committee approved the amendment thereto.

Clause 2.

Clause 2. (as amended) by the deletion of “credit reference agency” was approved

Clause 4. (7) (as amended) was approved

Clause 9. (1) (a) (as amended) was approved

Clause 15. and other clauses containing references to “his or her” (as amended) were approved.

Clause 71. (m) (as amended) was approved

Clause 79. (1) (as amended) was approved

References to the word “court” in the Bill.

The relevant amendments to clauses 2., 16.(4), 17.(2), 25.(e), 38.(11), 67.(1)(a), 70.(3), 73.(2)(a), 82. (1)(b) & (2), 85.(1), 88., 94.(2)(a) & (11) and 95.(3) were approved.

New clause 93. (1) and (2) – Right to compensation and liability was approved.

Old clauses 93. to 99. – numbered 94. to 100. were approved.

The draft report was amended and approved on the motion of Senator Ms. Alpheia M. Wiggins seconded by Senator Damien R. Sands.

Item 5: Any other business

Madam Chairman reported that the Barbados Association of Medical Practitioners (BAMP) have submitted a written submission albeit late. However, the submission was considered by Ms Shawn Belle. The recommendations therein

were similar to those otherwise considered by the Committee and had no impact on the amended bill. Madam Chairman thanked Ms Belle for her work on the BAMP submission.

Madam Chairman thanked the Committee for its work on the Bill and informed that the amended Report would be circulated for approval.

ADJOURNMENT

There being no further business Madam Chairman terminated the meeting at 3:10 pm.



Deputy Clerk of Parliament

Confirmed the 17th day of JULY 2019.



Chairman

Data Protection Bill 2019 Oral Submission

I would like to first thank the members of the Joint Select Committee for allowing the public to provide submissions on The Data Protection Bill.

Secondly, although I believe the Bill is an important one, I also think that amendments may be necessary to ensure that it facilitates:

1. Provision of a framework that allows companies to have the flexibility to target individuals, gain a competitive advantage through the utilisation of data and data analysis, while ensuring the privacy of individuals.
2. Consideration of the new methods in which data can be captured, generated or analysed for example through retail transactions and online methods.
3. Viewing the protection of data more so from the standpoint of the data use itself, than from the classification of the activities and tasks in the data process.

For conciseness and clarity in the proceeding paragraphs/ discussion, my submission points will be addressed under six (6) main headings with either page or section references where required. The main headings are as follows:

1. Data and Data Elements
2. Consent
3. Privacy and Security
4. Monitoring and Compliance
5. Cost
6. Other, where I believe the points were significant but did not fit into any of the other categories.

Data and Data Elements

1. **The Bill, in most instances, does not seem to take into consideration the nuances of online or transactional data or the issues that would accompany such data types. For example:**
 - a. Page 12 "Accessible records" I believe that online/ transactional records do not technically fall within any of the record types listed.
 - b. Page 16 "Sensitive personal data" or in "Data" on Page 13 does not speak to photographs, videos, comments etc. and does not include personal purchasing information.

- c. Page 79 (r) does not include transactional or online data.
 - d. Page 18 4 (1) (c) This would limit social media or other business ability to utilize data as part of their competitive advantage.
 - e. Page 20 5 (1) The point speaks to "deceiving or misleading" of individuals, however businesses often collect data for purposes other than what they purport or change the reasons they are collecting the data, usually for analysis and targeting reasons with no malice intent e.g. Facebook, Google. The wording being used in its current form could easy stifle small business, innovative business ventures.
2. **Online data by its very nature may be onerous to describe making the registration requirement on Page 60 51 (1) (c) challenging to comply with. For example:**
- a. Metadata (e.g. time stamp information, landing pages and exit pages etc.) in general would be difficult to describe but may be captured for analysis reasons. Additionally, data capture requirements may change to assist with online visitor analysis as the need arise, which could potentially hinder the innovation of businesses if notification regarding the description is required.
3. **In the ordinary course of business, data can be collected and used for profit or as a tool to gain a competitive advantage. So consideration would have to be given to the following points:**
- a. Page 25 e (i) (A) Data can be collected for profit especially in relation to social media and AI.
 - b. Page 33 18 (1)- (4) Could limit an organization's use of data modelling, algorithms, and profiling which may be how the company ensures its competitive advantage. For example, social media (Facebook, Instagram etc.).
 - c. Page 27 10 (1) to provide the logic for profiling methods used could impact on a company's competitive advantage.
 - d. I don't see a reference to the sale of transactional or other data regarding the purchase of a company. For example, during a merger or acquisition can a business purchase transactional, customer, and other data.
4. **The definition of direct marketing on Page 33 (3) does not appear to take into consideration telemarketing or online marketing since there are no restrictions specific to telemarketing or content marketing within the points on direct marketing. For example:**
- a. Where the company may initially call a customer making it seem as though it is a service call and then seek to upsell products or;

- b. Where the individual may be targeted with content that does not seem as though it is an advertisement.**
- 5. Although part of the General Data Protection Regulation (GDPR), for small businesses, the requirement to have a data privacy officer as a separate employee seems financial cumbersome. Page 74, 75, and 76 and would hinder small businesses seeking to utilize data as a competitive advantage.**

Consent

- 1. There is a need to specify in the Bill that consent needs to be explicitly given by "opting in" for any utilization, transfer or processing of the data. Therefore consideration would have to be given to the following points:**
 - a. Page 24 9 (1) (a) the term "written consent" would have to specify that the individual needs to "opt-in" and that there are not automatically opted in.**
 - b. Page 26 (4) Content even for medical research should be explicitly given. There should be a distinction between "medical treatment and reasons" versus "medical research". It would be unfair to individuals that their cells or organs could be used to advance medicine without their consent e.g . the most famous case of Henrietta Lacks.**
 - c. Page 44 (26) (a) The data subject has to give consent in writing through opting in.**
 - d. Page 45 (26) (b) (iii) Even if the data is being transferred in relation to the agreed interest of the subject there is still a need to notify and receive in writing or require opting in from the data subject.**
 - e. A general note that with direct marketing, telemarketing, or content marketing online or offline targeted marketing efforts, there should be no automatic consent.**
- 2. The Bill should seek to specify that individuals must be notified of the accidental disclosure, destruction, or breaches of their data. Page 70 64 (3) (b) seems like a loophole. Individuals should be informed of any infringements.**
- 4. Where an individual is no longer a user or a customer they should be able to ask for the removal of their data providing that it is not of historical records or that there are no legal ramifications should it be removed. Although stated on Page 28 12 (1) the following points would still need to be reviewed:**
 - a. Page 32 (16) (1) Should be able to ask for it to be removed not just simply stopped.**

- b. Page 33 (17) (1) Not only cease processing but remove the data.

Privacy and Security

1. **Although privacy and security seem paramount within the Bill. The following points still need to be reviewed:**
 - a. Page 19 7 The data controller must also ensure confidentiality as well as reliability.
 - b. Page 20 (8) (a) The data processor should ensure that the technical and organizational security is equal or above what is expected of the data controller, not simply "sufficient".

Monitoring and Compliance

1. **In the Bill there appears as though there is no obligation to comply or there are loopholes that would allow individuals to circumvent the requirements. For example:**
 - a. Page 31 14 (1) (c) The term "disproportionate effort" is subjective and can lead to data not being supplied.
 - b. Page 28 (3) and (4) seems as though they are loopholes to bog down the individual with hard copies or administration fees. Electronic means should be provided if requested.
 - c. Page 91 83. (1) This does not seem to take into consideration when someone does not comply.
 - d. Page 30 13 (2) [And a few other places] What is considered public interest? Public interest should be broader than public health Page 29 4 (c).
 - e. General note: I am not seeing the mentioned past directors (which was in a previous iteration of the Bill). I am also not seeing any mention of the seizing of the company's assets should fines not be paid.
2. **There is a need to specify the timeframe or frequency in which some activities should occur. The following points would need to be reviewed.**
 - a. Page 77 1 (g) how often must the monitoring occur.
 - b. Page 79 (u) timeframe for investigation of complaints.
3. **The Bill would need to specify that notice by the Commissioner should be given via registered mail.**

- a. Page 92 84 (1) Should indicate by registered mail or if electronically that read receipt or confirmation of the electronic mail is required.

Cost Issues

1. If there is a cost associated (legal, administrative or otherwise), with individuals requesting information or trying to ensure compliance via the tribunal or a court, it may become a deterrent to individuals. There are other instances of "cost" being mentioned but examples are.

- a. Page 28 (3) not sure a data subject should be made to pay a fee in retrieving information the data collector should have should cost as part of their operational cost or the service they provide to the public.
- b. Page 39 (12) The appeal to the Commissioner would have to be at no cost to the individual.

Other Issues

1. Page 10 Financial institutions may not fall under "credit reference agency" according to the definition but also have information regarding the credit standing of individuals, for example, the Student Revolving Loan Fund, banks etc. hold the financial status of individuals.
2. Page 26(m) (i) does not include sexual orientation, religion, etc. but probably should.
3. Page 17 3.1 (b) how is this going to be applied to global companies as Facebook etc.?
4. Data Collection Commissioner's function should also be responsible for educating and enforcing international data protection and privacy Acts that would affect the data collection in Barbados, e.g. the General Data Protection Regulation (GDPR) which came into force on 25th May 2018.

In conclusion, again I think the Bill is an important and necessary one. However, even with the recommendations above, I believe that the Bill needs to be changed in such a way that its focus, the focus of the Tribunal and the Commissioner is more on educating the public of their rights, and dealing with non-compliant issues as quickly as possible versus seeking to ensure compliance.

-Cynthia Wiggins

Inch Marlowe,
Christ Church,
Barbados,
BB17122

To:

**Clerk of the Parliament,
Barbados Parliament,
Bridgetown,
St. Michael**

Honourable Sir,

I, Stevenson Antonio Hollingsworth, acting in the capacity of a private citizen and as the Founder of a local technology start-up registered and domiciled in Barbados, do submit for consideration to this Joint Select Committee the following:

It is my opinion that the Data Protection Bill 2019, places an onerous financial and logistical burden on the average Barbadian at this time. I am relying solely on the definition of "data", "data controller", "data processor" and the position of Data Privacy Officer as presented in this most important Bill.

It is indeed obvious and necessary for there to be legislation that protects the Personally Identifying Data of the citizens of Barbados and the global community at large. As we enter into this Digital Revolution that brings great opportunities but also great threats, we should ensure that the citizens and residents of Barbados are protected from malicious or exploitative use of their personal data. I understand that the Government, in its steadfast march towards making Barbados an attractive place for investors, has seen it most urgent to bring before this most honourable house a Bill designed to protect those constituents who gave their resounding mandate to the custodian of the government.

Inch Marlowe,
Christ Church,
Barbados,
BB17122

However, upon examination of this Data Protection Bill, it does not appear to be, in its current form, in the interest of the average Barbadian entrepreneur, whether in the Technology field or otherwise. I will lay out examples of such cases and summarize a list of suggestions for your esteemed consideration.

1. Under this Bill, all operators and organizers of Tours, operators of guest houses, taxi drivers and other key players in the tourism industry, where booking and contact information are required, would by definition be data controllers and would by this Bill require to be registered and certified. These operators may be small enterprises that in our current economic situation may not be able to:
 - a. afford certification and registration.
 - b. Should they lack the technical ability, hire a certified and registered data controller.
 - c. Hire or contract a Data Privacy Officer.

For some of these businesses, a lost phone would constitute a serious breach and would require submission to the Data Commission as well as a Data Impact Assessment. Therefore, not only does this small business have to replace a critical component of their business infrastructure but they also have to incur the relevant legal fees to prepare a report for the Data Commissioner via the Data Privacy Officer.

2. Under this Bill, while the position of Data Privacy Officer may be shared in a group enterprise or amongst public authorities. The quality of the oversight and the diligence required as outlined in the Bill may be compromised or open to compromise given the demand for such individual(s). It may be that to execute this Bill, should it become an Act, the outsourcing of this specialist position to offshore services may require further drain the limited foreign exchange of Barbados. It should be noted that in public authorities, while the authority may be registered as a data controller, employees who

in the course of their duties have collated or accessed personal data, will upon dismissal or leave become by default, data controllers.

3. Under this Bill, the requirements of startups in the technology sector are made more difficult, especially innovative ones that utilize the latest technology. This has the potential to stifle the emerging technology sector in Barbados by now making it even more expensive and difficult to do business in Barbados. My company currently makes use of automated systems that are designed to learn over time. These systems are by default, not designed to target any individual but are designed to allow business or government to be able to better serve their clients. In order to operate, my company must meet international standards as relates to:

- a. privacy,
- b. cookie management,
- c. data handling,
- d. data collection method,
- e. what data is collected,
- f. why it is collected,
- g. how it is secured,
- h. contact person for services,
- i. contact email for services.

In addition, we must interface with data controllers and data processors larger than ourselves over whom we have no significant control or influence. Namely but not exclusive to:

1. The ISP networks that are used by us.
2. The ISP networks that are used by the data subject.
3. The Modem or device of the data subject.

4. **Cloud Based Services**
5. **Any unknown technology that may be designed to intercept or interfere with the secure transmission of data.**
6. **Emerging technology or changes in processes that improve the level of service but unexpectedly changes the status of a natural person or business entity from a data controller to a data processor.**

Given these identified scenarios in this submission, this bill places a disproportionate amount of liability (\$500 000 or 3 years in prison) on anyone deemed as a data controller or data processor who is in non-compliance. While large companies may be able to mitigate liability by preemptive budget or by Cyber Insurance, the individual, SME or the startup may not have the resources to risk such liability.

As such I would like to make the following suggestions for your consideration.

1. **Clarify in this Bill how relates to or supersedes Article VI of the Electronic Transaction Act.**
2. **Reduce the requirements of the data controller to fall within the established Article VI of the Electronic Transaction Act until such time as the public is aware of and fully understands the value of personal data and the adequate data security protocols they should use.**

3. The requirement of registration and certification of the data controller be phase over a period of three years from enactment, with priority placed on the registration of those data controllers and data processors who carry the greatest Data Privacy Impact. This assessment of Data Privacy Impact should also inform the just penalties to be imposed in the case of non-compliance and as a percentage of the revenue of the non-compliant party. Not all persons classified as data controllers are as familiar with digital security as they should be and the Government should ensure that it does not by accident or by design frustrate or prevent the enjoyment of the individual's property as enshrined in the Supreme Law.
4. Clarify the term "in writing" as it relates to the Electronic Filing Act.
5. The definition of "profiling" is not in sync with current technology trends. This section of the Bill hinders the advancing of Smart technologies to provide better service and security to the citizens of Barbados.
6. There is no pressing justification for the sensitive data as defined by this Bill to be legitimately processed by political, religious or philosophical bodies, given that the Bill itself gives the data subject the right to migrate their data from one data controller to another. There is an implied action that:
 - i. Sensitive data was extracted by consent.
 - ii. Sensitive data was extracted by clandestine means.
 - iii. Sensitive data was not destroyed.

This Bill ignores the recognition of the brain as a storage device that cannot be deleted. Thus, sensitive data should only be processed by persons who fall under implied or explicit confidentiality:

Priests in the exercise of confession or absolution,

Practising psychologist,

Guidance counsellor,

A person who holds a position of trust.

The above may be bound by confidentiality under the appropriate preexisting Acts.

7. "Automated decision" be clearly defined to distinguish whether,
 - a. Electronic PBX services
 - b. Electronic Cognitive Services,
 - c. Machine Learning Algorithms,
 - d. Artificial Intelligence systems.

These systems use disaggregated data but given the volume and parameters of the data, may by statistical deduction appear to identify an individual or group. Artificial Intelligence and Machine Learning will play an integral part in the development of any industry, globally. This Bill should not create the position where, due to the request of a data subject to delete data, an algorithm must be retrained or redesigned, especially given the small dataset footprint of Barbados. Neither should it restrict the free use of and development of such technology in the services sector if productivity and competitive edge are the objectives of the Government.

Inch Marlowe,
Christ Church,
Barbados,
BB17122

Respectfully,

Stevenson Antonio Hollingsworth, BSc. Engineering

Founder Director,

Bajan Digital Creations Inc



Soledad González <soledad.gonzalez@quidgest.com>

6/19/2019 11:44 AM

Data Protection Bill | Interest in cooperation

To parliamentbarbados@caribsurf.com Copy international@quidgest.com • bguimaraes@quidgest.com

Dear Clerk of Parliament,

We were interested to read that the Joint Select Committee of both Houses of Parliament of Barbados is going to meet to hear submissions on the Data Protection Bill, next Wednesday, June 26.

My name is Soledad González and I am writing on behalf of Quidgest. Quidgest is a software company with headquarters in Lisbon and is actively involved in supporting private and public institutions with data protection, including meeting regulatory requirements and adoption of the European GDPR regulations.

Adoption of these regulations has been a major challenge for many companies and entities dealing with personal data of EU citizens (inside and outside of the Union). With the new rules and roles arising from the regulation, it was the right time for us to sit down with experts to define the workflow around the processes to meet the requirements of the GDPR. This led us to a first prototype and an evolving system that now is able to manage the whole life cycle of compliance with the Regulation, including management of data subject's rights.

Because of the similarity of the EU regulations with the Draft Data Protection Bill proposed in Barbados we would be happy to contribute at this stage of review of the Bill through sharing our previous expertise and lessons learned.

We deeply believe that technological consultants should take part of such processes and the implementation of regulations regarding Data Protection.

We do not know if IT solutions are going to be discussed within the session of Wednesday, June 26, in the Senate Chamber at Parliament, but we wanted to make ourselves available to the Government of Barbados in case any technological support is needed in that matter.

Sincerely,

Soledad González

Business Developer for Latin America



R. Viriato, 7 - 4ª | 1050-233 LISBOA | Portugal
Tel. (+351) 213 870 563 | Fax. (+351) 213 870 697 | www.quidgest.com

H

$$= \frac{1}{2} \left(\frac{1}{2} + \frac{1}{2} \right) = \frac{1}{2}$$

$$= \frac{1}{2} \left(\frac{1}{2} + \frac{1}{2} \right) = \frac{1}{2}$$

$$= \frac{1}{2} \left(\frac{1}{2} + \frac{1}{2} \right) = \frac{1}{2}$$

2

2

2

2

2

2

2

2

2

2

2

2

2

H



Barbados ICT Professionals Association
C/ o Barbados Coalition of Service Industries
Building #3, Unit 2B, Harbour Industrial Estate, St. Michael
Tel: (246) 429-5357 | Email: secretary@barbadosict.org |
Website: www.barbadosict.org

The Clerk of Parliament
The Barbados Parliament
Bridgetown
Barbados

Page 1

June 20 2019

Submissions on the 'Data Protection Bill 2019'

A comprehensive review of the Data Protection Bill 2019 laid in Barbados' Parliament on 15th day of May in 2019 was done by the Barbados ICT Professionals Association's (BIPA's) membership. The association hosted meetings which discussed the General Data Protection Regulation (GDPR) enforced on 25 May 2018 and more specifically, Barbados' Data Protection Bill 2019. Further, the association has made a submission following a call for comments on the bill from the Ministry of Commerce, 2018.

Position

We support the intent of this bill given the digital transformation plans for Barbados. However, the purpose of our submission is to highlight concerns and to make the appropriate recommendations as we see most fitting in this context. We strongly support the institution of such, given the importance for government to protect the privacy of its people respective to their personal data, by enforcing a regulatory framework by virtue of compliance, that businesses and organisations be accountable for the collection, processing, management and storage of all data collected whilst at the same time adhering to data privacy principles.

We wish to make the following comments:

Item #1

Reference: PART 1, Section 2, page 13: "data processor" means any person, other than an employee of a data controller, who processes personal data on behalf of the data controller';

Position: We support this clause but wish to make a recommendation that consideration be given to the incorporation and recognition of cognitive technologies.

Within the ICT industry, a Data Processor is a computer (software) or person that carries out the operations on data to retrieval, transformation or classification of information. We are of the view that the commands or instructions of the data controller guides the behaviour or conduct of the data processor. Therefore, whether a person or cognitive technology is used the Data Controller remain ultimately accountable once the data or data sets are effected. *Noting section 59 as applicable.*

Should the use of cognitive technologies be recognised, the 'Agreement', page 64, section 58 (4) can be had between the Data Controller and the owner of the cognitive technology.

The Barbados ICT Professionals Association (BIPA) is the island's foremost professional membership organisation for individuals and corporations whose primary focus is the expansion and development of ICT opportunities in Barbados and the Caribbean region.

Item #2

Reference: PART VI, Section 50 (2), page 59: "A person who desires to operate as a data controller may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose"

Position: We support the position and office of a Data Controller. However, apparently it is not practical for every Micro Small Business and Medium Sized Enterprise (MSME) to have a Data Controller due to operational cost.

Similar to Section 50, (6) (c), can consideration be given to a local agency that provides Shared Services to the MSME? We believe such an initiative would create equal opportunity for this 'venerable group' respective to compliance like the large conglomerates, that can afford such personnel. We foresee that the local agency would assume liability for its clients and notably Section 50 (2), page 59 would be applicable to each Data Controller hired by the agency.

Item #3

Reference: Reference: PART VI, Section 58 (2), page 66: "A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both"

Position: We support the notion of a penalty but oppose the fixed sum in the amount of \$500,000.

When we examine data-driven organisations and those where data is their greatest asset, \$500,000 is what we would call 'pocket change'. So instead of the penalty being a deterrent to the conglomerates, it becomes part of their annual budget under the heading of 'Risk Management' or hidden under 'Miscellaneous' or 'Incidentals', multiplied by 3, since data breaches are almost inevitable. Any astute Chief Information Officer (CIO) or Chief Operating Officer (CEO) together with their Financial Controller (FC) who is very knowledgeable and savvy re IT industry, will not only budget \$500K but multiple it by 3 or even 4, to ensure they have adequate coverage throughout the Financial year. They will even seek to get insurance coverage against law suits and associated liabilities. Such Policies can be recognised under the following names; Cyber Liability, Data Protection Insurance, Cyber and Privacy Insurance and so on.....
https://www.chubb.com/uk-en/assets/documents/info-tech-pi-cyber-policy-holder-summary-of-coverage-14_06_2017.pdf (an example of one such insurance policy)

We would like to suggest that the penalty be prorated on a percentage (5) basis and commensurate with a companies' gross annual earnings. Not only will the conglomerates now appreciate and understand the seriousness of the offense, but this model would create an equal opportunity for business sustainability amongst the MSME segment. Most MSMEs operations are likely to collapse if the penalty of \$10,000, \$50, 000 were due, furthermore the \$500,000.

Stuart

General queries:

1. What is the registration fee for a Data Processor?
2. Will there be a registration fee for a Data Controller?
3. Why does the Data Protection Commissioner has to be an attorney-at-law?

Conclusion

The members of BIPA fully endorse the aggressive digital transformation initiatives. As we are aware, 'Data' is king in such environments. We are pleased to have provided the aforementioned submissions in hope that our contribution will lend itself to a more sustainable economic and data-driven economy. We have carefully examined and engaged industry stakeholders to gather the concerns and queries outlined. Those are:

1. To recognise a blend of cognitive technology and human input specific to the data processor role
2. To recognise an agency or 'Shared Services' Provider that can act in the role of Data Controller for Micro Small Medium Size Enterprises
3. Consider a percentage based fine commensurate with gross annual earnings instead of fixed rate

Yours Respectfully,



Shireen Flann CDP
BIPA - Board Member *for*

Steven Williams
BIPA President



Solving Problems that are Hindering Barbados' Development.

Tel: (246) 232-9783 • E-mail: NextParty246@gmail.com • Web: SolutionsBarbados.com

20th June 2019

Clerk of Parliament
Parliament Buildings
Heroes Square
BRIDGETOWN

Attention: Clerk of Parliament

Re: Data Protection Bill, 2019

Dear Sir:

We appreciate being allowed to comment on the Data Protection Bill (2019), before it becomes law.

Legislation should allow what is intended, and discourage what is not intended, but which may be inadvertently allowed. Therefore, we have reviewed the bill with the aim of helping to remove its vulnerabilities. For your convenience, both the Section references and page numbers are provided.

Preamble (Page 11): Grammatical errors are common throughout the document. While a common-sense read of the bill appears to allow it to be understood as intended, the errors should be cleaned up in the final version. We have identified some of the most glaring errors. "*provide for provide for matters*" should read "*provide for matters*".

Section 9.1(e)(iii) (Page 25): The non-consent processing of sensitive information by political parties, trade unions, or other groups is allowed, once the data belongs to their members. However, these groups are allowed to process the data of persons who "*have regular contact with it in connection with its purposes*" without their consent.

This should not be allowed. I may have regular contact with the union as an employer, but I do not consent to the union processing any of my sensitive personal information.

Section 10.3 (Page 28): "*The data controller shall provide a copy of the personal data undergoing processing to the data subject*" The data subject can also have their information amended (Section 11.1), and erased (Section 12.1), "*without undue delay*".

It is critical that the Data Controller verify the identity of the data subject before giving them any data, or amending or erasing any data. This verification addressed in **Section 21.14** below.

"Where a data controller has reasonable doubts concerning the identity of the individual making a request pursuant to sections 10 to 18, the data controller may request the provision of additional information necessary to confirm the identity of the data subject." (Section 21.14)

The term "may" appears to make identity verification optional. May should be replaced with "shall" or "must". Further, it should be mandatory that authentic verification documents should be presented before releasing someone's data to a potential fraud.

Section 15.3 (Page 31): *"In exercising his or her right to data portability"*

The gender references should be consistent. Therefore, either mention both male and female, or mention male to mean both male and female, or make it gender neutral by using the plural, "their".

Section 22 (Page 40): *"Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects."*

Section 23 tries to define "adequate", and Section 24 tries to define "appropriate safeguards". However, every country will likely claim that they meet the defined standard. For the avoidance of doubt, a schedule containing an approved list of countries, or a negative list of countries, should be part of the legislation.

Section 50.4 (Page 59): *"A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both."*

A data controller is anyone who is responsible for processing data, which can include every employer and educational institution. This needs clarification. Also, see Section 55.4 below.

Section 55.1 (Page 62): *"A person shall not operate as a data processor unless he is registered in the Register of Data Processors"*

If there is no separate registration act for the new profession, should it then be included the Profession, Trade and Business Registration act (Cap 373), like other professions.

Section 55.4 (Page 62): *"A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both."*

The Profession, Trade and Business Registration act specifies a penalty of \$500 and no imprisonment for this offence. Why the discrepancy? There should be harmonisation?

Section 68.3&4 (Page 75): *"The data controller and data processor shall ensure that the data privacy officer does not receive any instructions regarding the exercise of the duties and functions referred to in section 69."* and *"A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69."*

Two of these functions specified in Section 69 follow.

"A data privacy officer shall cooperate with the Commissioner" and "act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in section 66, and to consult, where appropriate, with regard to any other matter." (Section 69.1 (d & e))

This appears to make the data privacy officer the Commissioner's spy, but paid for and maintained by the company as per Section 68.2 below. It also appears to be micro-managing the private-sector post.

"The data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 69 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge." (Section 68.2)

Section 73.1 (Page 80): *"The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information."*

The last sentence appears to be a glaring loophole for mischief. If the Commissioner instructs his employee to release someone's personal information to one of their competitors, then while it is clearly unethical, this clause appears to make it legal.

Section 73.3 (Page 80): *"A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both."*

For releasing someone's personal information to one of their competitors, the fine should be a minimum of \$500,000.

Section 74 (Page 81): *"The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act."

This loophole seems to excuse professional negligence. The bill defines this as a professional post, and professionals cannot simply only say "sorry" for negligence without consequences. The standard should be the same for all professionals.

Section 75.1 (Page 81): *"The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct."*

Is there any penalty for not submitting the report within 3 months?

Section 79.1 (Page 84): Grammatical error. "... requiring the data controller to **furnishhim** with ..." should read "requiring the data controller to **furnish him** with ..."

Section 85.2(d) (Page 93): *"inspect and seize any documents or other material found on the premises;"*

Copies of documents may be seized, but the person should be allowed to make copies if the material seized is unrelated to the charge, and is part of his business, but belonging to another client.

Section 85.3 (Page 93): *"A judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect."*

What about educational institutions processing student records?

Section 89 (b) (Page 95): *"Any person who fails without reasonable excuse to give any police officer executing such a warrant **such assistance as he may reasonably require** for the execution of the warrant; is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 2 years or to both"*

So, if the person fails to help a police officer with a ladder, while that officer wants to search an elevated part of the property, is the person guilty of obstruction?

Section 93.3 (Page 98): *"A person who, contravenes subsection (1), is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 6 months or to both."*

Section 93.4: *A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.*

Section 93.5: *A person who offers to sell personal data is guilty of an offence where he has obtained the data in contravention of subsection (1); or he subsequently obtains the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.*

For revealing or selling personal information, the fine should be \$500,000. This is where persons will be likely tempted the most.

We trust that meaningful consideration will be given to our recommendations, and where there is disagreement, discussion will be allowed to facilitate a possible convergence of views.

Yours respectfully,

SOLUTIONS BARBADOS



Grenville Phillips II
President

Clerk of Parliament,
Parliament,
Government of Barbados
St Michael

Re: Comments On Data Protection Bill Barbados

Attention: Mr Pedro Eastmond

Dear Sir,

We need a Data Protection Bill

With a national debt over \$10 Billion BDS, it is essential that Barbados address its economic challenges through attracting foreign investment, bolstering tourism revenues and improving the productivity of its national workforce. This will require require the steady and measured adoption of new technologies within both the private and public sectors as well as the re-training of various customer-facing staff in order to facilitate increased trade and productivity by doing business online.

With this increased adoption of technology, Barbados is introducing a Data Protection Bill in order to address the current gaps in the protection of its citizen's data privacy rights as provided by the Laws of Barbados. This Data Protection Bill seeks to protect the privacy of individual's personal data by regulating the collection, keeping, processing, use and dissemination of personal data. Indeed, many Governments worldwide are following the standards set out by international laws such as the General Data Protection Regulation (GDPR), a regulation in EU law which aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Unfortunately, unlike the GDPR, the Barbados Data Protection Bill includes a loose definition of "personal data" which makes no distinction between which will negatively impact any entity (individual, organization or otherwise) which collects or aggregates data for commercial and non-commercial purposes. As a result, Barbados risks retarding the business activities of any such entity which may find it difficult to meet the necessary compliance requirements in terms of re-training, auditing, registration and purchase of necessary data management software

How small business may be negatively impacted

As previously mentioned, the Data Protection Bill 2019 introduces several punitive and onerous measures for any businesses which collect consumer data regardless of the nature of said data or the intended usage. This means that any business which maintains a list of telephone contacts for a few hundred customers via a Whatsapp group or email listing is subject to the same level of scrutiny as a Hospital which manages sensitive health information for all citizens of Barbados. Indeed, this Bill includes several onerous requirements for compliance which are not necessary for protecting the data privacy rights of the online citizen. A few examples of these requirements which may prove to be crippling to many small businesses (including snow-cone vendors and any retail store) are as follows:

1. Each company must hire and train a Data Privacy Officer, Data Processors and Data Controllers
2. Data Privacy Officer, Data Processors and Data Controllers are required to pay an undisclosed registration fee
3. Providing data audit reports to the Data Commissioner on an as-needed basis
4. Requiring (written) consent from each potential data subject
5. The data retention practices which may require the purchase of customized software

These measures may ultimately cause a regression in the current slow pace of adoption of technology among our small businesses since the hiring and training of new roles may force an artificial increase in the cost of doing business which may be passed onto the consumer. Additionally, the increased cost of adopting the necessary technology in mission-critical industries such as tourism, retail, and real estate may either force local operators to depend on overseas suppliers who may or may not be required to comply (due to their jurisdiction's regulations) or they may continue with using pen & paper for managing customer data.

Benefits of the Bill

There are indeed benefits to establishing this Data Protection Bill which include, but are not limited to, the following:

1. The online citizen needs to have their data privacy rights protected and will finally have recourse if their private information has been abused or used

without consent (e.g. if someone takes a photo of a couple at a party or an injured family member)

2. Policing of current bad actors among the business sector who have abused access to private customer contact information and resold it as email lists and whatsapp groups
3. Barbados will be able to address privacy concerns of doing business locally and introduce necessary measures of recourse for misuse of sensitive
4. Standardization of local software industry towards the adoption and promotion of privacy standards in the design and development of software
5. Data privacy laws will provide the necessary protections for the emergence of new technologies which can improve the standard of life locally such as in the industries of health analytics, telemedicine, electronic payments, etc

Consequences of the Bill

However, depending on the methods of enforcement and adoption of the Bill, there may also be several potential consequences particularly for a small business community which is currently being urged to improve their productivity and exports via the adoption of new technologies. These consequences include, but are not limited to, the following:

1. High cost of compliance for small businesses who need to hire/contract a Data Privacy Officer and train customer-facing staff who collect private information to become Data Controllers
2. Potential regression of the current trend of the adoption of software towards customer engagement in Barbados which is already painfully slow (e.g. lack of online shopping or online engagement with service providers)
3. Increased cost of doing business due to additional staff hires as well as need to purchase customized software suited to Barbados' Data Privacy
4. The need for data consent form needs to be clarified so that businesses will not burden customers with the need to sign several privacy disclosure forms in order to access their services
5. In-depth education campaigns are necessary for the business sector to ensure they understand the consequences of non-compliance as well as are made aware of suitable software service providers

Suggestions for improving the Bill

1. The requirements for compliance for businesses should match the level of access that company has to customer's private information such that a company that deals with sensitive information (e.g. health, banking, religion, etc) should be subject to further scrutiny than a company with limited access to only basic contact information (e.g. retail, general service providers, etc)
2. The fines should be adjusted to be a percentage of the gross revenue of the company in order to address the fact that large service providers have the most access to private data and would not be deterred by a \$500,000 BBD fine however a small business may indeed be crippled by such.
3. The enactment of the Data Protection Bill needs to be delayed or an interim period established until the measures of enforcement have been adequately clarified prior to enforcement. Similar to the enforcement of the GDPR, the Barbados Data Protection Bill may be enacted with a period of two to three years until it will be enforced.
4. A public education campaign is necessary in order to sensitize the public of their data privacy rights.
5. Business training sessions are necessary to educate and prepare the small and medium-sized businesses who are highly at risk of non-compliance. As per the GDPR, businesses should be required to adhere to established Codes of Conduct. The Bill should refer to the establishment of Codes of Conduct via consultation with the local business sector.

Additional Concerns

1. What provisions will be made for training small businesses who will need to drastically change business practices in order to avoid non-compliance?
2. Will consent from data subjects need to be collected in written format or is electronic format acceptable?
3. Considering that many small and medium-sized businesses depend on software services and technology platforms provided by foreign companies such as Google, Facebook and Microsoft for their daily business-critical practices, it should be considered that those companies are host to the majority of the sensitive data currently held on Barbadian citizens. Does this Data Protection Bill provide any recourse for data breaches on any of those technology platforms?

4. Will surveillance cameras be considered exempt from needing consent from data subjects? Or will businesses be unable to monitor the exterior of their environs?
5. Will credit reference companies be considered exempt? They are only mentioned once in the Bill in the list of definitions

Summary

The Barbados Data Protection Bill 2019 is timely and necessary to address the legislative gap in the protection of citizen's data privacy rights. However, as it is currently written, the Bill includes several requirements for compliance which are impractical for small and medium-sized businesses

Closing remarks

As Barbados moves steadily forward with its plans for Digital Transformation to revitalize its economy, it is necessary that the local and international business communities are not unnecessarily hindered or burdened by laws and regulations which do not serve to advance the adoption of new technologies which can improve worker productivity and customer service delivery.

Yours faithfully,

Mr Shannon Clarke
246-842-6587



Solving Problems that are Hindering Barbados' Development.

Tel: (246) 232-9783 • E-mail: NextParty246@gmail.com • Web: SolutionsBarbados.com

20th June 2019

Clerk of Parliament
Parliament Buildings
Heroes Square
BRIDGETOWN

Attention: Clerk of Parliament

Re: Data Protection Bill, 2019

Dear Sir:

We appreciate being allowed to comment on the Data Protection Bill (2019), before it becomes law.

Legislation should allow what is intended, and discourage what is not intended, but which may be inadvertently allowed. Therefore, we have reviewed the bill with the aim of helping to remove its vulnerabilities. For your convenience, both the Section references and page numbers are provided.

Preamble (Page 11): Grammatical errors are common throughout the document. While a common-sense read of the bill appears to allow it to be understood as intended, the errors should be cleaned up in the final version. We have identified some of the most glaring errors. "*provide for provide for matters*" should read "*provide for matters*".

Section 9.1(e)(iii) (Page 25): The non-consent processing of sensitive information by political parties, trade unions, or other groups is allowed, once the data belongs to their members. However, these groups are allowed to process the data of persons who "*have regular contact with it in connection with its purposes*" without their consent.

This should not be allowed. I may have regular contact with the union as an employer, but I do not consent to the union processing any of my sensitive personal information.

Section 10.3 (Page 28): "*The data controller shall provide a copy of the personal data undergoing processing to the data subject*" The data subject can also have their information amended (Section 11.1), and erased (Section 12.1), "*without undue delay*".

It is critical that the Data Controller verify the identity of the data subject before giving them any data, or amending or erasing any data. This verification addressed in **Section 21.14** below.

“Where a data controller has reasonable doubts concerning the identity of the individual making a request pursuant to sections 10 to 18, the data controller may request the provision of additional information necessary to confirm the identity of the data subject.” (Section 21.14)

The term “may” appears to make identity verification optional. May should be replaced with “shall” or “must”. Further, it should be mandatory that authentic verification documents should be presented before releasing someone’s data to a potential fraud.

Section 15.3 (Page 31): *“In exercising his or her right to data portability”*

The gender references should be consistent. Therefore, either mention both male and female, or mention male to mean both male and female, or make it gender neutral by using the plural, “their”.

Section 22 (Page 40): *“Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.”*

Section 23 tries to define “adequate”, and Section 24 tries to define “appropriate safeguards”. However, every country will likely claim that they meet the defined standard. For the avoidance of doubt, a schedule containing an approved list of countries, or a negative list of countries, should be part of the legislation.

Section 50.4 (Page 59): *“A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.”*

A data controller is anyone who is responsible for processing data, which can include every employer and educational institution. This needs clarification. Also, see Section 55.4 below.

Section 55.1 (Page 62): *“A person shall not operate as a data processor unless he is registered in the Register of Data Processors”*

If there is no separate registration act for the new profession, should it then be included the Profession, Trade and Business Registration act (Cap 373), like other professions.

Section 55.4 (Page 62): *“A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.”*

The Profession, Trade and Business Registration act specifies a penalty of \$500 and no imprisonment for this offence. Why the discrepancy? There should be harmonisation?

Section 68.3&4 (Page 75): *“The data controller and data processor shall ensure that the data privacy officer does not receive any instructions regarding the exercise of the duties and functions referred to in section 69.”* and *“A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69.”*

Two of these functions specified in Section 69 follow.

“A data privacy officer shall cooperate with the Commissioner” and *“act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in section 66, and to consult, where appropriate, with regard to any other matter.”* (Section 69.1 (d & e))

This appears to make the data privacy officer the Commissioner’s spy, but paid for and maintained by the company as per Section 68.2 below. It also appears to be micro-managing the private-sector post.

“The data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 69 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.” (Section 68.2)

Section 73.1 (Page 80): *“The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.”*

The last sentence appears to be a glaring loophole for mischief. If the Commissioner instructs his employee to release someone’s personal information to one of their competitors, then while it is clearly unethical, this clause appears to make it legal.

Section 73.3 (Page 80): *“A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both.”*

For releasing someone’s personal information to one of their competitors, the fine should be a minimum of \$500,000.

Section 74 (Page 81): *“The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act.”

This loophole seems to excuse professional negligence. The bill defines this as a professional post, and professionals cannot simply only say “sorry” for negligence without consequences. The standard should be the same for all professionals.

Section 75.1 (Page 81): *“The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct.”*

Is there any penalty for not submitting the report within 3 months?

Section 79.1 (Page 84): Grammatical error. *“... requiring the data controller to furnishhim with ...”* should read *“requiring the data controller to furnish him with ...”*

Section 85.2(d) (Page 93): *“inspect and seize any documents or other material found on the premises;”*

Copies of documents may be seized, but the person should be allowed to make copies if the material seized is unrelated to the charge, and is part of his business, but belonging to another client.

Section 85.3 (Page 93): *“A judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect.”*

What about educational institutions processing student records?

Section 89 (b) (Page 95): *“Any person who fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant; is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 2 years or to both”*

So, if the person fails to help a police officer with a ladder, while that officer wants to search an elevated part of the property, is the person guilty of obstruction?

Section 93.3 (Page 98): *“A person who, contravenes subsection (1), is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 6 months or to both.”*

Section 93.4: *A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.*

Section 93.5: *A person who offers to sell personal data is guilty of an offence where he has obtained the data in contravention of subsection (1); or he subsequently obtains the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.*

For revealing or selling personal information, the fine should be \$500,000. This is where persons will be likely tempted the most.

We trust that meaningful consideration will be given to our recommendations, and where there is disagreement, discussion will be allowed to facilitate a possible convergence of views.

Yours respectfully,
SOLUTIONS BARBADOS



Grenville Phillips II
President

SS/jb

June 25, 2019

Clerk of Parliament
Parliament
Parliamentary Building
BRIDGETOWN

Dear Sir,

**Re: Written Submissions presented to the Joint Select Committee of Parliament on the
Data Protection Bill, 2019("the Bill")**

The Barbados Bankers Association ("TBBA") welcomes the introduction of data protection legislation, which is beneficial to the public, private and public enterprises and the economy as a whole.

To be effective, however, the legislation should be implemented with as little disruption to businesses as possible. The banking industry in Barbados will be highly impacted by this legislation, as banks handle and process the personal data of tens of thousands of persons which has been collected over decades.

The most significant concerns of TBBA with the Bill, and our recommendations to address same are enclosed for your consideration.

Yours faithfully,


Donna Wellington
President

1. Financial records as “sensitive personal data” (section 2)

An individual’s “financial record or position” is classified as ‘sensitive personal data’ under the Bill. Such information is not treated as sensitive personal data under Article 9 of the General Data Protection Regulation (“the GDPR”), which binds the European Union (“EU”) and is considered to be the benchmark in data protection legislation.

It is recommended that “financial record or position” not be included in the list of personal data deemed to be sensitive personal data in keeping with the EU GDPR.

2. Credit Reference Agency (section 2)

Although a definition for ‘Credit Reference Agency’ has been included in the Bill, this term is not used anywhere in the Bill.

The Bill should carve out exemptions for registered or accredited Credit Reference Agencies as Barbados (through the Central Bank), is in the process of developing credit reporting legislation which makes it mandatory for credit providers to share certain information with a Credit Bureau, including financial information. The Data Protection Bill and credit reporting legislation should be consistent.

The proposed implementation of credit reporting legislation is intended to enhance the stability of the financial services sector in Barbados, and unduly onerous data protection requirements will make such services more difficult and expensive to secure.

Credit agency systems are not set up to erase customer data, and changes to system configuration and procedures are extremely costly. Accordingly, an individual’s ability to withdraw consent from the storing or processing of their data and the data controller/processor’s duty to erase data is not a practical or viable requirement.

3. Ensuring the reliability of employees that can access data (section 4(7))

The Bill requires a data controller to take reasonable steps to ‘*ensure the reliability*’ of any employees who have access to the personal data. This is vague and should be deleted or clarified.

4. Existing contracts with data processors (section 4(9))

Data can only be processed by a data processor under a written contract with a data controller.

This provision may require data controllers to (i) terminate existing contracts with data processors who are unable to comply with the Bill and implement new contracts with new

vendors who can comply, and/or (ii) renegotiate existing contracts with vendors who process data on their behalf.

The additional obligations imposed on data processors may result in higher fees or penalties for unilateral termination of existing contracts.

Key to cost and time effective negotiations will be the issue of model contract terms by the Data Protection Commissioner.

A transition period for implementation of the Bill would facilitate the above.

5. Lawfulness of processing (section 6)

Processing of data is deemed to be lawful only in certain circumstances, one of which is where it is necessary for compliance with a legal obligation. Section 6(1)(iii), however, exempts obligations imposed by contract. It is recommended that the exemption be deleted as unnecessary, as it is a basic principle in law that persons cannot contract outside of the law.

6. Children (sections 2 and 8)

It is recommended that “child” should be categorized as someone younger than 16 rather than 18 years old. It is noted that under the GDPR, member states may define a ‘child’ to be a person as young as 13 years old.

7. Processing of sensitive personal data (section 9)

Under section 9(1)(a), “written consent” is one of the grounds on which sensitive personal data (which is defined to include financial data), may be processed.

The requirement for consent in writing, does not take into account the various ways by which persons indicate their approval or consent in the technological age. It is also administratively onerous to banks which have hundreds of thousands of customers. It is recommended that “explicit consent” be used instead of “written consent”, as was done in the EU under the GDPR, which is a wider term.

Part V, titled ‘Exemptions’, exempts persons from the requirements under the Act, where such persons who process personal data solely for a reasons e.g. national security. Persons who only process personal data as part of staff administration should also be exempt.

8. Right to Erasure (section 12)

A data subject has the right to have his data erased by the data controller without undue delay. The data controller is also mandated to erase personal data, in certain circumstances. Erasure from all physical and electronic databases by a data controller and its processors will require for large multi-national banks, erasure in varying formats, in data bases in different countries and on multiple system platforms. This would be administratively challenging, and may not be possible for some computer systems which are not designed to erase information.

Banks systems are generally not set up to erase customer data, and changes to system configuration and procedures which might facilitate this, are extremely costly. An individual's right to request the erasure of his data is therefore not a practical or viable requirement.

In the event that this requirement is kept, a transition period of at least two years would facilitate the financing and implementation of the necessary technological changes to systems and processes.

9. Right to data portability (section 15)

Under section 15(1) of the Bill, data subjects will be entitled to receive the personal data they have provided to data collectors in a "*structured, commonly used and machine-readable format.*" In addition, section 15(2) allows data subjects to have such information transmitted directly to another data controller, but only where the processing of the data is carried out by automated means. In such a case, the data supplied would already be held in a machine-readable format.

Barbados does not currently have a framework for data protection, and data has accordingly not systematically been organized and filed in such a way as to be retrievable in machine readable format. Section 15(1) will require the transcription into electronic format of hundreds of thousands of files into machine-readable format should customers request their existing personal data. This will require significant time, human and technological resources and costs and impose a disproportionate burden on data controllers.

It is noted that under the EU GDPR, the right to data portability only exists where the processing of the data is carried out by automated means, and it is similarly recommended that section 15(1) require the same conditions as section 15(2).

10. Transfer of personal data outside of Barbados (sections 22 to 25)

Personal data may not be transferred to a country outside of Barbados unless (a) the country provides for an adequate level of protection for the rights of data subjects; (b) there are appropriate safeguards and legal remedies; and (c) data controllers and data processors develop

very detailed binding corporate rules. Where a data subject has given his consent to the transfer, and in other specified cases, (a) and (b) do not apply but binding corporate rules are still required.

Under the EU GDPR, data may be transferred to a country that has an adequate level of protection, as determined by an authority. This approach should be adopted instead. As such, the Data Protection Commissioner should determine whether any particular country has an adequate level of protection rather than require every data controller and processor to carry out his own costly assessment of the laws, international obligations, codes of conduct and security measures in another country.

Only in the absence of an assessment by the Data Protection Commissioner as to whether a country has an adequate level of protection should a data controller or data processor have the option to demonstrate that there are appropriate safeguards in place, and should not be a mandatory requirement for every data controller seeking to transfer data outside of Barbados.

11. Binding Corporate Rules (section 25)

At section 25(1)(c) data controllers and data processors are required to develop binding corporate rules which specify that they are legally binding both in and outside of Barbados. The reference to “outside of Barbados” should be removed as an entity cannot specify the legal effect of its rules in other countries.

12. Legal professional privilege (section 40)

This exemption should be widened to include information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

13. Registration as a data controller and data processor (ss 50 and 51)

It is recommended that persons who process personal data solely for a reason set out in Part V, titled ‘Exemptions’, should not be required to register as a data processor or data controller.

Persons who only process personal data as part of staff administration should also be exempt from registration.

14. Appropriate technical and organizational measures (ss 53, 58 and 62)

Section 53 of the Bill requires data controllers and processors to (i) implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the Act, and (ii) ensure the protection of the rights of the data subject.

Under section 62, the data controller and data processor are again required to implement appropriate technical and organizational measures.

It is recommended that the Data Protection Commissioner be required to issue codes of conduct and that these sections provide that adherence to such codes of conduct be capable of demonstrating compliance with the above-mentioned obligations. This will give far greater certainty of compliance.

15. Data Privacy Officer (section 68)

The Bill requires certain data controllers and processors, which will likely include banks, to engage a data privacy officer to be involved in all issues which relate to the protection of personal data. The data privacy officer must have expert knowledge of data protection law and practices and must report directly to the highest management level. Accordingly, banks may need to contract data privacy consultants and hire or identify and train data privacy officers, to facilitate implantation of the provisions of the Bill.

It should be made clear that the data privacy officer may be assigned other tasks and duties which do not pertain to the Bill, so long as there is no conflict of duty. This will allow banks to assign those tasks to an existing position without being forced to hire additional personnel.

Similarly, section 69 should make it clearer that the data privacy officer's duties include the list of duties listed but are not necessarily limited to the same.

A transition period of at least two years is necessary to facilitate the implementation of these provisions of the Act.

16. Functions of Commissioner (section 71)

The functions of the Data Commissioner should include the issue of model codes of conduct and approving same.

The Commissioner should also be empowered to issue advice to data processors and data controllers upon request.

17. Warrants (section 85)

A warrant can require any person on the premises to provide an explanation of any document found on the premises. This is not feasible or practicable. The person asked to explain the document should be duly authorised in writing.

In addition, where material to be seized or inspected consists partly of matters which do not fall under the warrant, the person executing the warrant should, upon request, provide the occupier with a copy of the material which is exempt.

18. Administrative penalty (section 94)

It is recommended that the Bill clarify that if a data controller or data processor, for the same or linked processing, breaches several provisions of the Act, the total penalty should not exceed \$50,000.00.

It is also recommended that where the Commissioner makes an order for an administrative penalty that notice of the order should be served on the relevant person and the 28 day deadline for appealing to the Tribunal should run from delivery, rather than the date of the order.

19. Processing of Historical Data

The Bill has no “grandfathering provision” for personal data collected without consent that meets the newly implemented standards. As such, historical data that may have been lawfully processed for decades under the broad based banker-customer consent and confidentiality provisions cannot be legally processed upon enactment of the Bill.

This will require data controllers and processors to either delete historical data, which is not viable; or seek new consent from existing customers. In the latter case, this could require a bank to seek the consent of tens of thousands of persons, and the data cannot be processed until the consents are obtained as the Bill does not provide for a transition period.

It would also be administratively onerous to manage the process of obtaining consents from existing customers as careful record would be required of consents received vs not, and data processed/not processed in accordance with same.

It is recommended that the legislation be applicable to information obtained on a go-forward basis and notice to existing customers suffice as consent.

Alternatively, a cut off period could be mandated, where historical data provided before the cut-off date is exempted from the application of any provisions under the Bill.

20. Employee data

Businesses that do not process large amounts of customer or vendor personal data are still likely to process the sensitive personal data of their employees. Those businesses will have to register as data processors/controllers and meet the requirements of the Bill.

This would require employers to obtain consent from employees to process their information for employment reasons. To accomplish this, trade unions or legal representatives may need to be involved in the process. Employers will also need to inform employees of the data collected and what the employer will do with it. Many employers will find that they are required to perform costly data impact assessments and even engage Data Privacy Officers.

Given the likelihood of business disruption and increased costs, persons who only process personal data as part of staff administration should also be exempt from registration.

If all employers are required to register and comply with the Bill, clear guidelines, training and education should be provided to all businesses, trade unions and members of the public to assist with their understanding of the Bill.

A generous transition period is required to facilitate the above.

Exemptions should be considered for small business, which are unable to bear the costs of compliance.

21. Liability of data controllers and data processors

It is recommended that the Bill specify whether the data controller and or the data processor is liable for the damage caused by processing which infringes the Act. The Act should also explicitly provide that data controllers and data processors are exempt from liability if they are not in any way responsible for the event giving rise to the damage.

22. Transition period

Many of the rights enjoyed by data subjects under the EU GDPR were provided under pre-existing data protection legislation that came into effect in 1995, albeit in a more limited format. Despite having this framework, the EU Parliament still deemed a two year transition period to be necessary for the GDPR to be effectively implemented. Barbados has no pre-existing data protection framework, and will be starting the process from far further behind than the EU countries.

A transition period of at least two years is vital for the legislation to have the desired effect and for businesses to grow during the implementation process.

23. Costs

The implementation and administration of the Bill will be extremely costly, particularly for the financial services sector which processes the information of tens of thousands of persons. The

estimated cost to business of implementation in the EU was approximately €200-300 per customer.

The administrative costs will have to be borne by the data controllers and data processors, as data subjects are not be required to pay any fees to enforce the rights given to them under the Bill. It is possible however, that the costs or part thereof may be passed on to the customer for businesses to remain viable.

The provisions of the Bill should also take into consideration the costs that will be incurred by the office of the Data Protection Commissioner in the exercise of its functions.

Barbados Bar Association
Written Submissions to The Joint Select
Committee of Parliament on the
Data Protection Bill, 2019

Table of contents

Executive Summary 2

GENERAL 4

PART I - PRELIMINARY 5

PART III - RIGHTS OF A DATA SUBJECT 7

PART IV - TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS 9

PART VI - DATA CONTROLLER AND DATA PROCESSOR 12

PART VII - DATA PROTECTION COMMISSIONER..... 14

PART X - MISCELLANEOUS PROVISIONS 15

Executive Summary

The Data Protection Bill is an important step in protecting Barbadians from fraudulent activity and unauthorized access of their personal data. The right of privacy and the protection of personal data must now enjoy the full protection of the law. It is enshrined in the Constitution of Barbados that every person in Barbados is entitled to the fundamental rights and freedoms of the individual, including protection for the privacy of his home and other property and to the protection of the law. The right to data protection was elevated to that of a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union. By Article 197 of the Economic Partnership Agreement 2008 between the European Union and the signatory CARIFORUM States, the parties recognised their common interest in protecting fundamental rights and freedoms of natural persons, and in particular, their right to privacy with respect to the processing of personal data.

It is important that the provisions of the Bill are such that it works to maintain an effective data protection regime which protects the rights and interests of the data subjects as consumers while allowing the transborder flows of information at a regional an international level.

The Barbados Bar Association makes a number of recommendations:

1. There is a call for the office of the Data Protection Commissioner to be afforded a much greater level of independence as the supervisory and regulatory authority charged with the administration of the Act. There should be far greater functional independence in the operation of the post.
2. While it is noted that the legislature may have imposed the criminal burden of proof standard in order to ensure compliance, it is submitted that this Bill should either impose civil liability alone or dual civil or criminal liability for more serious breaches.

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

3. As an adjunct to the Data Protection Bill, there is a call for supporting legislation or for amendments to existing electoral laws to protect the public from fraudulent and malicious manipulation of data to affect political outcomes.

The Barbados Bar Association is grateful for the opportunity, through the Clerk of Parliament, to submit its comments before the Joint Select Committee of both Houses of Parliament on the Data Protection Bill.

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

<u>Provision</u>	<u>Comment</u>	<u>Recommendation</u> <u>(where applicable)</u>
	<u>GENERAL</u>	
Regulations	It is important to include the draft regulations, otherwise there will be a lacuna between proclamation and implementation. It is always useful to hold consultations and discussions on the regulations in tandem with discussions on the Bill.	A draft of the regulations should be circulated for discussion.
Enforcement provisions generally	<p>Penalties for breach or failure to comply occur throughout the Bill. It is submitted that the Bill may be too ambitious in attaching criminal liability for most enforcement provisions.</p> <p>While it is noted that the legislature may have imposed the criminal burden of proof standard in order to ensure compliance with the Bill, it is submitted that this Bill should either impose civil liability alone or dual civil or criminal liability for more serious breaches for the following reasons:</p> <ul style="list-style-type: none"> • The criminal standard of 'beyond a reasonable doubt' may be too high a burden in many instances to prove that the offending party committed the breach in question. 	Consider the imposition of civil liability or administrative fines for breaches of the Act

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<ul style="list-style-type: none"> • Imposition of this criminal standard will only serve to further clog the criminal courts which are already overburdened with traditional criminal matters. • Given the specialised technicalities of the Bill, specialised judges would be best suited to deal with the adjudication of this Bill in circumstances where matters do not go before the Tribunal established under this Bill. • For many minor breaches under this Bill, the imposition of possible imprisonment terms is unnecessary. Imposing damages or compensation provisions should be adequate to deal with such breaches. The sanctions need to be effective, proportionate and dissuasive. More importantly, it can be a more practical and efficient means of regulating and administering the Act. <p>Where the offending party is a corporate entity, penalties may be imposed on a scale and on the basis of percentages of income or turnover, so that there is proportionality in the imposition of a fine.</p>	
	<p><u>PART I - PRELIMINARY</u></p>	
<p>Section 2 Interpretation</p>	<p>There are a number of references to 'court' in the Bill.</p>	<p>To avoid any ambiguity, where applicable, define 'Court' whether Magistrates Court, High Court or otherwise</p>
<p>Definition Of 'court'</p>	<p>In certain sections of the Bill, reference to the level of the Court, that is to High Court, is clearly specified, such as 21, and section 92 (Any party to an appeal to the Tribunal under section 91 may appeal from the decision of the Tribunal on a point of law to the High Court). In other</p>	

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p>sections, it is not clearly set out to which level of court a party should proceed. This should be clarified by defining Court.</p> <p>Not every reference requires definition, in particular if the reference is to any court or to the order of a court (as in section 38) or to a general reference to an order made by a court of competent jurisdiction (section 73)</p> <p>Other references which may have some ambiguity include:</p> <p>Right to prevent processing likely to cause damage or distress: Section 16(4) <i>Where a court is satisfied... the court may order the data controller to take such steps for complying with the notice as the court sees fit.;</i></p> <p>Right to prevent processing for purposes of direct marketing: Section 17(4) <i>Where a court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the court may order the data controller to take such steps for complying with the notice as the court sees fit.</i></p> <p>Binding corporate rules section 25 (1) (e) <i>the right to lodge a complaint with the competent supervisory authority or Commissioner and the courts</i> s. 82(1) and (2) - circumstances under which a court grants leave for a notice to be served; s. 88 - warrants;</p> <p>94(3) <i>Where the Commissioner makes an order under subsection (1) the Commissioner shall file in the registry of the Court a copy of the order certified by the Commissioner,</i></p>

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

<u>PART III - RIGHTS OF A DATA SUBJECT</u>		
Sections 10-21	<p>The Barbados Bar Association welcomes the establishment of rights of the data subject.</p> <p>The right to data protection was elevated to that of a fundamental right level in the Charter of Fundamental Rights of the European Union. The <u>EU Charter of Fundamental Rights Article 8</u> stipulates that EU citizens have the right to protection of their personal data. Some academics are of the view the provisions of the Charter in establishing the fundamental right goes further than the right to privacy.¹</p> <p>The right to privacy is established in section 11 of the Constitution of Barbados which provides:</p> <p><i>Section 11 provides:</i></p> <p><i>"11. Whereas every person in Barbados is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the individual rights and freedoms of others and for the public interest, to each and all of the following, namely-</i></p> <p><i>(a) life, liberty and security of the person;</i></p> <p><i>(b) protection for the privacy of his home and other property and from deprivation of property without compensation; (emphasis added)</i></p> <p><i>(c) the protection of the law; and</i></p> <p><i>(d) freedom of conscience, of expression and of assembly and</i></p>	<p>Examine the provisions of the Bill to ensure that the right to privacy is sufficiently grounded in the legislation or whether further amendments are necessary</p>

¹ Gonzalez Fuster, Gloria, 'The Emergence of Personal Data Protection as a Fundamental Right of the EU'

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p style="text-align: center;"><i>association,</i></p> <p><i>the following provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest."</i></p> <p>The question is whether there needs to be consideration for a further grounding of the right, or whether the existing constitutional provisions to the right to privacy as contained in the preamble are sufficient. In the CCJ case of <u>Nervais and Severin v The Queen</u>² the CCJ determined, for the first time, that the rights articulated in the preamble are enforceable. They stated: (para 17) "that section 11 declares the entitlement of the fundamental and inalienable rights of the citizens of Barbados" and (para 42) "we find that section 11 is separately enforceable."</p>	
<p>right to compensation</p>	<p>Section 25 (1) (e) of the Bill provides that Data controllers and data processors shall develop binding corporate rules which shall specify the rights of data subjects to obtain any other available form of redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>It is noted however in PART III that there is no specific right to compensation for the data subject. In the absence of a right to compensation for damage suffered arising whether in respect of material and non-material damage, then it places a burden to show and prove pecuniary or other loss. In the realm of data and privacy, infringements</p>	<p>Examine the provisions to determine whether the legislation should confer a right to compensation</p>

² [2018] CCJ 19 (A) CCJ This was a criminal appeal, and Court examined other provision of the preamble.

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	can be difficult to quantify. The question is whether data subjects would indeed pursue recourse under the Act against data processors who have infringed their rights.	
	<p style="text-align: center;"><u>PART IV - TRANSFERS OF PERSONAL DATA</u> <u>OUTSIDE OF BARBADOS</u></p>	
Sections 22-28	<p>It was clearly the intention of the legislature and an important facet of this Bill to hold foreign governments and foreign corporations/businesses liable for the processing of data of Barbadians as is evidenced by Part IV, Sections 22-28 of the Bill.</p> <p>Section 22 of the Bill speaks to a general principle for data transfers. This section states that the country or territory where data is transferred to must provide an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their data and appropriate safeguards for the processing of that data which include legal remedies for data subjects.</p> <p>Based on Section 23 of the Bill which speaks to what will constitute as adequate protection as stated in Section 22, enforcement of the protection of the data of Barbadians is dependent on whether the foreign country has adequate legislation, the laws in force in the country or territory in question and the international obligations of that country.</p>	

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p>If the country in which the company is domiciled has no or inadequate legislation, then there must be an examination of whether there would be inadequate legal recourse for data subjects in the event there is an infringement of rights and their data is misused.</p>	
	<p>In today's international business environment, a corporation may be domiciled anywhere in the world.</p> <p>The issue is whether there is a process to identify those countries/territories or foreign companies who regularly process the data of Barbadians and, where necessary, approach those countries or countries where those foreign companies are domiciled to enter into reciprocal agreements in order to enforce and give effect to Section 22 of the Bill. Such provisions cannot reasonably be enforced otherwise and it is submitted that Part IV of this Bill will largely be ineffective and wholly inadequate in holding such countries/ foreign companies otherwise accountable.</p> <p>This issue may be considered in light of many of the popular social media sites used by Barbadians and owned by the same group of companies (Facebook, Instagram, WhatsApp) and other popular sites and apps such as Google, or retail sites such as Amazon. These international media sites arguably process the data of a majority of Barbadians. We must examine the mechanisms to hold international companies responsible for this processing.</p> <p>In the event that the country of domicile is not compliant, are there mechanisms and appropriate safeguards to protect the data subject, for</p>	<p>Examine whether reciprocal agreements could provide greater safeguards for data subjects in the event of infringement of rights under the Act.</p>

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p>example, to censure or block from processing data any further until and or unless adequate legislation is passed.</p> <p>This is particularly important in light of the myriad of highly publicised privacy breaches committed within the last three years alone. Since issues surrounding Cambridge Analytica arose, governments in countries such as the United States and United Kingdom are still struggling come to terms with the repercussions of those breaches.</p> <p>The territorial scope of the Data Protection Bill is largely underpinned by other foreign actors performing certain actions (adequate legislation, international agreements, registering as data processors/ data controllers) in order for the rights of Barbadian citizens to be enforced.</p>	
	<p>There is a call to look at supporting legislation to hold foreign governments and/ or private companies accountable for instances where its agents manipulate the data of Barbadians to affect political outcomes. Additional legislation such as amendments to our existing electoral laws should also be considered.</p> <p>The consequences of Cambridge Analytica's actions and the implication of Facebook's possible role in some of these projects is not far removed from Caribbean or Barbadian society. There have been allegations of that company's involvement in regional affairs such as in Trinidad and Tobago, St. Lucia and St. Vincent and the Grenadians. In the peculiar case of St. Kitts and Nevis, a former Prime Minister was asked to testify on Cambridge Analytica's involvement in that country's political affairs before The Digital, Culture, Media and Sport committee (DCMS) of the</p>	<p>Call for supporting legislation or amendments to existing electoral laws to protect data subjects from fraudulent and malicious manipulation of data to affect political outcomes.</p>

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p>House of Commons of the Parliament of the UK House of Commons. The Report stemming from these hearings (DCMS Report) was published in February 2019 and may provide some guidance in tackling these new phenomenon of foreign actors using social media to affect political outcomes.</p> <p>Therefore, the threats faced by foreign entities in the possible electronic interference in democracy should not be taken lightly if we are to join other countries in tackling this new serious global threat.</p>	
	<p><u>PART VI - DATA CONTROLLER AND DATA PROCESSOR</u></p>	

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

<p>Sections 50 , 51 Data controllers must be registered</p>	<p>Sections 50 and 51 require data processors or data controllers to register and imposes fines and criminal sanctions on organisations who fail to do so.</p> <p>Where the offending party is a corporation, it is submitted that civil liability through the imposition of fines and penalties would be a more efficient means of enforcement. For example, imposition of a late fee or penalty.</p> <p>It is submitted that these provisions alone or a flat fine will not incentivise large foreign corporations with annual revenue earnings of billions of dollars to implement data protection policies in order to be in compliance with this Bill. As was recommended in this report under the 'General' section, where the offending party is a corporate entity, penalties may be imposed on the basis of percentages of income or turnover, so that there is proportionality in the imposition of a fine.</p>	<p>The provisions of this section should be carefully reviewed</p>
---	---	--

BARBADOS BAR ASSOCIATION
Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

Territorial scope	<p>In comparing this Bill with the European Union’s General Data Protection Regulation, Article 3 deals with territorial scope of that Regulation. Article 3 states that this regulation ‘applies to the processing of personal data of data subjects of the Union by a controller or processor not established in the Union (emphasis added) where such processing relates to the offering of goods and services regardless of whether payment is required and the monitoring of their behaviour as far as their behaviour takes place within the Union’. When benchmarked against this Data Protection Bill, the GDPR automatically imposes a burden or obligation on data controllers and data processors to be compliant with the Regulation once they process the data of EU citizens under the mentioned circumstances, regardless of whether such controllers or processors have registered as being controllers or processors of the data of EU citizens.</p> <p>(see comments under PART IV) - The territorial scope of the Data Protection Bill is largely underpinned by other foreign actors performing certain actions (adequate legislation, international agreements, registering as data processors/ data controllers) in order for the rights of Barbadian citizens to be enforced.</p>	Recommendation to consider whether can shift burden of compliance for processing the data
	<u>PART VII - DATA PROTECTION COMMISSIONER</u>	
Sections 70-75	The Bill establishes post of Data Protection Commissioner who is charged with the responsibility of general administration of the Act and is in fact the regulator.	Review provisions with a view to establishing greater independence

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<p>The role of the Data Protection Commissioner is extensive and wide ranging but also includes conducting investigations on the application of the Act; inquiring generally where it may appear that the privacy of persons in respect of personal data may be infringed; investigate complaints.</p> <p>The Data Commissioner must regulate the Act not only in respect of private individuals and private corporations, but also regulate the public sector and state owned entities.</p> <p>Moreover it is an important part of our international obligations as a nation to establish an independent supervisory authority to protect the right to privacy with respect to processing of data and to maintain effective data processing regimes.</p> <p>By Article 197 of the Economic Partnership Agreement 2008 between the CARIFORUM States and European Community, of which Barbados is a signatory, the parties agree to establish "appropriate legal and regulatory regimes, as well as appropriate administrative capacity to implement them, including independent supervisory authorities, (emphasis added) in order to ensure an adequate level of protection of individuals with regard to the processing of personal data, in line with existing high international standards"</p>	<p>as a supervisory authority</p> <p>Consider amendments Bill to allow for some element of:</p> <ul style="list-style-type: none"> • staffing independence • budgetary independence • security of tenure - barring mental incapacity or some other intervening circumstance, may not be removed from office for a period of years • functional independence - provisions expressly affirming the independence of the Data Privacy Commissioner
	PART X - MISCELLANEOUS	

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

<p>Section 99 Commencement</p>	<p>It is highly recommended that upon the passing of this Bill, a suggested grace period of at least 6 months to 1 year be inserted for the enforcement and commencement date of this Act for the following reasons:</p> <ul style="list-style-type: none">• By way of benchmarking, it is noted that the commencement date of the European Union's General Data Protection Regulation was May 31 2018, 2 years after the passage of this Regulation. Cf. GDPR Article 99(2).• The highly technical nature of this Bill and the obligations arising therefrom will require sensitization of the general public by way of mass public education campaigns on its implications.• Data subjects and data controllers alike in both the private and public sectors need time to fully understand the obligations that this Bill will place on state actors and the private sector. It will further take time to train employees on their duties relative to their organisation's implementation of data protection policies in compliance with the Bill.• State entities and private businesses will require time to become compliant with such obligations, particularly small businesses who will not easily have access to the resources (such as finances to seek legal/ICT advice, hire data protection officers, draft binding corporate rules and/policies regulating the processing of data within these organisations etc.) in order to do all that is required to be in compliance with this Bill.	<p>Establish a grace period of one (1) year for commencement of the Act</p>
------------------------------------	---	---

BARBADOS BAR ASSOCIATION

Written Submissions presented to The Joint Select Committee of Parliament on the Data Protection Bill, 2019

	<ul style="list-style-type: none">• The Government of Barbados may require time to appoint the Data Protection Commissioner, Data Privacy Officers and put adequate provisions in place for the establishment of the Tribunal and the appointment of the members of the Tribunal.	
	ENDS	

I welcome the opportunity to contribute to the Data Protection Bill, 2019, and I am supportive of efforts by the Government to protect the privacy of citizen's data. I present to you a Summary Brief on the Data Protection Bill and I would welcome the opportunity to make more substantive contributions at further intervals.

Abstract

Barbados is currently addressing a legislative gap by introducing the Data Protection Bill, 2019. The Bill seeks to protect the privacy of individual's personal data by regulating the collection, keeping, processing, use and dissemination of personal data. Although these are commendable steps, greater legislative scope must be considered as it relates to next-generation forms of data. These forms of sensitive data pertain to Social Networking Sites and Social Media Platforms. Increasingly, qualitatively and quantitatively, more personal and sensitive data can be obtained through these digital platforms, than through analogue mediums. Therefore, it is necessary that explicit legislative provisions are made that stipulate how social media data are governed.

Conceptualizing the importance of the social media in data protection

According to the Internet Society, Barbados has an 80% internet penetration rate while social media sites like Facebook are nearing 60%. Other high use social mediums include Twitter, professional networking sites such as LinkedIn, and social networking services such as Instagram. Due to the nature of interaction on these platforms there are high volumes of personal and sensitive data. Increasingly, it is more likely to uncover such data on these platforms, than can be retrieved at doctor's offices, financial institutions, places of study, governmental institutions and places of employment. This circumstance presents considerable issues regarding data privacy and the manipulation of data.

Threats to data-privacy and data manipulation

Threats to data-privacy and data manipulation have been evidenced in the region by the activities of Cambridge Analytica. The territories named in this scandal include Dominica, St. Lucia, Trinidad and Tobago, St. Kitts and Nevis, St. Vincent and The Grenadines and Antigua and Barbuda, while attempts have been made in Barbados. Cambridge Analytica unethically and illegally gathered user's Facebook data such as likes, comments, personal information and identifying markers. This data was used to formulate personality markers. Biased and fake news were subsequently peddled to individuals based on their personality markers with the intent to influence voting patterns. The Cambridge Analytical scandal highlighted that individuals' psychology can be tampered with without their knowledge and consent. Additionally, it highlighted the vulnerabilities of electoral systems and how democratic integrity can be undermined.

Main concern

Throughout the Bill, references are made to the protection of personal data as it relates to the use of social media. However, the same adequacy of protections are not afforded to what the Bill characterizes as sensitive personal data. Yet, it is the abundance of sensitive data that is generated or that can be determined through social media usage which present considerable challenges regarding data-privacy and manipulation. These include; gender; workplace; age;

language; location tags and user other generated such as posting, commentary and likes that could give considerable insight into owner's sensitive data. Therefore, considerations should be given into treating sensitive data to the same or similar degree that personal data receives.

Mitigating threats to data-privacy and sensitive data manipulation

Principally, data protection legislation should include a series of explicit regulatory measures that govern how sensitive social media data are protected, shared and processed by government and private enterprises. Where local or external companies track, analyze, share and process user's sensitive social media data, transparency, consent, privacy awareness and disclosure policies should be stipulated. These aspects should be provided to individual users and regulatory authorities when applicable.

Disclosure requirements for companies that process sensitive social media data

Companies that track, analyze, share and process user's social media data should disclose information to data owners about; what sensitive data are being collected; how sensitive data are used; how sensitive data are obtained; how the sensitive data is protected; the steps taken to comply with data protection legislation, and ensuring that outsourcing companies also meet disclosure requirements.

Disclosure should also involve details such as; the nature for sensitive data processing, type(s) of sensitive data that will be processed, the category of person who's sensitive data will be processed; whether there is sharing of sensitive data with other entities, and security protocols including encryption, restrictions on staff access, policies in the case of breaches, among others. In these instances, disclosure should pertain to individual users and regulatory authorities when applicable.

Protecting privacy through consent policies

Companies that track, analyze, share and process user's social media data should be granted permission by data owners through consent provisions. Additionally, when companies utilize sensitive social media data for advertising, competitions, tags and matching purposes, user permission should be granted. This consent should be provided through opt-in mechanisms. Opt-in consent should also be matched with revoking abilities insofar as no legal or contractual arrangements exists that prevent such a request.

Enhancing user's consent through increased transparency

The provision of meaningful consent should be matched with sufficient transparency, information and user awareness. Achieving these objectives require improving algorithmic transparency. Companies should inform data owners on; what sensitive data are collected; for what purpose is it collected, with whom are the sensitive data being used or shared, and what risk or harm could data owners face. This information should be presented visibly, in plain language, and in a user friendly way.

Enhancing user's control over data

Social media users should be afforded the ability to remove their data through the right to be forgotten principles. These principle are understood through erasure and de-indexing. Although the right to erasure is captured within the Data Protection Bill, the stipulations relate to the removal of inaccurate data. However, similarly to how users can delete their social media content, users should be able to instruct companies to remove their sensitive data. An additional approach could stipulate data storage time-periods during the user consent process.

Further considerations to improve data protection

Enhancing data protection may require improvements in the legislative frameworks that govern property and privacy. Various jurisdictions and social media platforms have, or are in the process of creating jurisprudence regarding social media content as property. These are evidenced by the U. S Bankruptcy Court for the Southern District of Texas, which held that businesses' social media accounts are property interests under the bankruptcy code. Additionally, under various social media platforms terms of service, the concept of ownership of social media content have been attributed to the owners of the accounts. Ownership proves important as it can help to determine and bolster privacy stipulations.

Steps should also be taken to enhance legislative frameworks on privacy. The Barbados Constitution simply makes reference to an individual's right to protect the privacy of their home and other property. However, territories such as Jamaica have enhanced their legal provisions on privacy. Jamaica's Charter of Fundamental Rights and Freedom Act grants the right to individuals to protect privacy, property and communication. This is particularly relevant in the case of social media data protection.

Final considerations should include user education to ensure users fully understand their rights and how to protect these rights. A cross-section of professions in the fields of law, computer science, cyber security and others, should be employed to address matters of enforcement. Consideration should also be given into including data protection diplomacy as part of Barbados' foreign relations, as our users utilize externally governed platforms.

Summary

Barbados' Data Protection Bill, 2019 is necessary. However, legislative considerations must be given to regulating social media use due to the quantity and quality of personal and sensitive data that reside on these platforms. Failure to do so can result in privacy and data manipulation concerns as seen with the Cambridge Analytica scandal. Subsequently, data protection must include; disclosure requirements; consent policies; increased transparency and greater user control over data. Additionally, considerations should be given to bolstering property and privacy legislative frameworks; data protection education, enforcement and data protection diplomacy.

Closing remarks

Social media use is likely to become more endemic within Barbadian society. Increasingly, social media content is an extension of ourselves and the data that is produced ought to be

sufficiently protected. Therefore, attempts at data protection ought not to be introductory but comprehensive in their outlook.

Devaron Bruce, MPhil Candidate.

CONCERNS RE DATA PROTECTION BILL 2019

8 (1) where the child is unconscious and no parent or guardian is available, medical emergency needs to be addressed.

9 (1) g speaks to law but no court order is necessary

and (l) (i) and (ii) health care professional- what about students- medical, nursing, pharmacy

9 (2) (3) (4) I do not understand what this is saying, what is a negative resolution and how exactly how exactly does this process work? So the minister may vary the act at will.

10 (2) How will the subject know? Who is to oversee that this is done and how will, they know? "shall have the right ..." to be informed by whom?

20 1, (f) unclear, exactly what is being said?

21 (16) what icons?

22, 23, 24 (a)- a legally binding.... Exactly what is this?

25 (3) isn't this micromanaging? In this case the commissioner is taking responsibility for the integrity and security of the data transmitted. This will also include the telecommunications industry. Very brave.

26 B (v) explain these circumstances.

(vi) (vii) (viii) - without a court order, automatically 22, 23 and 24 do not apply once a lawyer is involved. Defeats whole purpose of 22, 23 and 24.

27, fine of \$500 000.00 or 3 years or both on conviction, is excessive and draconian. what about public entities, who pays the fines? It said a **person** not corporation. Which public servant will be held accountable for data breaches? A doctor or nurse forgets to log out while attending to an emergency...

31 (3) non-disclosure does not apply with taxation. Carte blanche to BRA.

32 Health education social services – minors in educational institutions, personal data ...

45. appointments to the public services. I do not understand the need for this.

50 (2) another tax! what is this fee for? If the company is already registered in Barbados why pay another fee? If resident why pay a fee?

65 (5) publish the list when? By what month? Year end? how often?

69 Data privacy office is lawyer surprise, surprise !

70 Data Protection Commissioner is also a lawyer – advising on technical stuff but nothing in his qualifications state this. ridiculous! There needs to be 2 commissioners. A technical commissioner and a legal commissioner who report to and advise the minister.

73 (3) Oh so now when the commissioner or his staff breach the law they get a lesser fine of \$50 000.00 (10% of what we the masses get) and or 12 months in jail. One rule for the masses and another for the masters! The system is rigged!

74 they get immunity! System is rigged!

77 (2) you can appeal against the decision of the commissioner by writing to the commissioner! LOL, really now. Indeed system is rigged!

84 (3) electronic means—whats app? Twitter? Facebook post? Need to specify!

85 (2) LOL ..a person skilled in IT. That was not a requirement for the job of commissioner in 70!

86 (3) give to data comptroller OR owner of premises. This is not good, the owner should also receive a copy

87 2 (a) (b) lawyer client privilege. What about doctor patient confidentiality? The same protection should be extended to this relationship.

WHAT THE DATA PROTECTION BILL DOES NOT ADDRESS.

1. Health data-sharing and transmission among professionals-doctors, nurses, physiotherapists, social workers etc
2. On site and off site sharing.
3. Encryption protocols and standards
4. Storage- redundancy-back up off site storage, cloud storage,
5. Transportation- physical- jump drives, portable drives, laptops, smart phones, tablets COWS etc,
6. encryption technology, standards and protocols to be used.
7. Disposal of old storage data drives- software destruction protocols
8. Hard ware destruction process,
9. Disposal area-designated.
10. Duration of storage of medical data
11. Fate of data on retirement or death of a doctor.
12. Communication with patients with technology- webpage, whats app, email, twitter, smart phones etc
13. Electronic consent.

Dr Carlos A. Chase

P



Parliament,
Parliament Buildings,
Bridgetown,
Barbados, W.I.

Tel.: (246) 426-3717
436-0544
427-2019
Fax: (246) 436-4143

June 25th, 2019

Ms. Donna Wellington
President
Bankers Association of Barbados
CIBC First Caribbean
Warrens Head Office
Warrens
ST. MICHAEL

Dear Madam,

Re: Joint Select Committee on the Data Protection Bill, 2019

The Joint Select Committee (JSC) of both Houses of the Barbados Parliament has been given the responsibility to examine the provisions of the Data Protection Bill, 2019. The first meeting of the JSC took place on Monday, June 24th, 2019 in the Senate Chamber at 2:00 p.m.

We are therefore inviting your association to submit either written submissions or if representatives can make oral presentations before the JSC. The deadline for the written submissions is Thursday, June 27th, 2019. You may wish to visit the Barbados Parliament website at www.barbadosparliament.com to download a copy of the Data Protection Bill, 2019.

We apologise for the short notice for your response to this invitation.

Yours faithfully,


Peter Eastmond
Clerk of Parliament

Q

Parliament,
Parliament Buildings,
Bridgetown,
Barbados, W.I.



Tel.: (246) 426-3717
436-0544
427-2019
Fax: (246) 436-4143

June 25th, 2019

Ms. Liesel Weekes
President
Barbados Bar Association
"Leeton"
Perry Gap
Roebuck Street
Bridgetown
ST. MICHAEL

Dear Madam,

Re: Joint Select Committee on the Data Protection Bill, 2019

The Joint Select Committee (JSC) of both Houses of the Barbados Parliament has been given the responsibility to examine the provisions of the Data Protection Bill, 2019. The first meeting of the JSC took place on Monday, June 24th, 2019 in the Senate Chamber at 2:00 p.m.

We are therefore inviting your association to submit either written submissions or if representatives can make oral presentations before the JSC. The deadline for the written submissions is Thursday, June 27th, 2019. You may wish to visit the Barbados Parliament website at www.barbadosparliament.com to download a copy of the Data Protection Bill, 2019.

We apologise for the short notice for your response to this invitation.

Yours faithfully,

for

Pedro Eastmond
Clerk of Parliament

0

1000000

1000000

R



Parliament,
Parliament Buildings,
Bridgetown,
Barbados, W.I.

Tel.: (246) 426-3717
436-0544
427-2019
Fax: (246) 436-4143

June 25th, 2019

Dr. P. Abdon DaSilva
President
Barbados Association of Medical Practitioners (BAMP)
BAMP Secretariat
Spring Garden
ST. MICHAEL

Dear Sir,

Re: Joint Select Committee on the Data Protection Bill, 2019

The Joint Select Committee (JSC) of both Houses of the Barbados Parliament has been given the responsibility to examine the provisions of the Data Protection Bill, 2019. The first meeting of the JSC took place on Monday, June 24th, 2019 in the Senate Chamber at 2:00 p.m.

We are therefore inviting your association to submit either written submissions or if representatives can make oral presentations before the JSC. The deadline for the written submissions is Thursday, June 27th, 2019. You may wish to visit the Barbados Parliament website at www.barbadosparliament.com to download a copy of the Data Protection Bill, 2019.

We apologise for the short notice for your response to this invitation.

Yours faithfully,


Pedro Eastmond
Clerk of Parliament


8

2019/07/05

OBJECTS AND REASONS

This Bill would

- (a)* regulate the collection, keeping, processing, use and dissemination of personal data;
- (b)* protect the privacy of individuals in relation to their personal data; and
- (c)* provide for matters related to *(a)* and *(b)*.

Arrangement of Sections

PART I

PRELIMINARY

1. Short title
2. Interpretation
3. Application of Act

PART II

DATA PROTECTION PRINCIPLES

4. Principles relating to processing of personal data
5. Fairness of processing
6. Lawfulness of processing
7. Conditions for consent
8. Conditions applicable to child's consent
9. Processing of sensitive personal data

PART III
RIGHTS OF A DATA SUBJECT

- 10. Right of access**
- 11. Right to rectification**
- 12. Right to erasure**
- 13. Right to restriction of processing**
- 14. Notification regarding rectification or erasure of personal data or restriction of processing of personal data**
- 15. Right to data portability**
- 16. Right to prevent processing likely to cause damage or distress**
- 17. Right to prevent processing for purposes of direct marketing**
- 18. Automated individual decision-making, including profiling**
- 19. Information to be provided where personal data is collected from the data subject**
- 20. Information to be provided where personal data has not been obtained from the data subject**
- 21. Transparent information, communication and modalities for the exercise of the rights of the data subject**

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

- 22. General principle for transfers**
- 23. Adequate level of protection**
- 24. Appropriate safeguards**
- 25. Binding corporate rules**
- 26. Derogations**
- 27. Non-compliance**
- 28. Substantial public interest**

PART V

EXEMPTIONS

- 29. References to subject information provisions and non-disclosure provisions**
- 30. National Security**
- 31. Crime and taxation**
- 32. Health, education and social work**
- 33. Regulatory activity**
- 34. Journalism, literature and art**

35. Research, history and statistics
36. Manual data held by public authorities
37. Information available to the public by or under enactment
38. Disclosures required by law or made in connection with legal proceedings
39. Parliamentary privilege
40. Legal professional privilege
41. Domestic purposes
42. Confidential references given by the data controller
43. Armed forces
44. Judicial appointments and honours
45. Appointments to public service
46. Corporate finance
47. Negotiations with data subject
48. Examinations
49. Powers to make further exemptions by order

PART VI

DATA CONTROLLER AND DATA PROCESSOR

50. Data controllers must be registered

51. Register of Data Controllers
52. Notification of changes in respect of a data controller
53. Responsibility of the data controller
54. Data protection by design and by default
55. Data processors must be registered
56. Register of Data Processors
57. Notification of changes in respect of a data processor
58. Data Processor
59. Processing under the authority of the data controller or data processor
60. Records of processing activities
61. Cooperation with the Commissioner
62. Security of processing
63. Notification of a personal data breach to the Commissioner
64. Communication of a personal data breach to the data subject
65. Data protection impact assessment
66. Prior consultation
67. Designation of the data privacy officer
68. Position of the data privacy officer

- 69. Duties and functions of a data privacy officer**

PART VII

DATA PROTECTION COMMISSIONER

- 70. Data Protection Commissioner**
- 71. Functions of Commissioner**
- 72. Staff**
- 73. Confidential information**
- 74. Indemnity**
- 75. Report**

PART VIII

ENFORCEMENT

- 76. Enforcement notice**
- 77. Cancellation of enforcement notice**
- 78. Request for assessment**
- 79. Information notice**
- 80. Special information notice**
- 81. Determination by Commissioner as to the purposes of journalism or artistic or literary purposes**

- 82. Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes
- 83. Failure to comply with notice
- 84. Service of notice by Commissioner
- 85. Warrants
- 86. Execution of warrants
- 87. Matters exempt from inspection and seizure
- 88. Return of warrants
- 89. Obstruction of execution of a warrant

PART IX

DATA PROTECTION TRIBUNAL

- 90. Establishment of the Data Protection Tribunal
- 91. Right of appeal
- 92. Determination of appeals

PART X

MISCELLANEOUS

- 93. Right to compensation and liability
- 94. Unlawful obtaining of personal data

- 95. Administrative penalty
- 96. Disclosure of information
- 97. Act binds Crown
- 98. Amendment of *Schedule*
- 99. Regulations
- 100. Commencement

SCHEDULE

Data Protection Tribunal

BARBADOS

A Bill entitled

An Act to

- (a) regulate the collection, keeping, processing, use and dissemination of personal data;
- (b) protect the privacy of individuals in relation to their personal data; and
- (c) provide for matters related to (a) and (b).

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Data Protection Act, 2019*.

Interpretation

2. In this Act

“accessible public record” means any record that is kept by a public authority and to which members of the public are given access;

“accessible record” means

- (a) a health record;
- (b) an educational record; or
- (c) an accessible public record;

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual;

“child” means a person who is under the age of 18 years;

“Commissioner” means the Data Protection Commissioner referred to in section 70;

“consent” in relation to a data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him;

“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 such equipment;
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record; or
- (e) does not fall within paragraph (a), (b), (c) or (d) but is recorded information held by a public authority;

“data controller” means

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

“data privacy officer” means a person designated as such pursuant to section 67;

“data processor” means any person, other than an employee of a data controller, who processes personal data on behalf of the data controller;

“data subject” means an individual who is the subject of personal data;

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual;

“health care professional” includes a person who is registered under

- (a) the *Medical Professions Act* (Act 2011-1);
- (b) the *Dental Registration Act*, Cap. 367;
- (c) the *Nurses Act*, Cap. 372 or enrolled under that Act;
- (d) the *Pharmacy Act*, Cap. 372D; and
- (e) the *Paramedical Professions Act*, Cap. 372C;

“health record” means any record which

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

“personal data” means data which relates to an individual who can be identified

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

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

“process” in relation to information or data, means to obtain, record or hold the information or data or carry out any operation or set of operations on the information or data, including the

- (a) organization, adaptation or alteration of the information or data;
- (b) retrieval, consultation or use of the information or data;

- (c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

“profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

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

“public authority” means a public office or a ministry, department, agency, unit or other authority of the Government including a statutory body;

“recipient” means a person, public authority, agency or another body, to which the personal data is disclosed but a public authority shall not be considered a recipient where the personal data is received pursuant to an obligation imposed by the any enactment;

“relevant filing system” means any set of information relating to individuals to the extent that although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that the specific information relating to a particular individual is readily accessible;

“representative” means a representative of the data controller or data processor who is not established in Barbados and is nominated pursuant to

- (a) section 50(3) in respect of a data controller; or

(b) section 55(3) in respect of a data processor
and who represents that data controller or data processor with regard to their
obligations under this Act;

“restriction of processing of personal data” means the marking of stored personal
data with the aim of limiting their processing in the future;

“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) membership of a political body;
- (e) membership of a trade union;
- (f) genetic data;
- (g) biometric data;
- (h) sexual orientation or sexual life;
- (i) financial record or position;
- (j) criminal record; or
- (k) proceedings for any offence committed or alleged to have been
committed by him, the disposal of such proceedings or the sentence of
any court of competent jurisdiction in such proceedings;

“trade union” has the meaning assigned to it by the *Trade Unions Act*,
Cap. 361;

“Tribunal” means the Data Protection Tribunal established pursuant to section
90.

Application of Act

- 3.(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 Barbados;
 - (b)* the processing of personal data of data subjects in Barbados by a data controller or a data processor not established in Barbados, where the processing activities are related to the offering of goods or services to data subjects in Barbados.
- (2)** For the purposes of subsection (1) “established in Barbados” means
- (a)* an individual who is ordinarily resident in Barbados;
 - (b)* a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
 - (c)* a person who does not fall within paragraph *(a)* or *(b)* but maintains in Barbados an office, branch or agency through which he carries on any activity related to the processing of personal data.

PART II

DATA PROTECTION PRINCIPLES

Principles relating to processing of personal data

- 4.(1)** Personal data shall be
- (a)* processed lawfully, fairly and in a transparent manner in relation to the data subject;
 - (b)* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- (c)* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - (d)* accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- (2) A data controller shall, in relation to all of the personal data he processes, comply with the requirements set out in subsection (1).
- (3) A data controller may specify the purpose for which personal data is obtained pursuant to subsection 1(*b*)
- (a)* in any notice given for the purposes of section 5(3)(*a*) by the data controller to the data subject; or
 - (b)* in a notification given to the Commissioner pursuant to Part III.
- (4) In determining whether any disclosure of personal data is compatible with the purpose for which the data is obtained in accordance with subsection 1(*b*), regard is to be had to the purpose for which the personal data is intended to be processed by any person to whom the data is disclosed.

(5) Subsection 1(*d*) is not contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where

- (a) having regard to the purpose for which the data was obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and
- (b) the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicates that fact.

(6) Pursuant to subsection 1(*f*), having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to

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

(7) The data controller shall take reasonable steps to ensure that his employees who have access to the personal data comply with the requirements set out in subsection (1).

(8) Pursuant to subsection 1(*f*), where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall

- (a) choose a data processor who provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) take reasonable steps to ensure compliance with the measures referred to in paragraph (a).

(9) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with subsection 1(f) unless

- (a) the processing is carried out under a contract
 - (i) which is made or evidenced in writing; and
 - (ii) under which the data processor is to act only on instructions from the data controller; and
- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by subsection 1(f).

(10) A person who fails to comply with the requirements set out in subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Fairness of processing

5.(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 any 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

- (a) authorised by or under any enactment to supply the data; or
- (b) required to supply by the data any convention or other instrument imposing an international obligation on Barbados.

- (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; and
 - (iv) any 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) in any other case, 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 such a person 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 such a person within that period, the time when the data controller does become, or ought to become, so aware; or
 - (iii) in any other case, the end of that period.

Lawfulness of processing**6.(1) Processing shall be lawful where**

- (a)* the data subject has given consent to the processing of his personal data for one or more specific purposes; or
- (b)* the processing is necessary
 - (i)* for the performance of a contract to which the data subject is a party;
 - (ii)* for the taking of steps at the request of the data subject with a view to entering into a contract;
 - (iii)* for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
 - (iv)* in order to protect the vital interests of the data subject;
 - (v)* for the administration of justice;
 - (vi)* for the exercise of any functions of either House of Parliament;
 - (vii)* for the exercise of any functions conferred on any person by or under any enactment;
 - (viii)* for the exercise of any functions of a public authority;
 - (ix)* for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; or
 - (x)* processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which

require protection of personal data, in particular where the data subject is a child.

- (2) Subsection (1)(b)(x) shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for consent

7.(1) Where processing is based on consent, the data controller shall demonstrate that the data subject has consented to processing of his personal data.

(2) Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) A data subject has the right to withdraw his consent in respect of the processing of his personal data at any time and the data controller shall inform the data subject of his right to withdraw prior to him giving consent to the data controller to process his personal data.

(4) The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal.

(5) In determining whether consent is freely given, the data controller shall take into account whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Conditions applicable to child's consent

8.(1) The processing of a child's personal data shall be lawful only where and to the extent that consent is given or authorised by the parent or guardian of the child.

(2) The data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the parent or guardian of a child, taking into consideration available technology.

(3) Subsection (1) shall not affect contract law under any enactment in respect of the validity, formation or effect of a contract in relation to a child.

Processing of sensitive personal data

9.(1) Processing of sensitive personal data shall be prohibited unless

- (a) the data subject gives his consent to the processing;
- (b) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- (c) the processing is necessary in order to protect the vital interests of the data subject or another person, in a case where
 - (i) consent cannot be given by or on behalf of the data subject; or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject;
- (d) the processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- (e) the processing
 - (i) is carried out in the course of its legitimate activities by any body or association which
 - (A) is not established or conducted for profit; and
 - (B) exists for political, philosophical, religious or trade union purposes;
 - (ii) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
 - (iii) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and

- (iv) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (f) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- (g) the processing is necessary
 - (i) for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings;
 - (ii) for the purpose of obtaining legal advice; or
 - (iii) otherwise for the purposes of establishing, exercising or defending legal rights;
- (h) the processing is necessary for the administration of justice;
- (i) the processing is necessary for the exercise of any functions of either House of Parliament;
- (j) the processing is necessary for the exercise of any functions conferred on any person by or under an enactment;
- (k) the processing is necessary for the exercise of any functions of a public authority;
- (l) the processing is necessary for medical purposes and is undertaken by
 - (i) a health care professional; or
 - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
- (m) the processing
 - (i) is of sensitive personal data consisting of information as to racial or ethnic origin; and
 - (ii) is necessary for the purpose of identifying or keeping under review, the existence or absence of equality of opportunity or

treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and

(iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Minister may by order specify circumstances other than those identified in subsection (1) where sensitive personal data may be processed.

(3) An order made pursuant to subsection (2) is subject to negative resolution.

(4) For the purposes of subsection (1)(i) "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.

PART III

RIGHTS OF A DATA SUBJECT

Right of access

10.(1) A data subject has the right

- (a) to be informed by a data controller whether personal data of that data subject is being processed by or on behalf of the data controller;
- (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request from, and to be given by, the data controller, a description of
 - (i) the purposes of the processing;
 - (ii) the categories of personal data concerned;
 - (iii) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organisations;

- (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (v) the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (vi) the right to lodge a complaint with the Commissioner;
 - (vii) any available information as to their source, where the personal data is not collected from the data subject;
 - (viii) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (2) Where personal data is transferred to another country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 24.
- (3) The data controller shall provide a copy of the personal data undergoing processing to the data subject and where more copies are requested by the data subject, the data controller may charge a reasonable fee based on administrative costs.
- (4) Where the data subject makes the request for personal data by electronic means, and unless otherwise requested by the data subject, the personal data shall be provided in electronic form.
- (5) The right of the data subject to obtain a copy of personal data referred to subsection (3) shall not adversely affect the rights and freedoms of other data subjects.

Right to rectification

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

(2) Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed by the data controller, including by means of providing a supplementary statement.

Right to erasure

12.(1) The data subject shall have the right to obtain from the data controller the erasure of 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 is done pursuant to section 6(1)(a) or section 9(1)(a), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to section 16 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 17;
- (d) the personal data has been unlawfully processed;
- (e) the personal data has to be erased in compliance with a legal obligation in Barbados to which the data controller is subject.

(3) Where the data controller has made the personal data public and is obliged pursuant to subsection (1) or (2) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers who are processing the personal data that the data subject has requested the erasure

by such data controllers of any links to, or copy or replication of, the personal data.

(4) Subsections (1), (2) and (3) shall not apply to the extent that processing is necessary

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by any enactment 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 official authority vested in the data controller;
- (c) for reasons of public interest in the area of public health;
- (d) for archiving for the purposes of research, history or statistics in accordance with section 35; or
- (e) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

13.(1) The data subject shall have the right to obtain from the data controller restriction of processing of personal data where one of the following applies:

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

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

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

(3) A data subject who has obtained restriction of processing of personal data pursuant to subsection (1) shall be informed by the data controller before the restriction of processing of personal data is removed pursuant to subsection (2).

Notification regarding rectification or erasure of personal data or restriction of processing of personal data

14.(1) The data controller shall communicate any

- (a) rectification of personal data pursuant to section 11;
- (b) erasure of personal data pursuant to section 12; or
- (c) restriction of processing of personal data pursuant to section 13

to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The data controller shall inform the data subject about those recipients where the data subject requests such information.

Right to data portability

15.(1) The data subject has the right to receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format.

(2) The data subject has the right to transmit the personal data concerning him, which he has provided to a data controller to another data controller without hindrance where

- (a) the processing is based on consent pursuant to section 6(1)(a) or section 9(1)(a) or on a contract pursuant to section 6(1)(b)(i); and
- (b) the processing is carried out by automated means.

(3) In exercising his right to data portability pursuant to subsections (1) and (2), the data subject shall have the right to have his personal data transmitted directly from one data controller to another, where technically feasible.

(4) The exercise of the right referred to in subsection (1) shall be exercised without prejudice to section 12.

(5) The exercise of the right referred to in subsection (1) shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

(6) The exercise of the right referred to in subsection (1) shall not adversely affect the rights and freedoms of other data subjects.

Right to prevent processing likely to cause damage or distress

16.(1) Subject to subsection (2), a data subject is entitled, by a written notice, to require the data controller at the end of a 21 day period to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that

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

- (2) Subsection (1) does not apply
- (a) in a case where any of the conditions in section 6(1)(a) or (b)(i), (ii), (iii) or (iv) is satisfied; or
 - (b) in such other cases as the Minister may prescribe by order.
- (3) The data controller shall, within 21 days of receiving a notice under subsection (1), give the data subject written notice stating
- (a) that he has complied or intends to comply with the data subject's notice;
 - (b) the reasons for his refusal to comply with the data subject's notice; or
 - (c) the reasons for complying with part of the data subject's notice and the extent of that compliance.
- (4) Where the High Court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller in question has failed to comply with the notice, the Court may order the data controller to take such steps for complying with the notice as the Court sees fit.

Right to prevent processing for purposes of direct marketing

17.(1) A person is entitled at any time, by a written notice to a data controller, to require the data controller at the end of a 21 day period to cease processing for the purposes of direct marketing, personal data in respect of which he is the data subject.

(2) Where the High Court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the Court may order the data controller to take such steps for complying with the notice as the Court sees fit.

(3) For the purposes of this section "direct marketing" means the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.

Automated individual decision-making, including profiling

18.(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or similarly significantly affects him.

(2) Subsection (1) shall not apply where the automated processing or profiling of personal data is

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

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

(4) Subsection (2) shall not apply to sensitive personal data unless it is in the public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Information to be provided where personal data is collected from the data subject

19.(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 the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;

- (c)* the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
 - (d)* where the processing is done pursuant to 6(1)(b)(x), the legitimate interests pursued by the data controller or by a third party;
 - (e)* the recipients or categories of recipients of the personal data, if any;
 - (f)* where applicable, the fact that the data controller intends to transfer personal data to another country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers to the appropriate safeguards referred to in section 24 and the means by which to obtain a copy of them or where they have been made available.
- (2) In addition to the information referred to in subsection (1), the data controller shall at the time when personal data is obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
- (a)* the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (b)* the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
 - (c)* where the processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (d)* the right to lodge a complaint with the Commissioner;
 - (e)* whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well

as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- (f)* the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (3) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).
- (4) Subsections (1), (2) and (3) shall not apply where the data subject already has the information.

Information to be provided where personal data has not been obtained from the data subject

20.(1) Where personal data has not been obtained from the data subject, the data controller shall provide the data subject with the following:

- (a)* the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b)* the contact details of the data privacy officer, where applicable;
- (c)* the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d)* the categories of personal data concerned;
- (e)* the recipients or categories of recipients of the personal data, if any;
- (f)* where applicable, that the data controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers to the appropriate safeguards referred to in

section 24 Parliamentary Counsel and the means to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in subsection (1), the data controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) where the processing is done pursuant to section 6(1)(b)(x), the legitimate interests pursued by the data controller;
- (c) the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- (d) where processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (e) the right to lodge a complaint with the Commissioner;
- (f) from the source from which originated the personal data, and if applicable, whether it came from publicly accessible sources;
- (g) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) The data controller shall provide the information referred to in subsections (1) and (2)

- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data is processed;

- (b) if the personal data is to be used for communication with the data subject, at the latest, at the time of the first communication to that data subject; or
 - (c) if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.
- (4) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).
- (5) Subsections (1), (2), (3) and (4) shall not apply where and insofar as:
 - (a) the data subject already has the information;
 - (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes pursuant to section 35;
 - (c) obtaining or disclosure is expressly laid down by any enactment to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
 - (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by any enactment.

Transparent information, communication and modalities for the exercise of the rights of the data subject

21.(1) The data controller shall take appropriate measures to provide any information referred to in section 19 and section 20 and any communication under sections 10 to 18 and section 63 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

- (2) The information pursuant to subsection (1) shall be provided in writing, or by other means, including, where appropriate, by electronic means.
- (3) When requested by the data subject, the data controller may provide the information, pursuant to his rights under sections 10 to 15 and 18 orally, provided that the identity of the data subject is verified.
- (4) The data controller shall facilitate the exercise of data subject rights under sections 10 to 15 and 18.
- (5) The data controller shall provide information on action taken on a request under sections 10 to 15 and 18 to the data subject without undue delay and in any event within one month of receipt of the request.
- (6) The period of time referred to in subsection (5) shall be extended by two months where necessary, taking into account the complexity and number of the requests under sections 10 to 15 and 18.
- (7) The data controller shall inform the data subject of any extension granted pursuant to subsection (6) within one month of receipt of the request, together with the reasons for the delay.
- (8) Where the data subject makes the request pursuant to his rights under sections 10 to 15 and 18 by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- (9) Where the data controller does not take action on the request of the data subject under this section, the data controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Commissioner or appealing to the High Court.
- (10) Information provided under section 18 and section 19 and any communication and any actions taken under sections 10 to 15 and 18 and section 63 shall be provided free of charge.

(11) Where requests referred to in this section from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the data controller may either

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

(12) The data subject may object to the decision of a data controller made pursuant to subsection (11) by lodging a complaint with the Commissioner or appealing to the Tribunal.

(13) For the purposes of subsection (12), the data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of a request referred to in subsection (11).

(14) Where a data controller has reasonable doubts concerning the identity of the individual making a request pursuant to sections 10 to 18, the data controller may request the provision of additional information necessary to confirm the identity of the data subject.

(15) The information to be provided to data subjects pursuant to section 19 and section 20 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing and where the icons are presented electronically they shall be machine-readable.

(16) The Minister in consultation with the Commissioner, may make regulations for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

General principle for transfers

22. Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for

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

Adequate level of protection

23. For the purposes of section 22, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to

- (a)* the nature of the personal data;
- (b)* the country or territory of origin of the information contained in the data;
- (c)* the country or territory of final destination of that information;
- (d)* the purposes for which and period during which the data is intended to be processed;
- (e)* the law in force in the country or territory in question;
- (f)* the international obligations of that country or territory;
- (g)* any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and

- (h) any security measures taken in respect of the data in that country or territory.

Appropriate safeguards

24. For the purposes of section 22, appropriate safeguards may be provided for by

- (a) a legally binding and enforceable instrument between public authorities;
- (b) binding corporate rules in accordance with section 25;
- (c) standard data protection clauses prescribed by the Commissioner with the approval of the Minister;
- (d) contractual clauses authorised by the Commissioner between the data controller or data processor and the data controller, data processor or the recipient of the personal data; or
- (e) provisions, authorised by the Commissioner, to be inserted into administrative arrangements between public authorities which include enforceable and effective data subject rights.

Binding corporate rules

25.(1) Data controllers and data processors shall develop binding corporate rules which shall specify

- (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- (c) their legally binding nature, both in and outside of Barbados;

- (d)* the application of principles regarding purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of sensitive personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- (e)* the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with this Act, the right to lodge a complaint with the competent supervisory authority or Commissioner and the High Court and to obtain any other available form of redress and, where appropriate, compensation for a breach of the binding corporate rules;
- (f)* the acceptance by the data controller or data processor of liability for any breaches of the binding corporate rules;
- (g)* that the data controller or the data processor shall be exempt from the liability referred to in paragraph (f), in whole or in part, only where it is proven that the data controller or data processor is not responsible for the event giving rise to the damage;
- (h)* how the information on the binding corporate rules is provided to the data subjects;
- (i)* the complaint procedures;
- (j)* the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules;
- (k)* the mechanisms for reporting and recording changes to the binding corporate rules and reporting those changes to the supervisory authority;
- (l)* the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of

enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority or Commissioner the results of verifications of the measures specified in paragraph (j);

- (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

(2) The binding corporate rules referred to in subsection (1) shall be submitted to the Commissioner for authorisation.

(3) The Commissioner may specify the format and procedures for the exchange of information between data controllers, data processors and supervisory authorities for binding corporate rules.

(4) For the purposes of this section,

“binding corporate rules” means personal data protection policies which are adhered to by a data controller or data processor for transfers or a set of transfers of personal data to a data controller or a data processor in one or more countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

“enterprise” means a person engaged in an economic activity;

“group of undertakings” means a controlling undertaking and its controlled undertakings;

“supervisory authority” means an independent public authority which is established by in a country or territory outside of Barbados.

Derogations

- 26.** Section 22, 23 and 24 shall not apply where
- (a) the data subject has given his consent to the transfer of personal data;
 - (b) the transfer of personal data is necessary for
 - (i) the performance of a contract between the data subject and the data controller;
 - (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (iii) the conclusion of a contract between the data controller and a person other than the data subject which
 - (A) is entered into at the request of the data subject; or
 - (B) is in the interest of the data subject;
 - (iv) the performance of a contract described in subparagraph (iii);
 - (v) reasons of substantial public interest;
 - (vi) the purpose of, or in connection with, any legal proceedings including prospective legal proceedings;
 - (vii) the purpose of obtaining legal advice;
 - (viii) the purposes of establishing, exercising or defending legal rights; or
 - (ix) the protection of the vital interests of the data subject;
 - (c) the transfer of personal data is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer;

- (d) the transfer of personal data is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer of personal data has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

Non-compliance

27. A person who contravenes sections 22, 23 or 24 is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Substantial public interest

28.(1) The Minister may by order specify the

- (a) circumstances in which a transfer of the personal data of data subjects outside of Barbados is to be considered to be necessary for reasons of substantial public interest; and
- (b) circumstances in which a transfer of the personal data of data subjects outside of Barbados, which is not required by or under an enactment, is not to be considered necessary for reasons of substantial public interest.

(2) An order made pursuant to subsection (1) shall be subject to negative resolution.

PART V

EXEMPTIONS

References to subject information provisions and non-disclosure provisions

29.(1) In this Part

(a) “the subject information provisions” refers to

- (i) section 4(1)(a) to the extent to which it requires compliance with section 5(2); and
- (ii) section 10;

(b) “the non-disclosure provisions” refers to the following provisions to the extent to which they are inconsistent with the disclosure in question:

- (i) section 4(1)(a), except to the extent to which it requires compliance with the conditions in 6 and 9;
- (ii) section 4(1) (b), (c), (d), (e); and
- (iii) sections 11 to 18.

(2) Except as provided for by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding of information.

National Security

30. Parts II, III, IV, VI and section 79 do not apply where the processing of the personal data is required for the purpose of safeguarding national security.

Crime and taxation

31.(1) Personal data processed for

- (a) the prevention or detection of crime;

- (b) the apprehension or prosecution of offenders; or
- (c) the assessment or collection of any tax, duty or other imposition of a similar nature,

is exempt from section 4(1)(a), except to the extent to which it requires compliance with the conditions in section 6 and 9, and from section 10 in any case to the extent to which the application of those provisions to the data is likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Personal data which

- (a) is processed for the purpose of discharging statutory functions; and
- (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1)(a) to (c)

is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in subsection (1)(a) to (c).

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

- (a) the disclosure is for any of the purposes mentioned in subsection (1)(a) to (c); and
- (b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned in subsection (1)(a) to (c).

(4) Personal data in respect of which the data controller is a public authority and which

- (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 authority for any of the following purposes:
 - (i) the assessment or collection of any 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 of, or an unlawful application of, public funds; and

(b) is processed for either of those purposes

is exempt from section 10 to the extent to which the exemption is required in the interests of the operation of the system.

Health, education and social work

32.(1) The Minister may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data

- (a) consisting of information as to the physical or mental health or condition of a data subject;
- (b) in respect of which the data controller is an educational institution and which consist of information relating to persons who are or have been pupils at the educational institution;
- (c) in respect of which the data controller is a tertiary institution and which consist of information relating to persons who are or have been students at the tertiary institution;
- (d) of such other descriptions as may be specified in the order, being information processed
 - (i) by public authorities, charities or other entities designated by or under the order; and
 - (ii) in the course of, or for the purposes of, carrying out social work in relation to the data subject or other individuals.

(2) Notwithstanding subsection (1)(d), Minister shall not confer any exemption or make any modification under subsection (1)(d) except so far as he

considers that the application to the data of those provisions (or of those provisions without modification) is likely to prejudice the carrying out of social work.

(3) In subsection (1)

“educational institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41;

“tertiary institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41.

Regulatory activity

33.(1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed for the purpose of

- (a) protecting members of the public against
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;
 - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity;
- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;

- (c)* protecting the property of charities from loss or misapplication;
- (d)* the recovery of the property of charities;
- (e)* securing the health, safety and welfare of persons at work; or
- (f)* protecting persons other than persons at work against risk to health or safety arising out of, or in connection with, the actions of persons at work.

(3) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

- (a)* maladministration by public authorities;
- (b)* failures in services provided by public authorities; or
- (c)* a failure of a public authority to provide a service which it is a function of the authority to provide

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

(4) Personal data processed for the purpose of discharging any function which is designed for

- (a)* protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;
- (b)* regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
- (c)* regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market

is exempt from the subject information provisions to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

- (5) For the purposes of subsection (2) “relevant function” means
- (a) any function conferred on any person by or under any enactment;
 - (b) any function of a public authority; or
 - (c) any other function which is of a public nature and is exercised in the public interest.

Journalism, literature and art

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

- (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;
 - (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
 - (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the purpose of journalism or artistic or literary purposes.
- (2) In considering for the purposes of subsection (1)(b) 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 his compliance with any code of practice which is relevant to the publication in question and is designated by the Minister by order for the purposes of this subsection.
- (4) In any proceedings against a data controller where the data controller claims, or it appears that any personal data to which the proceedings relate are being processed
- (a) only for the purposes of journalism or for artistic or literary purposes; and

(b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time 24 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 (5) is met.

(5) The conditions referred to in subsection (4) 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.

(6) For the purposes of this section “publication”, in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

Research, history and statistics

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

(2) Personal data which is processed only for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from section 10 where

- (a) the personal data is processed in compliance with the relevant conditions; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

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

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

(5) In this section

“research purposes” includes statistical or historical purposes;

“the relevant conditions”, in relation to processing of personal data, means the conditions that the data

- (a) is not processed to support measures or decisions with respect to particular individuals; and
- (b) is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Manual data held by public authorities

36. Personal data which fall within paragraph (e) of the definition of “data” in section 2 is exempt from Parts II, III, IV and VI.

Information available to the public by or under enactment

37. Personal data is exempt from Parts II, III, IV and VI where the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

Disclosures required by law or made in connection with legal proceedings

38.(1) Personal data is exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the 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, or in connection with, any legal proceedings including prospective 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.

Parliamentary privilege

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

Legal professional privilege

40. 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.

Domestic purposes

41. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs including recreational purposes is exempt from Parts II, III, IV and VI.

Confidential references given by the data controller

42. Personal data is exempt from section 10 where it consists 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 any office; or
- (c)* the provision, or prospective provision, by the data subject of any service.

Armed forces

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

Judicial appointments and honours

44. Personal data processed for the purposes of

- (a)* assessing any person's suitability for judicial office or the office of Queen's Counsel; or
- (b)* the conferring by the Crown of any honour or dignity,

is exempt from the subject information provisions.

Appointments to public service

45. The Minister may by order exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for

- (a)* employment in the Public Service; or

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

Corporate finance

46.(1) Where personal data is processed for the purposes of, or in connection with, a corporate finance service

- (a) the data is exempt from the subject information provisions to the extent to which either
 - (i) the application of those provisions to the data could affect the price of any instrument which is already in existence or is to be or may be created; or
 - (ii) the data controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and
 - (b) to the extent that the data is not exempt from the subject information provisions by virtue of paragraph (a), the data is exempt from those provisions where the exemption is required for the purpose of safeguarding an important economic or financial interest of Barbados.
- (2) For the purposes of subsection (1)(b) the Minister may by order specify
- (a) matters to be taken into account in determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of Barbados; or
 - (b) circumstances in which exemption from those provisions is, or is not, to be taken to be required for that purpose.
- (3) In this section

“corporate finance service” means a service consisting of

- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
- (b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
- (c) services relating to such underwriting as is mentioned in paragraph (a);

“price” includes value.

Negotiations with data subject

47. Personal data which consist 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 in any case to the extent to which the application of those provisions would be likely to prejudice those negotiations.

Examinations

48.(1) The results of an examination are exempt from section 10.

(2) Personal data consisting of information recorded by candidates during an academic, professional or other examination is exempt from section 10.

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

Powers to make further exemptions by order

49.(1) The Minister may by order exempt from the subject information provisions personal data consisting of information the disclosure of which is

prohibited or restricted by or under any enactment where and to the extent that he considers it necessary for the safeguarding of

- (a) the interests of the data subject; or
- (b) the rights and freedoms of any other individual,

that the prohibition or restriction ought to prevail over those provisions.

(2) The Minister may by order exempt from the non-disclosure provisions any disclosures of personal data made in circumstances specified in the order, where he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other person.

(3) An order made under this section shall be subject to negative resolution.

PART VI

DATA CONTROLLER AND DATA PROCESSOR

Data controllers must be registered

50.(1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers.

(2) A person who desires to operate as a data controller may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data controller that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data controller who is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and

is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Controllers

51.(1) The Commissioner shall keep 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 pursuant to section 50, the following particulars:

- (a) the name and address and other contact information of the data controller;
- (b) the date of registration;
- (c) a description of the personal data processed by or on behalf of the data controller and of the categories of data subject to which they relate;
- (d) a description of the purposes for which the data is processed;
- (e) a description of any recipients to whom the data controller intends or may wish to disclose the data;
- (f) the names, or a description of, any countries outside Barbados to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and

- (g) where the data controller is not established in Barbados within the meaning of section 50(6), the name, address and other contact information of the representative nominated pursuant to section 50(3).
- (2) The Register of Data Controllers shall be open to inspection at the office of the Commissioner.
- (3) The Commissioner shall ensure that the Register of Data Controllers is kept accurate and up to date.

Notification of changes in respect of a data controller

- 52.(1) 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 in relation to him.
- (2) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register of Data Controllers as are necessary.

Responsibility of the data controller

- 53.(1) The data controller shall implement the appropriate technical and organisational measures to ensure that processing is performed in accordance with this Act taking into consideration the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to the rights and freedoms of individuals.
- (2) Where proportionate in relation to processing activities, the measures referred to in subsection (1) shall include the implementation of appropriate data protection policies by the data controller.

Data protection by design and by default

- 54.(1) The data controller shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement the

principles set out in section 4 in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects, taking into consideration the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

(2) The data controller shall implement the appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing is processed.

(3) Subsection (2) applies to the amount of personal data collected, the extent of processing of the personal data, the period of storage of the personal data and the accessibility to the personal data.

(4) The technical and organisational measures referred to in subsection (1) shall ensure that personal data is not, by default, made accessible without the individual's intervention to an indefinite number of individuals.

Data processors must be registered

55.(1) A person shall not operate as a data processor unless he is registered in the Register of Data Processors.

(2) A person who desires to operate as a data processor may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data processor that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data processor that is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and

is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Processors

56.(1) The Commissioner shall keep a register, to be called the Register of Data Processors, in which he shall cause to be entered in relation to each data processor, the following particulars:

- (a) the name and address and other contact information of the data processor;
- (b) the date of registration;
- (c) a description of the personal data processed by or on behalf of the data processor and of the categories of data subject to which they relate;
- (d) a description of the purposes for which the data is processed;
- (e) a description of any recipients to whom the data processor intends or may wish to disclose the data;
- (f) the names, or a description of, any countries or territories outside Barbados to which the data processor directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and

- (g) where the data processor is not established in Barbados within the meaning of section 55(6), the name, address and other contact information of the representative nominated pursuant to section 55(3).
- (2) The Register of Data Processors shall be open to inspection at the office of the Commissioner.
- (3) The Commissioner shall ensure that the Register of Data Processors is kept accurate and up to date.

Notification of changes in respect of a data processor

- 57.(1) 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 in relation to him.
- (2) On receiving notification of the data processor under subsection (1) the Commissioner shall make such amendments to the Register of Data Processors as are necessary.

Data Processor

- 58.(1) Where processing is to be carried out on behalf of a data controller, the data controller shall only use a data processor who shall implement the appropriate technical and organisational measures to ensure that processing will
 - (a) be in accordance with the requirements of this Act; and
 - (b) ensure the protection of the rights of the data subject.
- (2) The data processor shall not engage another data processor without prior specific or general written authorisation of the data controller.
- (3) Where there is general written authorisation pursuant to subsection (2), 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 such changes.

(4) Processing by a data processor shall be governed by a written contract between the data processor and the data controller which sets out the following:

- (a) the subject-matter and duration of the processing;
- (b) the nature and purpose of the processing;
- (c) the type of personal data and categories of data subjects;
- (d) the obligations and rights of the data controller.

(5) The contract prepared pursuant to subsection (4) shall also stipulate that the data processor

- (a) processes the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to countries outside of Barbados or an international organisation, unless required to do so by any enactment and in such a case, the data processor shall inform the data controller of that legal requirement before processing, unless the enactment prohibits such information to be shared on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to section 62.
- (d) respects the conditions referred to in subsections (2) and (7) for engaging another data processor;
- (e) taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights under Part III;

- (f)* assists the data controller in ensuring compliance with the obligations pursuant to sections 62 to 66 taking into account the nature of processing and the information available to the data processor;
 - (g)* on the determination of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless the enactment requires storage of the personal data;
 - (h)* makes 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, including inspections, conducted by the data controller or another auditor mandated by the data controller.
- (6) Where in relation to subsection (5)(h) an instruction from the data controller to the data processor infringes this Act, the data processor shall immediately inform the data controller.
- (7) Where a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller in accordance with subsection (2), the same obligations as set out in the contract between the data controller and the data processor as referred to subsections (5) and (6) shall be imposed on that other data processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Act.
- (8) Where that other data processor mentioned in subsection (7) fails to fulfil its data protection obligations, the initial data processor referred to in subsection (7) shall remain fully liable to the data controller for the performance of that other data processor's obligations.
- (9) The Commissioner with the approval of the Minister may prescribe standard contractual clauses for the matters referred to in subsections (5) and (7).
- (10) Where data processor contravenes this Act by determining the purposes and means of processing, the data processor shall be considered to be a data controller in respect of that processing.

Processing under the authority of the data controller or data processor

59.(1) The data processor and any person acting under the authority of the data controller or of the data processor, who has access to personal data, shall not process those data except on instructions from the data controller, unless required to do so by any enactment.

(2) A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

Records of processing activities

60.(1) A data controller and, where applicable, the data controller's representative, shall maintain a record of processing activities under its responsibility and that record shall contain all of the following:

- (a)* the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative and the data privacy officer;
- (b)* the purposes of the processing;
- (c)* a description of the categories of data subjects and of the categories of personal data;
- (d)* the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;
- (e)* where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
- (f)* where possible, the envisaged time limits for erasure of the different categories of data;

- (g) where possible, a general description of the technical and organisational security measures referred to in section 62(1).
- (2) A data processor and, where applicable, the data processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a data controller, which contains:

 - (a) the name and contact details of the data processor or data processors and of each data controller on behalf of whom the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the data privacy officer;
 - (b) the categories of processing carried out on behalf of each data controller;
 - (c) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
 - (d) where possible, a general description of the technical and organisational security measures referred to in section 62(1).

Cooperation with the Commissioner

61. A data controller and the data processor and, where applicable, their representatives, shall cooperate, on request, with the Commissioner in the performance of his tasks.

Security of processing

62.(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the data controller and the data processor shall implement appropriate technical and

organisational measures to ensure a level of security appropriate to the risk, including:

- (a) the pseudonymisation and encryption of personal data;
- (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;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

(3) The data controller and data processor shall take steps to ensure that any individual acting under the authority of the data controller or the data processor who has access to personal data does not process the personal data except on instructions from the data controller, unless he is required to do so by any enactment.

Notification of a personal data breach to the Commissioner

63.(1) Where there is a personal data breach the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

(2) Where the notification of the personal data breach to the Commissioner is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

- (3) The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.
- (4) The notification of the personal data breach to the Commissioner referred to in subsection (1) shall
- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data privacy officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- (5) Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- (6) The data controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in order to facilitate the Commissioner in his assessment of the data controller's compliance with this section.

Communication of a personal data breach to the data subject

- 64.(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.
- (2) The communication to the data subject referred to in subsection (1) shall describe in clear and plain language the nature of the personal data breach and

contain the information referred to in paragraphs (b), (c) and (d) of section 63(4).

(3) The communication to the data subject referred to in subsection (1) shall not be required where any of the following conditions are met:

- (a) the data controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise;
- (c) it would involve disproportionate effort and in such a case, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Data protection impact assessment

65.(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A single assessment pursuant to subsection (1) may address a set of similar processing operations that present similar high risks.

(3) The data controller shall seek the advice of the data privacy officer, where designated, when carrying out a data protection impact assessment.

(4) A data protection impact assessment referred to in subsection (1) shall in particular be required in the case of:

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

(5) The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to subsection (1) and the Commissioner shall publish that list in the *Official Gazette*.

(6) The Commissioner shall establish and make public a list of the kind of processing operations where no data protection impact assessment is required and the Commissioner shall publish that list in the *Official Gazette*.

(7) A data protection impact assessment referred to in subsection (1) shall contain

- (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in subsection (1); and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account

the rights and legitimate interests of data subjects and other persons concerned.

(8) Where appropriate, the data controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(9) Where necessary, the data controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Prior consultation

66.(1) The data controller shall consult the Commissioner prior to processing where a data protection impact assessment under section 65 indicates that the processing would result in a high risk to the rights and freedoms of an individual in the absence of measures taken by the data controller to mitigate the risk.

(2) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe this Act, in particular where the data controller has insufficiently identified or mitigated the risk, the Commissioner shall, within a period of up to 8 weeks of receipt of the request for consultation, provide written advice to the data controller and, where applicable to the data processor.

(3) The period mentioned in subsection (2) may be extended by 6 weeks, taking into account the complexity of the intended processing.

(4) The Commissioner shall inform the data controller and, where applicable, the data processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay.

(5) The period mentioned in subsection (2) may be suspended until the Commissioner has obtained information he has requested for the purposes of the consultation.

(6) When consulting the Commissioner pursuant to subsection (1), the data controller shall provide the Commissioner with:

- (a) where applicable, the respective responsibilities of the data controller and data processors involved in the processing, in particular for processing within a group of undertakings;
- (b) the purposes and means of the intended processing;
- (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Act;
- (d) where applicable, the contact details of the data privacy officer;
- (e) the data protection impact assessment provided for in section 65;
- (f) any other information requested by the Commissioner.

Designation of the data privacy officer

67.(1) The data controller and the data processor shall designate a data privacy officer in any case where:

- (a) the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
 - (b) the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c) the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.
- (2) A group of undertakings may appoint a single data privacy officer provided that a data privacy officer is easily accessible from each establishment.
- (3) Where a data controller or the data processor is a public authority or body, a single data privacy officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

- (4) In cases other than those referred to in subsection (1), the data controller or data processor or associations and other bodies representing categories of data controllers or data processors may designate a data privacy officer.
- (5) The data privacy officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions referred to in section 69.
- (6) The data privacy officer may be a staff member of the data controller or data processor, or fulfil the tasks on the basis of a service contract.
- (7) The data controller or the data processor shall communicate the contact details of the data privacy officer to the Commissioner.

Position of the data privacy officer

- 68.(1) The data controller and the data processor shall ensure that the data privacy officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- (2) The data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 69 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.
- (3) A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69.
- (4) A data privacy officer shall report directly to highest management level of a data controller or a data processor.
- (5) Data subjects may contact the data privacy officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.
- (6) A data privacy officer is required to keep confidential all matters concerning the performance of his duties and functions referred to in section 69.

Duties and functions of a data privacy officer

- 69.(1)** A data privacy officer shall
- (a)* inform and advise the data controller or the data processor and the employees who carry out processing of their obligations pursuant to this Act;
 - (b)* monitor compliance with this Act and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c)* provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 65;
 - (d)* cooperate with the Commissioner;
 - (e)* act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in section 66, and to consult, where appropriate, with regard to any other matter.
- (2)** A data privacy officer shall in the performance of his duties and functions under this section have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

PART VII

DATA PROTECTION COMMISSIONER

Data Protection Commissioner

70.(1) There shall be a public officer, to be called the Data Protection Commissioner, who shall be responsible for the general administration of this Act.

(2) A person is qualified to hold or to act in the post of Data Protection Commissioner, where that person is qualified to practise as an attorney-at-law and has so practised for a period of not less than 7 years, or for periods amounting in the aggregate to not less than 7 years.

(3) In this section “practise as an attorney-at-law” includes any period during which a person served as an attorney-at-law, advocate, barrister-at-law, solicitor, parliamentary counsel, magistrate or registrar of a court of competent jurisdiction in some part of the Commonwealth, or as a professor or teacher of law at the University of the West Indies or at a school for legal education approved by the Judicial and Legal Service Commission.

Functions of Commissioner

71. Without prejudice to the generality of the functions set out in this Act, 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) organise activities addressed specifically to children to educate them about the risks, rules, safeguards and rights in relation to processing;

- (e) conduct, at his own discretion or where requested to do so by any person, an audit of the personal data processed by the person, for the purpose of ascertaining whether or not the data is processed in accordance with this Act;
- (f) upon request, provide information to any data subject concerning the exercise of their rights under this Act;
- (g) monitor the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data, and
 - (i) report to the Minister on the results of that monitoring; and
 - (ii) where appropriate, make recommendations on the need for, or desirability of, taking legislative, administrative or other action to give protection or better protection, to the privacy of persons in respect of their personal data;
- (h) examine any proposed legislation or proposed policy of the Government that
 - (i) the Commissioner considers may affect the privacy of persons in respect of their personal data; or
 - (ii) provides for the collection of personal data by any public authority or the disclosure of personal data by one public authority to another public authority,and report to the Minister the results of that examination;
- (i) conduct investigations on the application of this Act, including on the basis of information received from a public authority;
- (j) receive and invite representations from members of the public on any matter affecting the privacy of persons in respect of their personal data;

- (k)* consult and cooperate with other persons concerned with the privacy of persons in respect of their personal data;
- (l)* make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interest of the privacy of persons in respect of their personal data;
- (m)* provide, at his own discretion or where requested to do so, advice to any Minister, public authority or person on any matter relevant to the operation of this Act;
- (n)* inquire generally into any matter, including any law, practice or procedure, whether governmental or non-governmental, or any technical development, where it appears to the Commissioner that the privacy of persons in respect of their personal data is being or may be infringed thereby;
- (o)* undertake research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons in respect of their personal data is minimised, and report to the Minister the results of such research and monitoring;
- (p)* report to the Minister on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of persons in respect of their personal data;
- (q)* monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- (r)* prepare appropriate codes of practice for the guidance of persons processing personal data;
- (s)* recommend the adoption and development of standard contractual clauses and standard data protection clauses pursuant to this Act;

- (t) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to section 65(5) and (6);
- (u) investigate complaints from persons concerning abuses in the processing of personal data;
- (v) approve binding corporate rules pursuant to section 25;
- (w) keep internal records of contraventions of this Act and of measures taken to address those contraventions;
- (x) do anything incidental or conducive to the performance of any of the preceding functions; and
- (y) exercise such other functions as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

Staff

72.(1) There shall be appointed to assist the Commissioner in the discharge of his functions such number of public officers as may be required.

(2) A person appointed pursuant to subsection (1) section is subject to the Commissioner's direction and control in the performance of functions under this Act.

Confidential information

73.(1) The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.

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

- (a) an order made by a court of competent jurisdiction;
- (b) a duty or obligation imposed by any enactment; or

(c) an international agreement to which Barbados is a party.

(3) A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both.

(4) In this section, “confidential information” means information of any kind and in any form that relates to one or more persons and that is obtained by or on behalf of the Commissioner for the purpose of administering or enforcing this Act or any enactment that the Commissioner has jurisdiction to administer or enforce, or that is prepared from such information, but does not include information that does not directly or indirectly reveal the identity of the person to whom it relates.

Indemnity

74. The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act.

Report

75.(1) The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct.

(2) A copy of the report of the Commissioner referred to in subsection (1) shall be printed and laid before both Houses of Parliament and published in the Official Gazette not later than 3 months from the date of receipt thereof by the Minister.

PART VIII

ENFORCEMENT

Enforcement notice

76.(1) Where the Commissioner is satisfied that a data controller or a data processor has contravened or is contravening this Act, the Commissioner may serve him with a notice, to be referred to as an “enforcement notice” requiring him, to do either or both of the following:

- (a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified; or
 - (b) to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing the personal data for a purpose so specified or in a manner so specified, after such time as may be so specified.
- (2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.
- (3) An enforcement notice shall contain
- (a) a statement of the provision of the Act which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion; and
 - (b) particulars of the right of appeal conferred by section 91.
- (4) Subject to subsections (5) and (6), an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the notice need not be complied with 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 notice a statement to that effect and a statement of his reasons for reaching that conclusion.

(6) Where subsection (5) applies, the notice shall not require the provisions of the notice to be complied with before the end of the period of 7 days beginning with the day on which the notice is served.

Cancellation of enforcement notice

77.(1) Where the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with this Act, he may cancel or vary the enforcement notice by written notice to the person on whom it was served.

(2) 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 notice on the ground that, by reason of a change of circumstances, all or any of the provisions of the notice need not be complied with in order to ensure compliance with the provisions of this Act to which the notice relates.

Request for assessment

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

(2) On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate, unless he is not supplied with such information as he may reasonably require 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 him to raise a matter of substance;
 - (b) any undue delay in making the request; and
 - (c) whether or not the person making the request has a right to access the personal data in question as specified in section 10.
- (4) Where the Commissioner has received a request under this section he shall notify the person who made the request
- (a) whether he has made an assessment as a result of the request; and
 - (b) to the extent that he considers appropriate, having regard in particular to any exemption from section 10 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

Information notice

- 79.(1) Where the Commissioner
- (a) has received a request under section 78 in respect of any processing of personal data; or
 - (b) reasonably requires any information for the purpose of determining whether a data controller has complied or is complying with the data protection principles,

he may serve the data controller with a notice, to be referred to as an “information notice”, requiring the data controller to furnish him with specified information relating to the request or to compliance with the provisions of this Act.

- (2) An information notice shall contain
- (a) in a case falling within
 - (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
 - (ii) 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
 - (b) particulars of the right of appeal conferred by section 91.
- (3) The Commissioner may specify in an information notice
- (a) the form in which the information must be furnished; and
 - (b) the period within which, or the time and place at which, the information must be furnished.
- (4) Subject to subsection (5), a period specified in an information notice under subsection (3)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the information need not be furnished 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, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event subsection (4) shall not apply, but the notice shall not require the information to be furnished before the end of the period of 7 days beginning with the day on which the notice is served.

(6) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of

(a) any communication between a professional legal adviser 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

(b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any 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 such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser includes references to any person representing such a client.

(8) A person shall not be required by virtue of this section to furnish the Commissioner with any information where the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence of perjury, expose that person to proceedings for that offence.

(9) Any 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, other than an offence under section 83, unless in the proceedings

(a) in giving evidence the person provides information that is inconsistent with it; and

(b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(10) The Commissioner may cancel an information notice by written notice to the person on whom it was served.

(11) This section has effect subject to section 82(3).

- (12) In subsection (1) "specified information" means information
- (a) specified or described in the information notice; or
 - (b) falling within a category which is specified or described in the information notice.
- (13) In subsection (9), "relevant statement", in relation to a requirement under this section, means
- (a) an oral statement; or
 - (b) a written statement made for the purposes of the requirement.

Special information notice

80.(1) Where the Commissioner

- (a) receives a request under section 78 in respect of any processing of personal data; or
- (b) has reasonable grounds for suspecting that, in a case in which proceedings have been stayed under section 34, the personal data to which the proceedings relate
 - (i) is not being processed only for the purposes of journalism or for artistic or literary purposes; or
 - (ii) is not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may serve the data controller with a notice, referred to as a "special information notice", requiring the data controller to furnish him with specified information for the purpose specified in subsection (2).

- (2) The purpose referred to in subsection (1) is the purpose of ascertaining whether personal data is being processed
- (a) only for the purposes of journalism or for artistic or literary purposes; or

- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.
- (3) A special information notice must contain
 - (a) particulars of the right of appeal conferred by section 91; and
 - (b) in a case falling within
 - (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
 - (ii) subsection (1)(b), a statement of the Commissioner's grounds for suspecting that the personal data is not being processed as mentioned in that paragraph.
- (4) The Commissioner may also specify in the special information notice
 - (a) the form in which the information must be furnished; and
 - (b) the period within which, or the time and place at which, the information must be furnished.
- (5) Subject to subsection (6), a period specified in a special information notice under subsection (4)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.
- (6) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event subsection (5) shall not apply, but the notice shall not require the information to be furnished before the end of the period of 7 days beginning with the day on which the notice is served.

(7) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of

- (a) any communication between a professional legal adviser 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
- (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any 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 such proceedings.

(8) In subsection (7) a reference to the client of a professional legal adviser include a reference to any person representing such a client.

(9) A person shall not be required by virtue of this section to furnish the Commissioner with any information where the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence of perjury, expose him to proceedings for that offence.

(10) Any 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 any offence under this Act, other than an offence under section 83, unless in the proceedings

- (a) in giving evidence the person provides information inconsistent with it; and
- (b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(11) In subsection (10) "relevant statement", in relation to a requirement under this section, means

- (a) an oral statement; or
- (b) a written statement made for the purposes of the requirement.

(12) The Commissioner may cancel a special information notice by written notice to the person on whom it was served.

(13) In subsection (1) "specified information" means information

- (a) specified, or described, in the special information notice; or
- (b) falling within a category which is specified, or described, in the special information notice.

Determination by Commissioner as to the purposes of journalism or artistic or literary purposes

81.(1) Where at any time it appears to the Commissioner, whether as a result of the service of a special information notice or otherwise, that any personal data is not being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; or
- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may make a determination in writing to that effect.

(2) Notice of the determination shall be given to the data controller; and the notice must contain particulars of the right of appeal conferred by section 91.

(3) A determination under subsection (1) shall not take effect until the end of the period within which an appeal can be brought and, where an appeal is brought, shall not take effect pending the determination or withdrawal of the appeal.

Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes

82.(1) The Commissioner may not serve an enforcement notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless

- (a)* a determination under section 81(1) with respect to those data has taken effect; and
- (b)* the High Court has granted leave for the notice to be served.

(2) The High Court shall not grant leave for the purposes of subsection (1) *(b)* unless he is satisfied

- (a)* that the Commissioner has reason to suspect a contravention of the data protection principles which is of substantial public importance; and
- (b)* except where the case is one of urgency, that the data controller has been given notice of the application for leave.

(3) The Commissioner may not serve an information notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless a determination under section 81(1) with respect to those data has taken effect.

Failure to comply with notice

83.(1) A person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence and is liable on summary conviction to a fine of \$15 000 or to a term of imprisonment of 6 months.

(2) A person who, in purported compliance with an information notice

- (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,

is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

(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.

Service of notice by Commissioner

84.(1) Any notice authorised or required by this Act to be served on or given to any person by the Commissioner may where the person is

- (a) an individual, be served on him by
 - (i) delivering it to him;
 - (ii) sending it to him by post addressed to him at his usual or last known place of residence or business; or
 - (iii) leaving it for him at that place; or
- (b) a body corporate or partnership, be served on it by
 - (i) sending it by post to the proper officer of the company at its principal office; or
 - (ii) addressing it to the proper officer of the partnership and leaving it at the office of the proper officer.

(2) This section is without prejudice to any other lawful method of serving or giving a notice.

(3) Nothing in subsections (1) and (2) precludes the service of a notice by electronic means.

Warrants

85.(1) Where a Judge of the High Court is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting that

- (a)* a data controller or a data processor has contravened or is contravening Parts II, III or IV; 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 any premises specified by the Commissioner,

the Judge may issue a warrant.

(2) A warrant issued, under subsection (1), shall authorise a police officer accompanied by the Commissioner, staff or such other person skilled in information technology as the police officer may deem necessary for the purpose, within 7 days of the date of the warrant, to

- (a)* enter the premises;
- (b)* search the premises;
- (c)* inspect, examine, operate and test any 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 any person on the premises to provide
 - (i)* an explanation of any document or other material found on the premises;
 - (ii)* such other information as may reasonably be required for the purpose of determining whether the data controller has contravened or is contravening Parts II, III or IV.

(3) A Judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect.

Execution of warrants

86.(1) A police officer executing a warrant may use such reasonable force as may be necessary.

(2) Where the person who occupies the premises in respect of which a warrant is issued is present when the warrant is executed, he shall be shown the warrant and supplied with a copy of it and where the person is not present, a copy of the warrant shall be left in a prominent place on the premises.

(3) A police officer seizing anything in pursuance of a warrant shall make a list of any items seized with the date and time of the seizure and shall give the list to

- (a) the data controller; or
- (b) the occupier of the premises.

Matters exempt from inspection and seizure

87.(1) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of personal data which, by virtue of section 30, is exempt from any of the provisions of this Act.

(2) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of any communication between

- (a) a professional legal adviser 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
- (b) a professional legal adviser and his client, or between such an adviser or his client and any 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 those proceedings.

Return of warrants

88. A warrant shall be returned to the High Court

- (a)* after being executed; or
- (b)* where not executed within the time authorised for its execution;

and the police officer by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him under the warrant.

Obstruction of execution of a warrant

89. Any person who

- (a)* intentionally obstructs a person in the execution of a warrant;
- (b)* fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant;
- (c)* makes a statement in response to a requirement under section 85(2) *(e)* which that person knows to be false in a material respect; or
- (d)* recklessly makes a statement in response to a requirement under section 85(2) *(e)* which is false in a material respect,

is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 2 years or to both.

PART IX

DATA PROTECTION TRIBUNAL

Establishment of the Data Protection Tribunal

- 90.(1)** There is established a tribunal called the Data Protection Tribunal.
- (2) The *Schedule* has the effect as to the constitution of Tribunal and otherwise in relation to the Tribunal.

Right of appeal

- 91.(1)** A person on whom an enforcement notice, an information notice or a special information notice has been served may appeal to the Tribunal against the notice.
- (2) A person on whom an enforcement notice has been served may appeal to the Tribunal against the refusal of an application under 77(2) for cancellation or variation of the notice.
- (3) Where an enforcement notice, an information notice or a special information notice contains a statement by the Commissioner in accordance with section 76(3), section 79(5) or 80(6) then, whether or not the person appeals against the notice, he may appeal against
- (a) the Commissioner's decision to include the statement in the notice; or
 - (b) the effect of the inclusion of the statement in respect of any part of the notice.
- (4) A data controller in respect of whom a determination has been made under section 81 may appeal to the Tribunal against the determination.
- (5) A person on whom an order has been made pursuant to under section 94 may appeal to the Tribunal against that order.

Determination of appeals

92.(1) Where on an appeal under section 91(1) the Tribunal considers

- (a)* that the notice against which the appeal is brought is not in accordance with this Act or any regulations made thereunder; or
- (b)* to the extent that the notice involved an exercise of discretion by the Commissioner, and it is determined that the Commissioner ought to have exercised his discretion differently,

the Tribunal shall allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner and in any other case the Tribunal shall dismiss the appeal.

(2) Upon appeal pursuant to subsection (1), the Tribunal may review any determination of fact on which the notice in question was based.

(3) Where on an appeal under 91(2) the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal shall cancel or vary the notice.

(4) On an appeal under 91(3) the Tribunal may direct

- (a)* that the notice in question shall have effect as if it did not contain any such statement as is mentioned in that subsection; or
- (b)* that the inclusion of the statement in accordance with section 76(3), section 79(5) or 80(6) shall not have effect in relation to any part of the notice, and may make such modifications in the notice as may be required for giving effect to the direction.

(5) On an appeal under section 91(4), the Tribunal may cancel the determination of the Commissioner.

(6) Any party to an appeal to the Tribunal under section 91 may appeal from the decision of the Tribunal on a point of law to the High Court.

PART X

MISCELLANEOUS

Right to compensation and liability

93.(1) An individual who suffers damage or distress due to any contravention of this Act by the data controller or the data processor is entitled to compensation from that data controller or the data processor for that damage.

(2) In proceedings brought by an individual pursuant to subsection (1), it is a defence for the data controller or the data processor to prove that he took all such measures in the circumstances as would be reasonably required to comply with the provisions of this Act.

Unlawful obtaining of personal data

94.(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 shows that
- (a) the obtaining, disclosing or procuring
 - (i) was necessary for the purpose of preventing or detecting crime; or
 - (ii) was required or authorised by or under any enactment, by 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, as the case may be, 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), is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 6 months or to both.
- (4) A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.
- (5) A person who offers to sell personal data is guilty of an offence where
 - (a) he has obtained the data in contravention of subsection (1); or
 - (b) he subsequently obtains the data in contravention of subsection (1)and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.
- (6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

Administrative penalty

95.(1) Where the Commissioner after a hearing determines that a person has contravened section 52(1), section 57(1) and sections 60 to 67 and the Commissioner considers it to be in the public interest to make an order, the Commissioner may order the person to pay to the Crown a penalty of an amount not exceeding \$50 000.

(2) In addition to the public interest, where the Commissioner seeks to make an order pursuant to subsection (1), he shall have due regard to the following:

- (a) the nature, gravity and duration of the contravention taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the contravention;
- (c) any action taken by the data controller or data processor to mitigate the damage suffered by data subjects;
- (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 or data processor gave notice of the contravention; and
- (h) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

(3) Where the Commissioner makes an order under subsection (1) the Commissioner shall file in the registry of the High Court a copy of the order certified by the Commissioner, and on being filed the order shall have the same force and effect, and all proceedings may be taken on it, as if it were a judgment of the High Court, unless an appeal has been filed pursuant to section 91.

(4) A penalty imposed by the Commissioner in the exercise of his powers under this Act shall be payable into the general revenue and may be recovered by the Crown as a civil debt and for the purposes of the proof of such debt a

certificate under the hand of the Commissioner shall be receivable in evidence as sufficient proof of such debt.

(5) A person aggrieved by an order made by the Commissioner pursuant to subsection (1) may appeal to the Tribunal within 28 days of the date of the order.

Disclosure of information

96. No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the Tribunal with any information necessary for the discharge of their functions under this Act.

Act binds Crown

97. This Act binds the Crown.

Amendment of *Schedule*

98. The Minister may by order amend the *Schedule*.

Regulations

99. The Minister may make Regulations generally for the purposes of giving effect to this Act.

Commencement

100. This Act comes into operation on a date to be fixed by proclamation.

SCHEDULE

(Section 90)

Data Protection Tribunal

Constitution

Members of the Tribunal

1.(1) The members of the Tribunal shall be appointed by the Minister by instrument in writing from among persons who appear to him to be qualified as having had experience of, and shown capacity in, matters relating to data protection and privacy or such other related discipline.

(2) The Tribunal shall comprise 5 members who shall be appointed by the Minister.

(3) At least one of the members of the Tribunal shall be an attorney-at-law of at least 10 years standing, and he shall be the Chairman of the Tribunal.

(4) The members of the Tribunal shall hold office for such period not exceeding 3 years as the Minister may specify in the instrument of appointment.

(5) The Minister shall appoint a person appearing to him to have the qualifications necessary for appointment under paragraph 1(3) to act temporarily in the place of the Chairman where the Chairman is absent or unable to perform his functions.

Resignation

2. A member of the Tribunal may at any time resign his office by instrument in writing addressed to the Minister and such resignation shall take effect from the date of the receipt by the Minister of that instrument.

Revocation of appointments

3. The Minister shall revoke the appointment of any member of the Tribunal where that member

- (a) fails to carry out any of the functions conferred or imposed on him under this Act;
- (b) becomes of unsound mind or becomes permanently unable to perform his functions by reason of ill health;
- (c) becomes bankrupt or compounds with, or suspends payment to, his creditors;
- (d) is convicted and sentenced to a term of imprisonment or to death; or
- (e) is convicted of any offence involving dishonesty.

Gazetting appointments

4. The appointment, removal or resignation of a member of the Tribunal shall be recorded in the *Official Gazette*.

Protection of the members of the Tribunal

5. No action, suit, prosecution or other proceedings shall be brought or instituted personally against a member of the Tribunal in respect of any act done in good faith in pursuance of their functions under this Act.

Remuneration of the members of the Tribunal

6. There shall be paid to the members of the Tribunal such remuneration and other such allowances as the Minister may determine.

**FIRST MEETING
OF THE
JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, 2018
HELD IN
THE HONOURABLE THE SENATE**

MONDAY, JUNE 24, 2019

First SESSION 2018-2023

PRESENT:

Senator the Hon Miss K. S. McCONNEY
(Madam Chairman)
Hon. D. D. MARSHALL, Q.C., M.P.
Hon. Miss C. Y. FORDE, M.P.
Hon. D. G. SUTHERLAND, M.P.
Mr. N. G. H. ROWE, M.P.
Senator R. J. H. ADAMS
Senator Miss C. N. DRAKES
Senator D. R. SANDS
Senator Miss A. M. WIGGINS
Senator K. J. BOYCE

Also Present were:

Miss SHAWN BELLE *(Senior Parliamentary Counsel)*
Mr. CHESTERFIELD COPPIN *(E-Commerce
Development Officer)*
Mr. STEVE CLARKE *(Advisory Partner, Deloitte)*
CLERK OF PARLIAMENT Pedro Eastmond
DEPUTY CLERK Nigel Jones
DEPUTY CLERK Miss Beverley Gibbons
Miss Suzanne Hamblin, *(LIBRARY ASSISTANT)*
PROCEDURAL OFFICER TO THE COMMITTEE
(Ag.)

ABSENT

Bishop the Hon. J. J. S. ATHERLEY, M.P.
Hon. Ms. C. S. V. HUSBANDS

THE CLERK: The first Order of Business would be to appoint a Chairman from the Committee and to take a Motion for such appointment.

Hon. D. D. MARSHALL: Colleagues, staff of Parliament and other distinguished individuals, I would like to propose that Senator McConney be appointed Chair of this Select Committee.

Senator R. J. H. ADAMS: I second that motion.

THE CLERK: Senator McConney, please take the Chair.

MADAM CHAIRMAN: Thank you very much, colleagues. Before we get into the Agenda I would like to invite a motion to have the amended agenda adopted.

Senator Miss A. M. WIGGINS: I am putting forward a motion that the amended Agenda be adopted.

Hon. D. D. MARSHALL: I second that motion.

MADAM CHAIRMAN: Thank you. The next item on the agenda is certainly to welcome all of you. I want to say thank you to all of the Members of the Honourable the Senate and the Honourable the House of Assembly for coming to participate and be part of this Joint Select Committee on the Data Protection Bill. As you know, the Bill is designed to regulate the collection, keeping, processing, use and dissemination of personal data and to protect the privacy of individuals in relation to their personal data. This is a brand new Bill. It never existed in Barbados before so we are breaking new ground in this regard.

For this Committee, the Terms of Reference which many of you would have received and the intention is to inquire into and determine whether the Bill as drafted fulfils the expressed objects of improving the protection of personal data. Secondly, to examine whether the Bill as drafted, will upon effective implementation contribute to an ethos of compliance with data protection; thereby promoting transparency and accountability. The Third aspect of the Terms of Reference is to make recommended changes if deemed necessary, to the Bill as drafted for further consideration by the Chief Parliamentary Counsel. With your permission, I will move to the next Item on the agenda which is the Quorum. I would wish to recommend that a quorum for the purpose of this Joint Select Committee be constituted of five persons, and I would like to put it to the Joint Committee as to whether or not this would be acceptable.

Hon. D. D. MARSHALL: Madam Chairman, I do not know that we should have a difficulty. The Joint Select Committee on Integrity in Public Life had a Quorum of five on a far weightier issue, and then I seem to recollect one or two other Joint Select Committees that also had five so, I would not want us to veer away from that unless we have good reason, and so I support your suggestion.

MADAM CHAIRMAN: Any other Members? May I invite a Motion for the Quorum to be set at five, please?

Asides.

Senator D. R. SANDS: I move that the Quorum be set at five.

Senator Miss C. N. DRAKES: I second that

Motion.

MADAM CHAIRMAN: I thank you. The next item on the Agenda is Technical Support, and for the duration of this Joint Select Committee for our work technical support will be provided by the Chief Parliamentary Counsel's Office in the person of the Senior Parliamentary Counsel, Miss Shawn Belle, who is here for that period. The No. 5 item on the agenda, if I may move to the next item, is Procedure. What I would propose is that we seek to wrap up the work of this Joint Select Committee and have it back to the Senate by.... just give me a minute to check the specific date. I thought I had written it here but I have not. Just give me a moment, please.

Asides.

MADAM CHAIRMAN: I propose to have it back for consideration to the Honourable the Senate by July 10th 2019, and for us to have it further prepared to be submitted to the Honourable the House of Assembly by July 23, 2019.

Asides.

MADAM CHAIRMAN: This is bearing in mind that once we take the Report back to the Senate and the Senate reads it for the third time, that would conclude the work for the Senate and then it would be ready to go down to the Honourable the House of Assembly. Effectively, what we want to do is to have the work of the Committee concluded so that the Report can be completed by the Chief Parliamentary Counsel and submitted to the Honourable the Senate by July 10, 2019. Is that reasonable? Are there any concerns?

Asides.

MADAM CHAIRMAN: Okay. One other aspect of Procedure that I would like to put to the Committee is this. The deadline for submissions to this Committee was set for Thursday, June 20, 2019. We have received several submissions, about five or six of them, and we have also received an additional request for one additional submission from Mrs. Anne Reid. I am not sure which organisation she is representing at this time because she wears many different hats. The question I would wish to put to the Committee is whether we should extend that deadline until this coming Thursday, to accommodate that additional submission. Would the Committee be open to that?

Asides.

MADAM CHAIRMAN: For the record, can someone please move a Motion that we extend the deadline for submissions until Thursday.

Senator Miss A. M. WIGGINS: Madam Chairman, I am making the submission that we extend the deadline until this Thursday because I actually always thought June 20, 2019 was a little bit too soon after the advertisement went out. Extending it, I think, may give her and possibly other persons who were preparing their submissions to send them in, so I think it is a good decision to make. Thank you, Madam Chairman.

MADAM CHAIRMAN: Excellent. I would also wish to put to the committee whether or not you would wish to have the presentation. In fact, let me

talk about the presentations first before I ask that question. The intention is that presentations will begin. Today's session will be a closed session, just us and the persons who will present after and that come Wednesday, starting at 10:00 in the morning, the presentations from those persons who have requested to present to this Committee that they start at 10:00 in the morning. As I said, so far we have about five of them and we believe we can get through them for the morning period just before lunch if everyone has about a half an hour at that time. Then we will break for lunch and after lunch, we will come back and consider the written submissions to see how those submissions may impact the Bill and to determine how we may wish to make adjustments or not to the Bill based on both the oral and the written presentations. I would invite you to read the presentations that would already have been submitted to you and the one at least that we know so far, that will be coming shortly, therefore, Wednesday's sessions will be a full day's session, starting at 10:00 a.m. going through the oral presentations, breaking for lunch and then in the afternoon, we come back and consider those written submissions and how they may impact the Bill and our own opinions that need to be inserted. Senator Wiggins.

Senator Miss A. M. WIGGINS: Thank you, Madam Chairman. I was wondering if – I am not sure if you said it just now because I did not hear – the session on Wednesday, if it will be publicly televised?

MADAM CHAIRMAN: Yes. I will put that to the Committee. Would you wish for it to be so?

Senator Miss A. M. WIGGINS: Yes, Madam Chairman. That is why I wanted to be sure what your thoughts were because in terms of even, addition to the extended deadline, I think people have not grasped yet that the Data Protection Bill is out there on the table and lots of times, even after July 24, 2019, you will be getting comments from people that they were unaware. I do believe that even if it is televised on Wednesday, and given that we have given the extension until Thursday, that more persons will want to make submissions. I think we are going to have to also consider that, whether we are going to allow additional persons because as you know, as soon as most things are in the public domain, people become more aware. The Barbados Government Information Service notice is not that impactful and as soon as the session on Wednesday is televised live, I am sure you will be getting more submissions and we might be looking at another extension.

MADAM CHAIRMAN: In that case, if we were to extend, may I propose to the Committee that we then we meet again on July 1, 2019 to consider those subsequent submissions?

Senator R. J. H. ADAMS: The question is, should we gauge the response to the televised hearing on Wednesday, on July 1, 2019 and make a decision based on renewed interest or additional interest to extend the hearings further?

MADAM CHAIRMAN: What I was suggesting was that anything that would have been

received by the new deadline would then be considered on July 1, 2019 bearing in mind the deadline and the timelines that we have for the final submissions on that point.

Senator Wiggins, when you talked about televised, were you talking about streaming as we do normally on Parliament television or where you thinking of something else?

Senator Miss A. M. WIGGINS: Yes, Madam Chairman.

MADAM CHAIRMAN: Okay. Then that clears that up. Any objections to the normal streaming via Parliament's channels? I'm being asked to break down how the presentations would be done - the oral presentations. What we are thinking is a ten minute...

The members indicated unanimously, no.

Hon. D. D. MARSHALL: Madam Chairman, while I think that consultation on a matter such as this is always a good thing, on behalf of the Cabinet let me say that there are some time imperatives that we face and in the interest of being open to the Committee we are in the process of implementing, I think you all would have seen it, the automated entry programme at the Airport and one of our practical challenges is our ability to receive and facilitate travellers from the European Union. It is no secret that our biggest market, I think, is England and cumulatively England, Germany and all of the other European Union passengers represent probably more than half of our air traffic. Unfortunately, because this requires the capturing and retaining of data on European Union citizens in an electronic environment then we are required to have a piece of legislation that will meet at least the European Union; minimum standards. There are other things that have to be done but this piece of legislation is one of them.

It is going to be very difficult for us to be able to achieve this very laudable aim at the Airport without getting this Bill done and out of the way. I do not think that there is any harm in keeping to our tight timelines simply because given the nature of this piece of legislation it is really not something that we would normally take to the public. We normally do a Joint Select Committee process where the piece of legislation is one that is likely to generate vast amounts of public interest and believe me this one does not, it is just one of those areas, and secondly where it is likely to affect the rights of people and so on, so I would like to urge, Madam Chairman, that while I support full public participation, there are some larger imperatives. I believe that anybody who is going to make a substantial and relevant contribution on this area is going to be somebody who is already immersed in it and seized in it. It is the nature of the rarefied atmosphere that data protection occupies, and given the level of technical expertise that is required - and I want to laud the Chairman for her foresight in at least helping to prepare us to be able to understand what these people are going to say by having these presentations today - anybody who wants to make a contribution on this will be somebody who knows it well and can make a

contribution in well under two weeks preparation time, so I will urge us to stay within the timeline so that we can move this thing swiftly along.

MADAM CHAIRMAN: Thank you, Attorney-General. I want to agree with what the Attorney-General has said but I also would wish to add that in arriving at this Bill, this would have been circulated more than a year ago and there were several contributions at that time that were taken on board in arriving at this particular Bill, so there have been several revisions that have been done just over a year ago, so it has been in the public's domain especially among the technical people, and I think you are absolutely right that the public also needs to be engaged in a significant way. I think you understand too also the imperatives that we are dealing with in terms of timelines. Are there any further comments on this?

CLERK OF PARLIAMENT: Madam Chairman, just so that I am clear, do we still send to those persons mentioned by Senator Wiggins and, if we do, are we still sticking to the deadline of Thursday? I just want to be sure on this.

MADAM CHAIRMAN: Committee. I am trying not to be a dictator.

Senator Miss A. M. WIGGINS: Madam Chairman, in relation to what you said just now if the Bill was in circulation for a year it certainly suggests then that persons would have had, but I did not know that, the opportunity to refashion the Bill as we have it today so one of the interesting people would have been the Bankers Association and the Medical Association. Do you know if they have more or less contributed to the construction of the Bill as it is now?

MADAM CHAIRMAN: I would want to give you accurate information so permit me to check and be able to get back to you on that.

Senator Miss A. M. WIGGINS: Thank you.

MADAM CHAIRMAN: I believe that the Senior Parliamentary Counsel would want to make a contribution.

Miss SHAWN BELLE: Good afternoon all. I just want to make an intervention to say that there have been several iterations of the Data Protection Bill, but in terms of contributions made by stakeholders, comments were received from the Barbados ICT Professionals Association, the Barbados Chapter of Information Systems Security Association and the Barbados Chapter of the Internet Society. Others were sent in as well so I just wanted to alert the Committee of that.

MADAM CHAIRMAN: This would have been over what period?

Miss SHAWN BELLE: Madam Chairman, specifically with those that I just read out they would have been within the last few months but my understanding is that over the years there have been a number of consultations that have taken place with stakeholders.

MADAM CHAIRMAN: Thank you. Has the Committee determined that we still need to send out to these individual stakeholders at this point in time, or should I simply rule?

Senator R. J. H. ADAMS: I think it is worth doing even if we do not get the full range of replies. I was not aware that a year had gone by on this consultation, and I think on the two points that Senator Wiggins raised or the two constituents, doctors and bankers, that it is worth knowing if they have not just been solicited but if they intend to reply or if it has fallen between two stools as far as I am concerned, so I am for the deadline but not such that it impacts the comments that the Attorney-General made.

MADAM CHAIRMAN: Well, I believe then that we will go ahead and send those out and understand what would happen at that point and we can be flexible, so before I move on, may I recap the procedures that we have agreed and invite a motion to adopt those procedures:

1. That we work towards a deadline of sending the final Report back to the Honourable the Senate at least on or before July 10, 2019.
2. That we then seek to have a deadline for submitting for consideration of the Honourable the House of Assembly by July 23, 2019;
3. That we do extend the deadline for submissions to Thursday, July 27, 2019;
4. That we do agree to have the contributions of those who wish to present to this Committee streamed via the Parliament's website;
5. That all presentations will start on Wednesday June 26, 2019, starting at 10:00 a.m. with 10 minutes per presentation and between 15 to 20 minutes for the questions of the Committee; and
6. That the Committee will receive oral presentations in the morning, break for lunch and then in the afternoon come back to give our consideration of the written submissions and to determine how we see these submissions written and oral, impacting the Bill and what changes we would agree to be made at that time.

MADAM CHAIRMAN: May I have a motion adopt these procedures as stated?

Senator K. J. BOYCE: Just one correction, Madam Chairman, you said the 27 of July, 2019, is that supposed to be the 27 of June, 2019?

MADAM CHAIRMAN: 27 of June, 2019, thank you.

Senator Miss. A. M. WIGGINS: Miss Madam Chairman, I beg to move the motion that these procedures be adopted.

This was seconded by Hon. D. D. MARSHALL.

MADAM CHAIRMAN: Thank you. Now, we are on the final item of the Agenda, which is presentations. We have invited a number of persons to make presentations to this Joint Select Committee. We have listened to all the Members of this Committee who have said, we want to learn a little more. This is a new Bill, we have read the Bill but we may have some questions, and so we have invited three presenters today, the first would present an overview of the Data Protection Bill, and that is Mr. Chesterfield Coppin, he is the E-commerce Development Officer. The second

presentation will be by our own Miss Shawn Belle, who is the Senior Parliamentary Counsel, who made significant contribution to drafting this Bill, and she will present on the provisions of the Data Protection Bill. The final presentation will be by Deloitte, Mr. Steve Clarke, who is the Advisory Partner and he will speak to us about best practices as it relates to Data Protection. I felt that given the questions that many of you raised with me, that it was important for us to give ourselves a good foundation, and I believe these three presentations will do just that. We will now invite the persons in and...

Senator K. J. Boyce: Madam Chairman, if I may?

MADAM CHAIRMAN: Yes.

Senator K. J. BOYCE: I indicated my difficulty later on this afternoon. I was wondering if to facilitate that difficulty, the order of the persons, I would be very interested to hear Miss Belle before I leave as well then perhaps Deloitte, and then perhaps the overview. So if I have to dip out, you know the overview could be... I do not know but that is subject to your... but I am very keen on hearing the perspective of Miss Belle, with regard to the...

MADAM CHAIRMAN: The provisions?

Senator K. J. BOYCE: Yes.

MADAM CHAIRMAN: How much time do you have? You know that was a logical provision, the overview then get into the meeting, then you understand best practices, so....

Senator K. J. BOYCE: The reason being Madam Chairman, I think is that we are all pretty much familiar with the big picture of the Bill, because it has been debated, and you led it out so thoroughly when you led it before us, Madam Chairman. So in terms of the, well at least the Members in the Upper House, Madam Chairman, who had the benefit of that presentation? I do recognise that our Attorney-General, as well as the other Members of Parliament did not have the benefit Madam Chairman of being there, so if that one indulgence could be granted, Madam Chairman, that will be my only request.

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Can we invite our guests? You all are very accommodating to your colleagues.

Asides.

MADAM CHAIRMAN: Thank you very much for coming gentlemen. I believe directly in front of us is, Mr. Chesterfield Coppin, who is by way of introductions, the E-commerce Development Officer. Next to him is, Mr. Steve Clarke, from Deloitte, Advisory Partner. Next to him is Mr. Charlie Browne, who is the Permanent Secretary at the Ministry of Innovation Science and Smart Technology. Gentlemen, just letting you know that contrary to the arrangements we had made previously, we have a Member of the Committee who needs to leave urgently and has asked the Committee, and the Committee has agreed, to

switch the order of the presentations. Now, we know we had a very logical order, but right now we are seeking to be accommodating, so all presentations will be done, but we would recommend that Miss Belle, would go first with the provisions of the Bill. Mr. Clarke, will go second with the best practices for Data Protection, and then Mr. Coppin would go last. So please, Miss Belle, if you can begin and you may sit and present.

Miss SHAWN BELLE: The greetings protocol having been observed, good afternoon to all. My name is Shawn Belle, and I am from the office of the Chief Parliamentary Counsel and I am here just to give a presentation on the Data Protection Bill. As you would know, the objectives of the Bill are to regulate collection keeping, and processing use and dissemination of personal data. To protect the privacy of individuals in relation to their personal data. Now, in relation to, just as a general break in terms of the derivation of the Bill's various parts, we have parts 2, 3, 4, and 6. Part 2 being on the Data Protection Principles, Part 3 being on the Rights of the Data Subject, Part 4 being the Transfer of Personal Data outside of Barbados, and Part 6 the Data Controller and the Data Processor. Those parts are generally informed by the general protection regulations of the European Union, and the citation is regulation EU 2016/679 of the European Parliament and Council of the European Union. This particular directive would have over ruled the EU directive 95/46/ EC. Further, Part 5 deals with exemptions, Part 8 deals with enforcement, work informed by the data protection law in Cayman Islands and the United Kingdom Data Protection Act, 1998. Part 7 deals with the Data Commissioner and is informed by general provisions relating to functionaries and Article 57 of the General Data Protection Regulations (GDPR) from the European Union. Part 9 deals with the data protection tribunal, and the schedule which deals with the constitution of the tribunal, those are general provisions related to the establishment of tribunals and clause 93 dealing with unlawful obtaining of personal data was informed by the Data Protection Law of the Cayman Islands and United Kingdom Data Protection Act.

Miss SHAWN BELLE: Clause 95 which deals with disclosure of information was informed by reference to general provisions related to appropriate disclosure. In terms of the salient features of the Data Protection Bill, we note some key definitions and terms. As you know, Clause 2 which is the Interpretation Clause of the Bill deals with terms and words used in the Bill that would aid in interpretation of its various provisions. Therefore, to speak to the general terms that should be highlighted, they are as follows:

- Personal Data means the data which relates to the individual who can be identified from the data; or from data together with other information which is in possession or likely to come into possession of the Data Controller;
- Sensitive Personal Data means personal data consisting of information on a data subject's

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

In terms of the personal data, there will be standards that will be required to protect the personal data but also special standards that will deal with protection of sensitive personal data, and this is that data that would usually be considered confidential. Often within the Bill, it would refer to "processing" or "process" of personal data which usually means as follows:

- In relation to information or data, means to obtain, record or hold the information or data or carry out any operation or set of operations on the information or data, including the organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data; disclosure of the information or data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data.

The "data subject" is the individual who is the subject of the personal data. This is the person who is supposedly protected by this Bill. Note, we are speaking about an individual and not a legal person; it is a natural person that you would be dealing with. Additionally, you should note the definition of "data controller" which is as follows:

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

Finally, the "data processor" means any person, other than an employee of a data controller, who processes personal data on behalf of the data controller. It is important to note the scope of the application of the Act. This in particular to those persons who are wondering about outside entities that would be regulated. You look to Clause 3 of the Bill which speaks to the Bill

applying to the processing of personal data in the context of the activities of a data controller or a data processor established in Barbados; or the processing of personal data of data subjects in Barbados by a data controller or a data processor not established in

Barbados, where the processing activities are related to the offering of goods or services to data subjects in Barbados.

Therefore, those data processors and data controllers who are not established, the scope that you would be regulating with those processing activities that are related to the offering of goods or services to data subjects in Barbados. This is very important to note. What it means to be established in Barbados is as follows in Clause 50(6):

- An individual who is ordinarily resident in Barbados; a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

This type of Establishment Clause has been requested to be in compliance with the Organisation for Economic Cooperation and Development (OECD) requirements to establish connection within the jurisdiction to prevent money laundering, recording and enforcement issues that have arisen over the years in relation to those standards. Moving onto the Data Protection Principles in particular which are informed by Article 5 of the GDPR, they seek to regulate the way persons, primarily data controllers and processors collect, keep, use or disseminate personal data with the objective to respecting an individual's right to privacy, while balancing the legitimate interests of others to keep and process as well.

This is set within the parameters of the Act. Going through specifically the Data Principles in Article 5 (1) of the GDPR, it requires that personal data shall be as follows:

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

In regards to "processed lawfully, fairly and in a transparent manner", the term "lawfully" is particularly discussed in Clause 6; the term "fairly" is particularly discussed in Clause 5 and you would see a discussion of what would be "transparent" in the context of Clause 19 (2) which speaks to information being provided.

Clause 20 (2) speaks to where the information to be provided deals with personal data that has not been obtained from the data subject. Transparent Information and Communication Modalities for the exercise of the rights of the data subject refers to if you are providing information it has to be legible and the person must have consent, *et cetera*. Those are the types of provisions you would be looking at when referring to processing in a transparent manner in relation to the data subject.

The other Data Protection Principles would also require that personal data shall be as follows:

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

Clause 9 imposes additional standards which must be adhered to when dealing with sensitive, personal data and these additional standards are also informed by Article 9 of the GDPR. It is important also to highlight the need for consent in relation to the processing of data. The standards for consent are informed by Articles 7 and 8 of the GDPR. There are general conditions for consent spoken to in Clause 7 which specifically deals with the Data Controller making sure that consent has been given. Particularly, if there is a declaration in written form that that consent is not clear in plain language.

Miss SHAWN BELLE: The data subject is free to withdraw consent. The Data Controller must verify that the appropriate consent is obtained where a child is concerned, and that is in pursuance of the provisions of the GDPR.

We go on to highlight the rights of the data subjects and PART III speaks to that generally. In brief, you have the right to access which was informed by Article 15 of the GDPR. It gives the data subject the right to access their personal data from the Data Controller; the right to rectification, meaning that they have the right to correct any personal data that is held by the Data Controller and that is informed by Article 18 of the GDPR; the right to erasure or the right to be forgotten, that is also informed by Article 7 of the GDPR and dealt with in Clause (12) which allows for the data subject to request from the Data Controller that their information be erased.

Miss SHAWN BELLE: The right to restriction of processing is informed by Article 19 of the GDPR. This makes provision for an obligation on the part of the Data Controller to notify the data subject about the rectification, erasure or restriction of their personal data.

There is also the right to the data portability which means that this should allow the data subject to have

their personal data transmitted from one Data Controller to another without undue hindrance. This is also informed by Article 20 of the GDPR and dealt with in Clause 15.

The right to prevent processing likely to cause damage or distress. This is also informed by Article 21 of the GDPR. Clause 16 makes provision for the right of the data subject to prevent the Data Controller from processing their personal data in a manner that will cause damage or distress to the data subject.

There is also the right to prevent processing for purposes of direct marketing. This is specifically retaining clauses from the United Kingdom Data Protection, 1998, because those provisions seem to have more protective force in relation to preventing processing for direct marketing purposes.

There is also the automated decision-making, including profiling. This is informed by Article 22 of the GDPR and in Clause 18 of the Bill it makes provision for the right of the data subject not to be subject to automated decision-making based solely on processing and particularly profiling.

Miss SHAWN BELLE: Madam Chairman, those are the main rights, there are other rights as well but I will go on to other matters that I think would need highlighting, and that leads me to the discussion of transfers of personal data out of Barbados. Now, under the former European Union directive the part, which is PART 4 of the Bill, would have been succinctly put as a data protection principle but what the GDPR has sought to do is to expand this protection to then have additional standards. So that, you would have the data protection principles that you would implement generally but then when you are transferring personal data outside of Barbados there are these additional grounds that have been expanded in PART IV and those are as follows:

(a) here is an obligation to provide adequate level of protection for the rights and freedoms of data subjects in relation to processing their personal data, and Clause 23 goes into a deeper discussion of what it would need to provide at an adequate level of protection;

(b) appropriate safeguards on the condition that the rights of the data subjects are enforceable and that they are available effective legal remedies for data subjects in the other jurisdictions to which you are transferring. Clause 24 speaks in more detail about how you would interpret that particular standard.

Clause 25 also provides for the adoption of binding corporate roles so that those corporate roles would be developed by the Data Controllers and the Data Processors and they are supposed to be approved by the Data Protection Commissioner to govern their personal data of data subjects

outside of Barbados.

Miss SHAWN BELLE: Madam Chairman, this is supposed to be an additional layer of protection for data subjects in that if it in a company format where these particular controller or processors would develop these standards so that within their normal processing or transactions they would have their own roles which are subject to compliance with the Act when enacted.

Madam Chairman, to go through some important actors in the context of the Data Protection Bill:

(a) here is the Data Subject which we discussed, person who would be the subject of protection under this Bill. As I said, that person is an individual and not a legal person; and

(b) here is also the Data Controller, that controller is required to be registered under Clause 50. Where they are not established in Barbados they must nominate a representative established in Barbados. The Data Controller is also responsible for maintaining records of processing activities pursuant to Clause 60, including –

(a) the name and contact details of the Data Controller the purpose of processing, the categories of data subject; and

(b) personal data and transfers of personal data outside the jurisdiction; among other obligations.

The Data Controller also deals with authorising all processing activities

Notifications of a personal data breach

They have to do [those notifications] within 72 hours of the breach

They also have obligations to conduct data protection impact assessment where new technologies may present high risk to the rights of individuals.

Miss SHAWN BELLE: Madam Chairman, all of these particular duties are things that are imposed under the GDPR, so that they are in compliance with that new directive.

Data Processor: all those definitions identified in the definition of “process,” those are the main functions that the Data Processor will be performing and they are usually under the authorisation of the Data Controller. They are also required to register under Clause 55 and they too have obligations to record the processing of activities and the development of technical and organisational measures, ensuring the security of the processing of data. These are also in line with the GDPR.

Miss SHAWN BELLE: Just one thing that I wanted to highlight in relation to the Data Processor. The role of the Data Processor, that has more emphasised focus in terms of regulation because under the EU directive,

their focus was more on the Data Controller, but it was recognised that the Data Processor should also have focus and their GDPR has I guess expanded the focus on regulating them more and making sure that they are adequately supervised and that is by the Data Controller in particular.

Miss SHAWN BELLE: We move onto the role of the Data Protection Commissioner. The Data Protection Commissioner has the responsibility of the general administration of the Act and the functions thereof would be set out in Clause 71. It should be observed that the Data Commissioner has administrative, investigative and enforcement functions. Among the administrative functions would be developing appropriate codes of practice for the guidance of persons in terms of personal data and recommending adoption and development of standard contractual clauses, standard data protection clauses approving corporate binding rules and examining proposed legislation or policy. It is also investigative functions particularly under Clause 78, where a request for assessment with the compliance with the Act can be done. Then there are also enforcement measures most notably under the enforcement notices pursuant to Clause 76 and he can also impose administrative penalties pursuant to Clause 94 in certain circumstances in the public interest. It should be noted that the Commissioner will be a public officer and the person holding that post would be a person who is qualified to practice as an Attorney-at-Law for a period of not less than seven years, or for periods amounting in aggregate to not less than seven years.

Miss SHAWN BELLE: We move onto the Data Privacy Officer. Now, this is a person who can be recruited as a new person under your organisation or can be appointed from within, but that person would be responsible for making sure that there is compliance with the Data Protection legislation within your organisation. The Data Controller or the Data Processor would be required to designate the Data Privacy Officer, where the processing is carried out by a public authority or body except for Courts in a judicial capacity. Court activity is of the Data Controller or the Data Processor consist of processing operations which by their virtue and scope require regular and systematic monitoring of data subjects on large or core activities of the Data Controller or the Data Processor which consist of processing on a large scale of sensitive personal data. This is one of the new features introduced by the GDPR and would not have necessarily been something that would have been emphasised by the previous EU standard.

Miss SHAWN BELLE: Finally, we deal with the Data Protection Tribunal under Clause 90 and the constitution of that Tribunal which is spoken to under Schedule of the Bill. The Tribunal will comprise of five members who will be appointed by the Minister in writing and they will be selected from persons who are suitably qualified with experience and has shown to have the capacity in matters relating to data protection and privacy and any other such discipline. The

Chairman of the Tribunal should be an Attorney-at-Law of at least ten years standing.

Speaking specifically to exemptions, Now you would have noticed that Part 5 deals with exemptions from the provisions of the Act and it is a very important part because generally, the exceptions fall within two specific categories, Subject Information Provisions or Non-Disclosure Provisions. The Subject Information Provisions are those that are exempt from the fair processing requirement or the right of subject access. Where the subject information provisions exemption applies to the Data Controller of the Data Processor, it means that the Data Controller or the Data Processor does not have to provide fair processing of information or accede to subject access requests. In terms of the non-disclosure provisions, those are the ones that are exempt from disclosure provisions provided for under Section 4.1, which deals with the data protection provisions, as well as Sections 11 – 18, which deals with the rights of the data subject. There are absolute exemptions as well. There will be absolute exemptions where it comes to national security, manual data held by public authorities as well as information made available to the public under an enactment or otherwise.

In terms of the enforcement provisions which are dealt with in Part 8, we have several different types of notices including enforcement notice, the information notice, and the special information notice. The enforcement notice is the main notice that is used where the Commissioner is compelling compliance with the general provisions of the Act. The notice can be cancelled or altered on the initiative of the Commissioner on request to do so by a person to whom the notice is served. There is the information notice which is used to compel information from persons and then the special information notice which is a notice that is used in the context of probably prosecuting the idea of persons who are seeking to deal with exemptions for journalistic purposes. That is the notice that is specific to trying to work out issues in relation to that particular purpose. Other methods of enforcement include the request for assessment which can be made to the Commissioner and then the Commissioner can also apply to the Judge for a warrant to facilitate his investigation or enforcement and he can be facilitated to allow for entry onto property searches and inspection of documents and seizure of items.

Just in relation to offences, as you know there are offences that attract fines that would be from \$10 000.00 to \$500 000.00, and terms of imprisonment from two months or more or to three years. Now it should be pointed out that in Barbadian legislation the penalty is expressed at its maximum, so the maximum threshold is spoken to in the legislation which means that the judge would have the discretion for imposing no penalty at all or the highest threshold. That is how you need to understand the penalty provisions in Barbadian legislation. It is not fixed penalties, it is more than you have that deemed expression is at its maximum. This is supported by the Interpretation Act so that you can consult that Act for more clarification.

Miss SHAWN BELLE: It should also be noted that in a previous iteration of the Bill, the Ministry was criticised for how low the penalties were and so in relation to that we then tried to maximise them. The comments on the Data Protection Bill from the Barbados Information Communication Technology Professionals Association, the Barbados Chapter of the Information Systems Security Association and the Barbados Chapter of the Internet Society were taken into account so that they are reflected in the Bill. In terms of administrative penalties, you should note that the Commissioner does have the power to impose them except in terms of penalties that do not exceed \$500 000.00, and he will do that in the public interest but he has to take into account the nature and gravity and duration of the contravention, the intentional and negligent character of the contravention, actions for mitigation, previous contraventions and the degree of cooperation with the Commissioner once contravention is found. Those are the kinds of factors which the Commissioner would take into account if he is seeking to impose the administrative penalty, and that penalty is only imposed in certain circumstances, in particular in respect of changes to the particulars to the Data Processor or the Data Controller as well as those provisions that speak to personal breach such as when you have to notify the Commissioner or the Data Subject in relation to personal breaches. Those are the kinds of contraventions which the Commissioner would be seeking to control.

Miss SHAWN BELLE: Madam Chairman, I also felt that it was necessary to speak to the commencement provision that is set out in Clause 9, which states that Act would come into operation on a date fixed by Proclamation. It is important to note that Section 16 of the Interpretation Act states that an Act can come into force in one of three ways on a date fixed by Proclamation, on a date fixed in the Act itself, on the date that the Act is published in the Official Gazette. Usually the Act would indicate whether the Act comes into operation on a date fixed by Proclamation or on any of the methods outlined. It should be noted that this particular Act comes into operation on a date fixed by Proclamation, so it means that when it goes through the procedures for Parliament and is assented to by the Governor General it does not mean that it will come into force. Clause 99 deals with the commencement. As I was saying, this Act makes provision for the Act to come into operation on a date fixed by Proclamation. That kind of commencement mechanism is allowed so that the Ministry would be given time to put any administrative measures in place before the Act is then proclaimed. It would therefore give them that time to also facilitate education of persons where necessary, so with that I conclude my remarks. Thank you.

MADAM CHAIRMAN: Thank you. Are there any questions? None at this time? Yes, go ahead, Senator Adams.

Senator R. J. H. ADAMS: I have one question. Thank you, Miss Belle. At one point you mentioned the adjustment that was made in the GDPR

between the powers that sit with the Controller and the Processor. Can you say why they made the adjustment or what was the point behind it?

Miss SHAWN BELLE: There is a recognition that in the processing actions that the Data Processor should also be regulated a bit more in terms of registration. In terms of giving an account of their activities, that was not really the focus of the previous European Union (EU) directive, and so in the GDPR they felt that because of the importance of the functions which the Data Processor was in fact implementing or performing, they should be regulated a bit more.

MADAM CHAIRMAN: Thank you. Any further questions. I am going to ask Mr. Steve Clarke of Deloitte to make his presentation at this stage.

Mr. STEVE CLARKE: Thank you very much, Madam Chair.

MADAM CHAIRMAN: He will be speaking on best practices.

Mr. STEVE CLARKE: Good afternoon, all. Thank you, Minister.

Asides.

Mr. STEVE CLARKE: There are three main areas I want to cover today: Essentially what role GDPR plays in the data privacy regulations and what we have seen as a firm globally and regionally, and also....

Asides.

Mr. STEVE CLARKE: That is the first thing: Looking at GDPR and how it applies to data privacy regulations and what we have seen; not just from a best practice perspective but essentially what we also see from challenges and implications of this type of legislation where you are basically on GDPR. Then lastly, in terms of conveying this message to the public, to people at large and to organisations to ensure that they fully understand the ramifications of the legislation. Those are the three main areas I am going to cover. I am starting with data privacy and the role that GDPR plays. There are many countries and organisations which use GDPR as a framework to develop their global compliance programme and for multi-jurisdictional compliance, but to truly understand why they do this you first need to understand a bit more of GDPR and what it is. Just for two minutes I want to spend explaining that aspect of it.

Specifically, GDPR replaces the local data protection laws and is valid in every country in the EU, and it is applicable globally as well. The intent of the legislation was to harmonise data protection and data privacy laws throughout the member states of the EU. Initially, this was to bring the EU states together because everyone was doing their own thing hodge-podge, and the idea was that the EU wanted to put something together. It was adopted on April 27, 2016 and it was enforceable from May 25, 2018. That was the day it went into effect. For a lot of you, some of you may have started seeing at that time certain emails and triggers coming through asking about data privacy, particularly if you had overseas connections. That was the date it started.

Madam Chairman, the other key thing is that it imposes strict penalties on organisations that fail to comply, and those strict penalties are essentially two per cent of gross revenue or €10 million or four per cent of gross revenue or €20 million. That is important to note. Those are significant figures. We kind of understand now that is just a basic framework of what GDPR is. The next part is why frame your data processing regulations on that?

Obviously, it is a very comprehensive regulatory guidance from the European Union (EU). It is the most comprehensive guidance there is out there and the most sophisticated and the most active so it is something that once you are based on this type of regulation you are at the top of the food chain and so this is one of the main reasons for having it. The most recent and active regimes whose data privacy regulations are based on this are Singapore, Nigeria, Mexico and Japan, with Japan being the most recent meaning they actually sought adequacy from the EU and they, as a country, had to go about the process of what we are doing, implementing legislation, *et cetera*, so they are the first and the only at this time who actually have adequacy from the EU. That is a good benchmark as well, to look at for us to see how things pan out.

Also, our GDPR continues to grow so it is essential the (*de facto*) international standard at this point. Even within the United States of America (USA) there is one State in particular, which is the State of California which has very, very, very similar legislation to what you will see with the GDPR. That part is more to explain what role it plays.

Now let us look at what some of the challenges that we have seen globally from our firm and essentially there are three main ones.

- 1) Applicability, and that goes a lot to extraterritoriality. That is a key challenge in terms of legislation and I will talk a bit about that;
- 2) Accountability particularly re the DPO or the Data Protection Commissioner in terms of exactly the focus on them and what they are to do, what their background should be, *et cetera*. That is another challenge; and
- 3) Lastly, for funding of the supervisory authority. Where is it funded?

On the first part: applicability. Applicability outside the jurisdiction is extremely complex and you have to carefully consider it and articulate it with clear and consistent guidance. On balance, it is necessary since localised application is impractical to enforce and prone to abusive litigation in courts but well-funded organisations. Most non-European Union jurisdictions have used extraterritoriality. That is key and essentially that is the case where to give an example. There was a breach of an organisation who are based in Barbados that happened in the EU but that particular organisation in the EU does not have any substance of assets of which it can go on against by the particular DPA in that

territory, how do they actually claw back and come back to punish or to penalise that individual. This is a challenge and this is what we have been seeing in terms of what we have been advising for a lot of the Governments and clients that they need to think of. Remember, it is the responsibility as well of every company to report to the relevant European Union DPA as well if there is a breach so if there is a breach and you look at it from a Governmental perspective but you take it down to the micro level, if there is a company and they have a breach, they have to report any breach as well to the specific European Union DPA.

The other aspect and the other challenge is accountability re the DPO. The accountability of Governments of a compliance programme within the organisations is complex on a GDPR for the presence of a Data Protection Commissioner/DPO. Organisations and the legislation should focus on a robust Government's programme with appropriate oversight. What does that mean? What that means is the focus within the legislation should not be targeted specifically to the DPO, what their background is to be, *et cetera*. The goal really is that it addresses that the regulations address the proper processes and oversight and this is what we are finding in practice. That is mainly the key. Ultimately, you may need someone to report but that could be done almost in an ad hoc basis. Again, as an example, some companies have outsourced this DPO. Obviously from a Governmental level, a Commissioner, the focus again should be just making sure you have almost like a Committee, something structured but that you have people that can actually focus on compliance and oversight and not concentrate on the particular position.

Lastly, the funding of the supervisory authority is also challenging and something you have to be careful on. There are two ways you can look at it. It could be self-funded through penalties or it could be funded, obviously, in-house via the Government. The Government funded is obviously the most flexible but, again, what we are seeing and what is being suggested is some sort of balance between the two.

The last area regarding the messaging essentially. Again, we are looking at what we have seen and what other territories have been doing so obviously the main thing is stuff like town halls and that type of sessions are very important but the key thing is the type of industry associates that you want to be attending such as like the Bar Association, DPSSA, these types of things, but more importantly, industry and commerce are the priority since they may need to implement the mechanisms for individuals to take advantage of their rights. This is one way you have and these are actually some of the things the EU had actually done to help convey these messages.

The other thing, obviously, is specifically to do with Press coverage so you need to include direct engagement with them and the main media outlets to get the word out and then the regulation itself should mandate that organisations conspicuously notify individuals of their rights upon collection or at the first

processing of the personal data. This is also pretty important because it is them as well that need to be able to notify and then they will be a vehicle as well for putting this thing out there.

That is just a highlight. I do not want to get too much into the details. There is more to give a frame for some of the considerations, what we are seeing as a firm globally and I open it up for questions.

MADAM CHAIRMAN: Any questions?

Senator R. J. H. ADAMS: I have a question. Have you seen a split in the capacity of firms to respect the legislation as a function of their size, whether they are small, medium or large?

Mr. STEVE CLARKE: Yes. A simple answer, but let me give an example. The larger organisations tend to use a bit more in-house. Let us, for instance, take the DPO position. They would tend to use in-house. The suggestion as well as – and I hate to go against this one – is not to use attorneys, for the same DPO for several reasons. The smaller entities it is a problem and they tend to outsource the DPO but I think where a lot of people are missing a lot is the regulation from a GDPR perspective. When you get breaches, *et cetera*, it has a lot more to do with intent than just a case where you happened to breach something with some person. I was giving an example to a client recently whereby you may say - well okay the hotel industry in Barbados - you have a lot of people who may come here from the European Union and there is a potential of data privacy being breached *et cetera*, but let us say you have a BnB, Bed and Breakfast, here, an entity, that you just take people from all over and you happened to get somebody from the European Union, it may not be that you are marketing this thing in the European Union so in practice they would not be at risk and that is not really what the GDPR is really intending to capture, however, you may have a hotel which has had a marketing arm in the United Kingdom, chartered flights, the intent is to market to the European Union and that is a different story, so it is not as straightforward and that is where it would affect not just the size of the organisation but where they are and what their intent is of what they are doing.

Senator R. J. H. ADAMS: I actually have a follow up question. I do not want to belabour this point but again in relation to small, medium and large, is there any sort of data around as to how onerous this is in financial terms, for example, as a percentage of total operating costs?

Mr. STEVE CLARKE: Sorry, I did not hear that?

Senator R. J. H. ADAMS: Is there any data around as to how financially onerous this legislation has proved specifically if there is any sort of a ready reckoner along the lines of percentage of total operating costs to implement?

Mr. STEVE CLARKE: Not yet. What I can tell you is the breaches that have occurred and the penalties that have occurred have been by extremely large organisations such as Facebook and Amazon. There have been a couple of others that have happened

that were reported to the French regulator that actually were a little bit smaller, so there has not been that many, what you are saying, penalties happening as yet? I think with time that would happen.

I think you also got to remember that even though the penalties are onerous and quite large you are talking about \$10 million Euro which can wipe out some countries far less organisations. The focus is not that that is what you will be charged. If you are assumed to be actually actively doing something to mitigate these breaches and trying to follow it, that impacts, that is a maximum penalty but that is not it, it is a range within that, so they look at that as well, so it is not just a case that is it and that is what people have to realise.

MADAM CHAIRMAN: Are there any other questions? We will just have the final presenter who is going to do an overview. We kind of did it the other way around.

Mr. CHESTERFIELD COPPIN: Good afternoon, all protocols observed. The question therefore may be asked why is data protection so important to the extent that we need to enact legislation to such an effect. As you might be aware, personal data has become the fuel driving much of the current online activity in this global information economy. Also, as more economic and social activities move online, the importance of data protection is increasingly recognised. Also, as the Government of Barbados seeks to promote and encourage the use of information and communications technologies at all levels, provide more of its services online by leveraging digital technologies, transforming into a digital economy and creating an environment which enables the ease of doing business, it must create the necessary legal and regulatory framework that ensures levels of confidence.

In this digital environment which is being created, much personal data will be processed at various levels, therefore, there must be the assurance of adequate levels of data protection. Also of importance is an appropriate dispute resolution mechanism so that if any malpractice occurs.

The Bill will therefore seek to make our data protection laws fit for this digital age, empower individuals to take care of their personal data and support businesses in their various operations. In essence, it will govern the collection, use and disclosure of individual's personal data by organisations in a manner that recognises both the right of the individuals to protect their personal data and the need for organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. When enacted, it will further strengthen our legal and regulatory framework in this digital environment. Already enacted are: The Electronic Transactions Act, Cap 308B, which seeks to give equivalence between documents in an electronic format and a paper-based format. This Act also makes provisions for the protection of data and privacy in Section 22; the Computer Misuse Act, Cap. 124B, which provides for the safeguards in respect of

information stored in computers and computer systems; and our Telecommunications Act, Cap. 282B, which was last amended in 2018, makes provisions for the management and regulations of telecommunications in Barbados.

The Government is also actively working to have laws enacted to deal with cybercrime and freedom of information. I must state, however, that the process of getting this Bill to this current stage started some time back in 2005, which is a bit lengthy. However, during this current process the Ministry of Small Business, Entrepreneurship and Commerce invited comments on the draft Bill and those comments were received by the Ministry and the Office of the Chief Parliamentary Counsel reviewed those comments and hence we have a draft issue which you can look at.

Another important factor to take into consideration about the Bill is the level of compliance with the European Union's General Data Protection Regulations which was just talked about. Those regulations came into effect on the 25th of May 2018 but according to those regulations a company with any office within the European Union or that processes data of any individual within the European Union must comply with the GDPR. Now, given the global nature of most businesses today it is most likely that companies that deals with trade online would be affected by the GDPR and this no doubt would affect our local businesses being we have our tourism markets where a lot of individuals from the European Union would come to Barbados on a yearly basis.

As was said by my colleague, the Bill is structured into ten parts and has a Schedule which deals specifically with the Data Protection Tribunal. The Tribunal will be established to hear appeals brought by the data user against decisions made by the Data Commissioner. You would have heard some of the provisions mentioned by my colleague Shawn Belle. The data protection principles set out how data should be processed and the rights of the data subject, for example the right to rectify any inaccurate personal data concerning him and the transfer of personal data outside of Barbados. Then there is the exemptions and penalties which were alluded to and the enforcement rights.

With respect to the administration of the Bill, the key party is the Data Protection Commissioner. There were some conversations as far as the Data Protection Commissioner is concerned. He is responsible for the general administration of this piece of legislation. He will also ensure that the good practices and protections and so on of which my colleague Steve spoke about are maintained. I would have mentioned, would have spoken about but because it came at this end, that is how it was structured, and to that, I thank you for your indulgence. Thank you.

ADJOURNMENT

MADAM CHAIRMAN: Many of you said "well, we do not quite understand", we need to have a

better overview. We want a little bit more detail, so are there any questions that are still lingering in your mind at this stage that you think you would want to put on the table or you can of course submit those questions later, as you think about what you have just heard. It was a lot of information in a short period of time. Any further questions? Alright with there being no further questions at this stage, I am going to invite a motion for us to adjourn with the intention of following procedure where we agreed that we would return on Wednesday at 10:00 a.m. to hear the submissions of those parties who requested to present before this Joint Committee. I would like to invite a motion.

The motion was seconded by Hon. D. D. MARSHALL.

MADAM CHAIRMAN: Thank you very much. I will see you all on Wednesday morning, there are some refreshments downstairs for you, so please join us and perhaps that would give us an opportunity too to speak informally as well about this.

ENDS TRANSCRIPT OF THE FIRST MEETING OF THE JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, HELD ON JUNE 24, 2019, IN THE SENATE CHAMBER.

**SECOND MEETING
OF THE
JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, 2018
HELD IN
THE HONOURABLE THE SENATE**

WEDNESDAY, JUNE 26, 2019

First SESSION 2018-2023

PRESENT:

Senator the Hon Miss K. S. McCONNEY
(Madam Chairman)
Hon. D. D. MARSHALL, Q.C., M.P.
Bishop the Hon. J. J. S. ATHERLEY, M.P. (Leader of
the Opposition)
Hon. Ms. C. S. V. HUSBANDS
Hon. D. G. SUTHERLAND, M.P.
Senator R. J. H. ADAMS
Senator Miss A. M. WIGGINS
Senator K. J. BOYCE
Senator Miss C. N. DRAKES
Senator D. R. SANDS

Also in Attendance:

Miss SHAWN BELLE *(Senior Parliamentary Counsel,
Office of the Chief Parliamentary Counsel)*
Mr. CHESTERFIELD COPPIN *(E-Commerce
Development Officer, Ministry of Small Business,
Entrepreneurship and Commerce)*
CLERK OF PARLIAMENT Mr. Pedro E. Eastmond
DEPUTY CLERK Mr. Nigel R. Jones
DEPUTY CLERK Miss Beverley S. Gibbons
Miss Suzanne Hamblin, (LIBRARY ASSISTANT)
PROCEDURAL OFFICER TO THE COMMITTEE
(Ag.)

ABSENT WERE

Mr. N. G. H. ROWE, M.P.

CALL TO ORDER/WELCOME

The Chairman called the meeting to order at 10:32 a.m. and welcomed those present.

MADAM CHAIRMAN: Recognising that there are five members of the Committee here which, according to procedures established in our first meeting, constitutes a quorum, we will get started with the quorum that is here currently. For all of those members who were unable to make it to the first meeting we want to welcome you to this meeting. Thank you very much for coming.

In moving to the second item on the Agenda which is the Minutes, I would like to invite a motion for the deferral of those Minutes given that we would have met only Monday and they are not yet quite prepared.

On the motion of Senator K. J. BOYCE, seconded by Senator Miss C. N. DRAKES, the Minutes of the last meeting were deferred.

MADAM CHAIRMAN: Thank you. The third item on the Agenda is Matters Arising from the Minutes. I would propose that there are no matters arising as we have deferred those Minutes.

The fourth item on the Agenda is Oral Submissions. For those members who were not present, we had established in procedures at our first meeting with regards to oral presentations that persons who had expressed an interest in presenting to us today orally. There were presentations that were written and some were oral. There were five requests for oral presentations for today. We had received notice that one of those persons will not be here and so we can expect four oral presentations so far based on the information we have to-date.

What we agreed on in the procedures on Monday at our first meeting is that each person would have the opportunity to present for about 10 minutes and then there will be 15 – 20 minutes of questions and answers that we can pose as a Committee and altogether no more than half an hour and we can show some flexibility given reason in that regard. We had also asked that Mr. Chesterfield Coppin, who would not have been named properly on the Committee would serve as a resource person, as he would have been the officer that was most intensely involved in the consultations with stakeholders in bringing this Bill to the next level and so I would ask the permission of the Committee to permit Mr. Chesterfield Coppin to sit as a technical resource as part of this Committee today. Are there any objections?

The Committee answered with a unanimous no.

MADAM CHAIRMAN: With that said, I think we have been able to move with dispatch to the submissions based on the speed with which we get through these submissions today, the thinking, again according to procedure we agreed, is that we would have heard the oral presentations in the morning, then we would break for lunch, and then after we would go through the written presentations with the intention by the end of the day of determining how those

submissions would or might impact the Bill and what adjustments, if any, would need to be made as required. Are there any other thoughts? Yes, Sir.

Bishop J. J. S. ATHERLEY: Madam Chairman, what time are we going to today?

MADAM CHAIRMAN: It depends on how fast we get through the presentations. Some presentations may take the full ten minutes, but the intention is to cover all today. Just let me use this opportunity to give notice too that following the request that was made for some groups to be reached out to directly that the Clerk of Parliament and the team did indeed reach out to those groups and we are now understanding that they maybe two additional submissions. So far, we have been notified that the Bar Association would also wish to make a submission as well as the Barbados Bankers' Association Inc.

According to the procedures which we established on Monday, we said that we would extend that deadline until Thursday, meaning tomorrow, for those submissions and then we will seek to hear those submissions if there is a request for oral presentations on Monday. If there is no request for oral presentations, we will then consider the written presentations on that day. Anything further?

Without further ado, I would recommend that we now go to the consideration of oral submissions. What we will do for ease, with your permission, of course, is to invite all of the presenters in and simply call them one at a time so that they can see the presentations of the others.

At 10:37 a.m., the presenters were ushered into the Senate Chamber to commence oral submissions.

Hon. D. G. SUTHERLAND joined the meeting at 10:38 a.m.

MADAM CHAIRMAN: I wish to acknowledge the presence of those persons and organisations that have requested to make an oral presentation before this Joint Select Committee. We will simply call you in the order in which your submissions were received and what we will ask is that, as you are called, you take your seat directly opposite, ensure that the green light is on so that we can hear your presentation. It will be a presentation from sitting. You have 10 minutes to make your presentation with about a 15 to 20 minutes for questions and comments from the Joint Select Committee. We want you to be aware that your presentation is being streamed live and you may begin when you are ready.

The very first person we would wish to call is Miss Cynthia Wiggins. When you come, kindly identify yourself and the organisation, if one, you are representing.

Miss Cynthia WIGGINS: Good morning. My name is Cynthia Wiggins. I am here as a user of data, an individual and a small business owner as well. May I begin?

I would first like to thank Madam Chairman and the members of the Joint Select Committee for

allowing the public to provide submissions on the Data Protection Bill, 2019.

Secondly, although I believe the Bill is an important one, I also believe that the amendments may be necessary to ensure that it facilitates:

1. The provision of a framework that allows companies to have the flexibility to target individuals, gain a competitive advantage through the utilisation of data and data analysis while ensuring the privacy of individuals.
2. Consideration of the new methods in which data can be captured, generated and analysed. For example, through retail transactions, online methods, block chain, *et cetera*.
3. Viewing the protection of data more so from the standpoint of the data use itself, than from the classification of the activities and the tasks in the data process.

For conciseness and clarity in the preceding paragraphs or discussion, my submission points will be addressed under six main headings with either page or section references where required. The main headings are as follows: Data and Data Element; Content; Privacy and Security; Monitoring and Compliance; Costs; and Others where I believe the points were important but did not fit under any of the above.

In relation to Data and Data Element, I believe the Bill in most instances does not seem to take into consideration the nuances of online and transactional data or the issues that would accompany such data types. For example, on Page 12, Accessible Records: I believe online transactions records do not technically fall within any of the record types listed. On Page 16, Sensitive Personal Data or Data in Page 13 does speak to photographs, videos, comments, *et cetera* that does not include personal purchasing information. Page 79 (r) does not include transactional or online data. Page 18, 4(1)(c) would limit social media or other business ability to utilise data as part of their competitive advantage.

On Page 25 (1), the point speaks to deceiving or misleading of individuals, however, businesses often collect data for purposes other than what they are proposed and change the reasons that they are collecting the data. For example, on Facebook you are connecting with your friends but, however, they actually analyse the data to advertise and gain revenue, *et cetera*. It is not necessarily for malicious reasons, it is just the nature of the business.

2. Under the same heading, online data by its very nature may be onerous to describe making the registration requirement on Page 60, 51 (2)(1)(c) difficult to comply with. For example, meta data, time stamps, information, location, landing pages, *et cetera* in general will be difficult to describe but may be captured for analysis reasons. Additionally, data captured requirements may change to assist with online visitors analysis as the need arise which would potentially hinder the innovation of a business if notification regarding the description is required.

3. In the normal course of business, data can be

collected and used for profit or as a tool to gain a competitive advantage, so consideration would have to be given to the following points: Page 25 (e), (i), (a), data can be collected for profit in relation to social media; Page 33, 18 (1)(4) could limit an organisation's use of data modelling, algorithm and profiling which may be how the company ensures its competitive advantage, for example, Social Media, Facebook, Instagram *et cetera*; Page 27 (10)(1) to provide the logic for profiling methods could impact on the company's competitive advantage. I do not see a reference to the sales and transaction or other data regarding the sale of actually companies. So whether or not when you sell a company it is the data that refers and relates to individuals may become part of the sale. Is that fine? Or do they need to actually inform the Commissioner?

The definition of direct marketing on Page 33 (3) does not seem to take into consideration telemarketing or online marketing since there are no restrictions specific to telemarketing or content marketing within the points on direct marketing. For example, where the company may initially call... I have had this where I would have gotten a call from one of the telecommunications companies under the pretence that they were informing me of a service problem and they started to upsell. That sometimes happened. I have had numerous calls at 7:30 in the night which I complained about and told them to place me on a do not call list, but there are loopholes within our legislation yes that allows for such things so it becomes difficult for an individual to actually say that this is a problem. Where individuals may be targeting within the content that does not seem as though it is an advertisement, so we often get things that are not classified as advertisements and it may just seem as though it is a normal conversation for BuzzFeed or YouTube funny videos but really and truly it is an advertisement. So how do we classify those things and what do we do about those things?

Although part of the general data protection regulations for small business, it seems as though the financial requirement would be a little bit onerous for small businesses to have data privacy officer (Pages 74, 75 and 76) and will hinder small businesses seeking to utilise data as a competitive advantage.

Just a note, I believe that we do not use data as much as we can or should as a competitive advantage. There are bigger businesses that are trying to seek to do that. Telecommunications companies tend to do that. Financial companies although they have the data do not use it as much, but they more than likely should.

Consent: Number 1- There is the need to specify in the Bill that consent needs to be explicitly given by opting in for utilising transfer or processing of the data therefore consideration would have to be given to certain points.

MADAM CHAIRMAN: Miss Wiggins, you do have two more minutes.

Miss. C. WIGGINS: Yes, that is fine. For utilising transfer or utilising of data, therefore

consideration would have to be given to certain points.

The Bill should seek to specify that individuals must notify on accidental disclosure, disruption or breaches which I do not think is currently there. Where an individual is no longer a user or a customer they should be able to ask for the removal of the data providing that it is not historical records or there is no legal ramifications.

Under Monitoring and Compliance, in the Bill, although there is no obligation to comply, there are loopholes which would allow individuals to circumvent the requirements. There is a need to specify time frame or frequency in which some of the activities should occur, Page 77 and 79.

I want to speak a little bit with the last minutes that I probably have with the cost issues which I think would come up for a lot of business owners. If there is a cost associated either legal administrative or otherwise with individuals requesting information or trying to ensure compliance via the tribunal or a quote, it may become a deterrent for individuals. For example, on Page 28 (3), I am not sure a data subject should be made to pay a fee in retrieving information that the data collector should have as part of their general service and their general operational costs. For example, you go to a bank and you want something printed from your account they are pressing print and that is about it and you are charged \$5.00.

I can see that being a loophole for persons to place cost to things that they do not need to place cost to.

Other issues, page 10. Financial Institutions may not fall under credit referencing agency according to the definition, but they also have information regarding credit standing. I will take for example, The Student Revolving Loan Fund that has on a number of occasions send information to your sureties only informing you that they will send information to your sureties, but they actually would have provided your sureties with your financial standing, technically. I see that as an issue. I am not sure of the minutes I have, if I have any more minutes, but I will stop here. I can always provide a written document as well.

MADAM CHAIRMAN: Thank you very much, Miss Wiggins. We really would have appreciated having at least the written document ahead, because it would have meant we could follow you more closely.

Senator Ms. A. M. WIGGINS: Yes.

MADAM CHAIRMAN: So thank you very much. I think that was very comprehensive as you touched on a number of the areas, which you thought you saw some loopholes there that you thought should be addressed, and that you saw some cost issues. You also need some clarification on definitions and a number of other important contributions that you made there.

Are there any questions from the committee at this point in time?

Senator Ms. A. M. WIGGINS: Or comments?

MADAM CHAIRMAN: Or comments?

BISHOP J. J. S. ATHERLEY: Madam Chairman, thank you, and thank you for your presentation, Miss Wiggins. I really would love to get a copy....

Miss C. WIGGINS: Yes that is fine. Time constraints. I would not want something that I have not proofed properly out there. It is just a time constraint issue. Yeah, that is fine. I will send it.

Senator Miss C. N. DRAKES: Madam Chairman, just one question for Miss Wiggins. Thank you very much for your presentation. You noted that you are a small business owner without giving the name of your business, but could you tell us the type of business you own?

Miss C. WIGGINS: I am in content marketing and social media advertisement. *et cetera*.

Senator Miss C. N. DRAKES: Thank you.

Miss C. WIGGINS: Yes, you are welcome.

MADAM CHAIRMAN: Thank you very much. We would simply ask that electronically, you submit your presentation to the Clerk of Parliament as you would have your initial.

Miss C. WIGGINS: Yes, sure.

MADAM CHAIRMAN: I would like now to call Mr. S Antonio Hollingsworth, to present to the Joint Select Committee. Identify yourself, and who you are representing, and then please continue as soon as you are ready.

Mr. S. ANTONIO HOLLINGSWORTH: Good morning Madam Chairman, Members of the Joint Select Committee. First of all, my name is S Antonio Hollingsworth. I represent myself personally, and I am the founder of Bajan Digital Creation Inc. We are a company that deals with conversational artificial intelligence and virtual reality content. I believe that you have received a copy of my written submission?

MADAM CHAIRMAN: Yes, we did.

Mr. S. ANTONIO HOLLINGSWORTH: Right. What I am about to say is to put everything that I would have written in context. This is a story of a Bajan who returned home to heal, his hands trembling, and his body ill. A shell of a man who left Barbados thirteen years ago. This Bajan returned at a time where jobs were scarce, and his thirteen years of educational experience in Mathematics meant little. He had to survive, so this industrious Bajan like every other proud Bajan used what he had to do and what had to be done. He used his skill set, will power, sweat and tears to build a business from a piece of drift wood to a digital entity with global reach in less than a year, bootstrapped. No loan because he had nothing, no political affiliation, he is the average Bajan from a working class family who lives by modest means in a Christ Church village. He was willing to work hard and build in a time when building was difficult and resources extremely scarce.

That story is familiar to most small to medium enterprises that would be affected by this current version of the Bill, they need to survive. The artist selling her art online, she needed to survive. The taxi driver hustling to collect one of his clients who called,

he needed to survive. The homeowner who runs an Airbnb to make extra, she needed to survive. The 60 plus year old seamstress who collects measurements on persons, she needed to survive. The start-ups that are still in gestation, they need to survive. These may not have the resources for another specialist employee called a Data Privacy Officer. They may not have the time or resources to go through a certification or registration process. It is already difficult enough to start or do business in Barbados, and this Bill in its current form makes it harder for small to medium enterprises to be profitable when money is scarce. Worse yet, under this Bill to take a chance with noncompliance is not only the end of whatever small business you may have, but the tarnishing of your reputation by incarceration of three years. I do not think that the Government has educated its constituents thoroughly enough to enforce such draconian measures that cannot be the reward for entrepreneurs at this time when the Country needs more entrepreneurs. Under this Bill the Government has introduced penalties that create a hostile environment for the average Bajan to enjoy his property, his business and his network that he has cultivated. In my most humble opinion this treads uncomfortably close to the spirit of the Constitution, which may stymie the growth of Small Business Enterprises due to fear of the increased liability. In my opinion, and others', the Government should delay the implementation of penalties until the public is fully aware or sensitised to the importance of Data Protection, and the inherent responsibilities of a Data Controller. For your consideration:

1. a suggested period of three years to prepare before penalties are incurred. That penalties be scaled to be commensurate with the revenue of the Data Controller or the Data Processor.

Also, we request that:

2. the registration and certification of the Data Controller be waived to reduce bureaucracy and also facilitate the proper execution of the duties of the Commissioner. A middle ground where the privacy may be maintained in terms of security.

According to Article 6 of the Electronic Transaction Act, and that only in the case where the Data Controller or Data Processors, Data Privacy Policy is unreasonably inefficient that a data privacy officer is required for oversight. Data Privacy is of utmost importance and I commend the Government for such swift move to protect the interest of their constituents. However, to make it onerous on the average Bajan to start and operate a small to medium enterprise is not in keeping with the resounding mandate that the constituents of this great nation, in full confidence, entrusted to the custodians of this Government. I thank you.

MADAM CHAIRMAN: Thank you very

much, Sir. Are there any questions at this stage? Sir, we reserve the right to ask you questions both on your oral presentation, as well as the written submission that you would have made.

Senator K. J. BOYCE: Through you, Madam Chair. Sir, I think your presentation was quite profound, I understand the perspective of where you are coming from in relation to the small business owner, and also as well the skill set which you bring to the table, [you] being a practitioner within the field. At the end of the day, however, the Government is obliged to balance its obligations with regard to generating business, while seeking to bring itself in a more compliant state, recognising that information and data being the new currency, that there are several external and even internal pressures to make sure that relevant legislation is in place. Recognising the need for that balance, and I have noted your suggestions with regard to delay of the implementation of the enforcement provision, as well as the other suggestions, but assuming you had a magic wand – and I am purely hypothetical – but how would you, in an ideal world, what would be the mechanism that you would suggest that would allow the Government to balance its obligations to ensure [that] the legislative framework is in place to provide the protection of the data, as well as to still encourage and facilitate small businesses which for better or worse have to find themselves in a position whereby they are able to comply with these new requirements, but may not have the resources to do so?

Mr. S. ANTONIO HOLLINGSWORTH: The suggestion on how small to medium enterprises might be able to meet the requirement, basically.

Senator K. J. BOYCE: [To] meet the requirement, and this is an ideal world scenario so you are not limited by any form of practicality, it is just that how they can meet the requirements, [while] recognising that the Government does have an obligation to the same citizens, with regards to the protection mechanisms that are being proposed in the legislation.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you. I will deal within the realm of practicality because within the realm of practicality what is defined as data, according to this Bill, goes beyond electronic, it implies written information that is filed in a filing cabinet; it implies information that may be stored in an app on a cell phone; it implies information that may be stored within a cell phone, and I am going to present a real world situation whereby I had a conversation recently with an individual who is running a small Airbnb and I had to sit down and go through with her the importance of compliance, that she should encrypt her phone, that she should lock the app. These are things that I may know because of my skill set but the average Bajan may not know. I would not be willing to bet, because this is not the place for that, but most Bajans or individuals who may have the latest smartphones may not know or may not be aware that [that] phone has passive listening, waiting for someone to say a key phrase, and they may not have trained it to

recognise their own voice, so that if you are going to bring a Bill into play that essentially could make every citizen a data controller, then the necessary sensitisation should occur before there is any debate. The fact that there are so few of us here to represent orally is an indication of how many people [who] do not understand these 104 pages and the implications of that Bill. So in terms of the practical application, the Government should not place into legislation any Bill that becomes an absurdity because you cannot enforce it. So I would go with a systematic education of the public on how important data is, the value of their data, how they can protect their data. I am just going to ask the question, if I may. How many Members in the room uses two-factor authentication?

(silence)

That is an indication, there are lots of Barbadians who do not know what two-factor authentication is. They may just be people [who are] trying to make a living, they would have lost their job, they might have just been laid off, [they might just be] trying to find a way to make a living and along comes this Bill that requires them to register. My concern is that it bears much similarity with [the] Jamaican Act which requires registration and an annual registration, which is not clarified in this Bill. So [that] for me, the average Barbadian seeing that I must register as a data controller and [that] in that registration there are fees that the Commissioner may impose, and those fees may be annual, [for me] essentially that is a tax.

Senator K. J. BOYCE: Just one follow-up question, Madam Chairman. If you were able then to suggest a delineation between the average person with a smartphone running an Airbnb's, the example that you gave, and the interpretation as to whether that would fall under this regime will be determined, what level do you think the test, what level do you think this legislation should apply for? In other words, do you believe there should be some prescription as to the amount of revenue, [be there] some type of prescription as to specific industries? You will note that there are specific areas which are excluded.

Mr. S. ANTONIO HOLLINGSWORTH: Yes, I know there are specific areas.

Senator K. J. BOYCE: So then, of course, that then raises an implication as to what is included. Would you be able to suggest, then, if we do not want to catch everyone in this net, what areas perhaps the Government should be trying to focus on, to be clear that this legislation should explicitly affect?

Mr. S. ANTONIO HOLLINGSWORTH: Thank you for the question. Maybe we might want to start at the general data protection legislation. It starts off speaking and addressing data controllers on a large scale, it is repeated on a large scale. Of course, that is relative to what is large, the European Union is much larger than Barbados so [that what is] large for the European Union might not be large for Barbados, so what I would recommend is that you look at maybe

the.... Well, that you look at the annual revenue and also you look at the impact that a data breach may have, because if I have ten telephone numbers or ten clients, a data breach of that magnitude could be significant to them in terms of a civil situation, but not necessarily to the extent that they incur half-million dollars and three years in prison. However, a large telecom company that maybe running data for all of Barbados, a breach in that magnitude is a significant breach or if the State has a breach [and] that [would] be a significant breach. Would that be required to be made public? One of the things that I would like to recommend that you also consider, is that while you have a Data Privacy Protection Act that you also have within the legislation or in another Bill, a Freedom of Information Act, if one does not exist. Because if I am surrendering my data to the Government of Barbados, let us say TAMIS, the TAMIS privacy policy is woefully inadequate, and I would like to know that if there is any breach that has occurred that the public authority is held to notify the public that a breach has occurred.

Senator K. J. BOYCE: No further questions. Thank You, Sir. No further questions from me Madam Chairman.

MADAM CHAIRMAN: Any other questions from the Committee? Senator Adams.

Senator R. J. H. ADAMS: Thank you Madam Chairman. This is more a comment. When we had our closed session we talked about the penalties, three years imprisonment or \$500 000.00, and it was my understanding, and I am open to correction here that that is really a question, legal presentation but any Judge would have a discretion to do some of the things you are talking about. Recognise the scale of the breach, the context of the breach and so on, but I wonder if, I think Madam Chairman or Ms. Belle could just lend some comment to that because I would hate to give you misinformation, but I think a discretion is built into that and I know that from your presentation and the way you have written an oral, the way you talked to it that it is of concern. But I believe that is recognised implicitly.

MADAM CHAIRMAN: I am going to ask Ms. Shawn Belle, who is the Senior Parliamentary Counsel who would have worked on the drafting of this Bill to respond to that comment.

Miss SHAWN BELLE: Thank you. Madam Chairman through you, just to speak to how penalty regimes usually work in Barbados by reference to the Interpretation Act Chapter 1. When you speak to penalties, there are expressed at their maximum. When you see \$500 000.00 and then three years in prison, that is the maximum that the Judge can impose for the particular offence that is identified. However, the Judge would have a discretion to impose their role or no penalty to the maximum threshold that is set out in the legislation. Within that discretion then the Judge would then look at the circumstances of the case and then consider the seriousness of the infraction, any mitigating factors before he would impose that penalty. What needs to be recognised is that it would not be a

fixed penalty as I see certain persons interpreting it, but more, that it is an expression of a maximum of that penalty.

Mr. S. ANTONIO HOLLINGSWORTH: May I respond?

MADAM CHAIRMAN: Sure.

Mr. S. ANTONIO HOLLINGSWORTH: I understand what you are saying. Again looking at it from a small business approach, the discretion of a Judge could be one dollar, it could be ten dollars, it could be \$100.00, legal fees to a small business can be the entire revenue of that small business for a month.

Miss SHAWN BELLE: Madam Chairman through you. Just to say that when you are going through civil proceedings, the cost, if it is that you are then the party that is I suppose it falls in favour of that you will be compensated by the other persons. Those are facilities that are provided for by the Supreme Court Rules, those are things that are provided for. I do appreciate that there would cost in starting civil proceedings or things like that but there are provisions for that. Additionally, I also need to point that according to the GDPR, you must take these breaches seriously, and so the State is under a mandate to make sure that they impose penalties that are sufficiently of notice to the public that it is serious. With that in mind, that is why the penalties appear in that form, so I just wanted to speak to that.

Mr. S. ANTONIO HOLLINGSWORTH: May I respond?

MADAM CHAIRMAN: Yes.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you for your submission. Based on what you have just said, I appreciate the benefit that would come for a small to medium enterprise that maybe taken to Court if they have sufficiently justified what has gone on. But, in so doing you have also opened up the door where a large entity who might have been in breach, maybe able to have all of the legal machinations to work against a private citizen, whereby the private citizen loses the case.

Miss SHAWN BELLE: Madam Chair, through you. Just to say there were some submissions in relation to liability insurance and so on, so the question is, whether there is actually a development in the insurance industry for covering the potential liability that you may incur. Now that part is something that would need to be developed maybe outside the sphere of this legislation, because for instance with Attorneys, if they are service providers, they are required to get insurance set up to cover such things where they may find themselves liable for certain actions or infractions of legislation, and that requirement works throughout certain industries or professions. I am just making that observation.

MADAM CHAIRMAN: I believe your time is up now. Thank you very much for your presentation and your contribution. Thank you especially for your comment about public education as we move forward, that certainly is a significant part of the work that has to be done in preparing the country for the implementation

of this particular Bill once it becomes an Act.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you Madam Chair. Thank you for the opportunity.

MADAM CHAIRMAN: The third presenter, I would like to invite, is Mr. Bartlett Morgan, who is representing Lex Caribbean. Please take this opportunity Sir to make any correction with regards to either your name or the organisation you represent for the record.

Mr. BARTLETT MORGAN: Thank you, Minister. Good morning Senators, Members of Parliament, to the Clerks present. First of all, I thank you very much for this opportunity. I think it is a positive signal as to the state of our democracy; it can only allow persons, members, citizens all to have some sort of input into important legislative developments like this. I do not know if clarification is the word, but I am here ostensibly in a personal capacity and with perhaps good reason that I can get into later, but to the extent that I have ten minutes to make my submissions, I would much prefer to sort of dive right in and then we can perhaps deal with those other matters later.

Mr. BARTLETT MORGAN: Now I must say just in the way of framing that I think it is clearly high time that we got about the business of passing legislation like this. I do not say that in the whimsical sense that we always thought it was a good idea and now have got around to it, but I say it in perhaps the more legalistic sense which is that we have passed due obligations to get this ball rolling. I say that among other things with reference to our obligations under the Economic Partnership Agreement (EPA), which we would have signed onto in 2008. I refer to that one specifically because, among the hundreds of Articles which we agreed to, when you read almost to the bottom of it one of the primary things was that we would pass comprehensive data protection legislation within seven years. We signed onto that in 2008, and so literally we are past due on a very serious international obligation, as it were, under the EPA to pass this legislation.

Madam Chairman, the other reason why I mentioned that is because it flows into my first set of submissions. To the extent that I have ten minutes, I suspect that I may not get past the first set and so I will get to the point of it really quickly. To my mind, there are four "big fish issues" which this Committee needs to be mindful of. I had a look at the Order Paper this morning, and I noted that it says that the purpose is really to consider the legislation and the degree to which, when passed, it will allow for the protection of personal data while allowing for transparency and accountability. I am mindful of that in my comments, and so to my mind the major big fish that we need to tackle is the whole question of the independence of the regulator, which is the Data Protection Commissioner. That is the first thing that jumps out at me on reading this latest iteration of the Bill. The other thing is the question of compensation for Data Subjects. Thirdly, is the framework for the Data Protection Commissioner to

actually audit Data Controllers and Processors. That framework may need some re-jigging.

In the main, what I want to start off with is a point which was addressed earlier. I was thinking of not mentioning it but it is the whole question of the implementation periods and the timelines for implementation. I think those are perhaps the four biggest ones. To start off with the whole question of independence, a part of the reason why I would have mentioned the EPA was that in Article 197, I believe, it obligates us to not just implement a regulator for a data protection regime but that the regulator has to be independent. It cannot simply be a sort of spawn of the Government and taking directions from the Government in the usual course of things. It has to operate in a truly independent sense. On review of this draft, I note that even though there are many functions listed under what the Data Protection Commissioner ought to do, there is nothing that speaks in detail to any sort of staffing or human resource-type independence in terms of the Commissioner's ability to impact who is selected, how many persons are selected and so on. There is no sort of budgetary independence that is outlined there. So effectively you have a regulator who will be in a real sense beholden to the Minister to whom he will report. To the extent that this Bill purports to have a regime that also encompasses the Government and Government agencies and so on, I am hard-pressed to see in a situation where, with all of those factors and also no security of tenure, a Data Protection Commissioner would readily and gladly step into a Government agency to audit them and to turn up negative findings.

Therefore, to my mind, if we are to consider this in the context of accountability, transparency and a regime that is effective in the main, unless that is tackled and those issues are tackled then I think it is quite likely that we may end up with a regime that looks really good on paper and looks good to our international partners, but in terms of actually protecting the data-related rights of Barbadians and persons in Barbados, we may not be setting up ourselves to actually achieve that in a real sense. I can perhaps go into more detail but given the time constraints, I will move on to the whole question of compensation.

Madam Chair, if we see this purely in the context of incentives – this is human nature – and if this Act is set up to protect the rights of persons in Barbados who are Data Subjects but there is no mechanism in the Act for Data Subjects to be compensated when their rights are breached, I am hard-pressed to imagine that very many persons would actually go about the hassle of seeking to enforce or to vindicate their rights pursuant to this Bill as drafted. I said that by the way to note that if you look at the legislation that is considered the gold standard nowadays, the GDPR (General Data Protection Regulations), they have that right and it is expressly and clearly stated. If we look at even the prior draft of this very Bill, it had that right to compensation, and so I would suggest that unless that is in place, again we are lessening the likelihood that this Bill when passed into law, will actually meet the test which we set

out for it.

The other question which I think requires some attention is the whole sort of auditing framework that is present in the Bill. As it stands right now and as I read the Bill, it is a process whereby in effect, yes, you can give an assessment notice but you cannot actually go in to assess the Data Controller or Data Processor until you have gotten a warrant from the Courts. That is going to be a very time-consuming and expensive process for the Data Protection Commissioner himself, and with whatever budget the Commissioner may have and however limited it may be, that is more expense and time incurred to simply get a warrant to go and investigate essentially. It would seem to me that, again in line with prevailing best practices globally, we ought to have within the Bill some provision whereby there can be at the very least what I would refer to as a consensual audit process. The Data Protection Commissioner, for whatever reason, may say, "I would like to investigate you", or even of your own volition as a Data Controller you may think your systems are up to muster and so you would want to ensure that they pass the test outlined in the Bill. You can therefore invite the Data Protection Commissioner in to have a look. There needs to be some mechanism to allow for that process because otherwise it becomes an unnecessarily expensive process for even the Data Protection Commissioner himself to partake in.

Madam Chair, as time goes I literally have two minutes left and therefore I will move right on to the whole question of the grace period for implementation. To me, this is a practical issue more than anything else. If we were to quickly pass the Bill into law as an Act in its entirety then most Barbadian entities would be in default or in breach. That is the simple reality of it, and so having a timeframe within which persons can get their houses in order, I think, is just a practical thing that we ought to be mindful of and to legislate for. Also, there is the other added benefit which is that it allows the Data Protection Commissioner to begin his work of awareness because that is one of his obligations. It would, therefore, seem to me that perhaps the best approach may be to pass those sections of the Bill into law that enliven or give power to the Data Protection Commissioner to, first of all, exist so that he can get about the business of sensitisation and awareness and also putting practical mechanisms in place for his own office to operate first before we actually get about the business of enforcing the Act.

In my last minute, I just want to quickly run past that to outline some other matters which I think....

MADAM CHAIRMAN: You are very creative with your time, Sir, but that is okay.

Mr. BARTLETT MORGAN: If my time is up then, that is fine, Ma'am.

MADAM CHAIRMAN: Go ahead. It is your minute.

Mr. BARTLETT MORGAN: Just very quickly, there are a number of other things and first of all I should perhaps apologise because, as I understood, the invitation was sort of to present orally, or otherwise

if you are not minded then to do written submissions. I would be happy to put together written submissions to articulate my position because there are a number of other things that are more like bread-and-butter matters but they need addressing. First things first, the provisions that deal with... Subsection 2, for example, the definition of data controller and data processor. To my mind, simply by using the word "person" it remains unnecessarily vague especially to the extent that this Bill purports to capture data controller and processors who are also governmental agencies and so on, simply using "person" as the definition of a data controller or a processor, to my mind, it may arguably miss the mark. My suggestion is that we actually spell it out. Do not leave it up to chance. Say a data controller is "a person or a corporate entity or a Governmental entity, *et cetera*." If you go beyond that quickly, Section 4.(1) which is sort of like the foundation of the entire Bill because that outlines that actually fundamental principles that a data controller and a processor would have to abide by. It requires the use of the word "and" in there somewhere because you have to abide by all of these obligations and so at some point, perhaps before, at the end of the second to last, the penultimate provision, there needs to be an "and" in there so that it is clear that you have to comply with of them as opposed to cherry-picking one and going well, I am transparent but you know, the whole data minimisation thing, I did not do that.

If you keep it going along those lines, another major one which needs to be addressed is Section 5, Subsection 3 and 4. That has to do with the whole question of fairness. The idea is, if you are being fair in how you collect data then one of your obligations is that at a very minimum tell the person you are collecting the data from here is what I am doing with it, here is who I am going to share it with, here is how I plan to store it, here is how I plan to process it, that kind of a thing. Those matters are outlined in Subsection 3 and 4 of Section 5 but the problem is, when you read through the Bill you realise that essential the same provisions, but in far greater detail are outlined at Sections, I believe, 18 and 19. In other words, we are basically repeating ourselves and to no good purpose. Especially in a context where this Bill will be used not just by lawyers but lots of everyday business persons. You would have seen that lots of the persons who have presented already are business people, small businesses and so on. They are going to be reading this Bill themselves and so, I think, it is upon us to be as clear as possible about what it is we are doing and what the obligations are and so on.

MADAM CHAIRMAN: Thank you for your submission.

Mr. BARTLETT MORGAN: Thank you very much for having me, Madam Chair.

MADAM CHAIRMAN: I am going to ask Ms. Belle to speak to a couple things because I think it is important that we have clarification as we go into our questions and answers session. There was the question of the definition of the data controller and the data

processor and whether there is a legal person as well as human person, *et cetera*. Number 1, can you speak to that? And then I will ask the second one after.

Miss SHAWN BELLE: Madam Chair, through you, when the use of the word "person" is used in legislation, well, at least, our legislation; it contemplates the inclusion of the individual as well as legal persons so that there would be no need then to specify companies, or other entities that have corporate or legal personality so from that point of view you can take what you can.

Hon. Ms. C. S. V. HUSBANDS joined the meeting at 11:34 a.m.

MADAM CHAIRMAN: There was also the reference to a consensual audit process preceding the need to go for warrants, *et cetera*, I wonder whether or not you wish to comment on that at this stage or you may defer it and we can come back later.

Miss SHAWN BELLE: Madam Chair, if we can defer so I can look more closely or maybe I need clarification in relation to what you mean by that.

Mr. BARTLETT MORGAN: Do you need that clarification now?

Miss SHAWN BELLE: Madam Chairman, through you, if it is that in your written presentation if you are planning to submit then you can write it out so I can see what you mean by it. That would be appreciated.

Mr. BARTLETT MORGAN: Very well.

MADAM CHAIRMAN: I will open the Floor to the rest of the Committee to ask any questions at this stage.

Hon. Ms. C. S. V. HUSBANDS: Sorry. Before you do, my apologies and good morning to everyone. I really enjoyed what I heard and what you had to say so I am looking forward to this engagement.

Mr. BARTLETT MORGAN: Thank you.

MADAM CHAIRMAN: Thank you Honourable Sandra Husbands. Senator Drakes?

Senator Miss C. N. DRAKES: Yes, Madam Chairman, thank you. First of all, Mr. Morgan, thank you very much for your presentation. I thought it was quite insightful. You made some interesting points as it relates to where the legislation lacks clarity on some issues and one of those things that I want to ask you and possibly put it out to the Committee is, we keep hearing this issue of one discrepancy between possibly the size of the company, the revenue it makes and the potential for the penalties that it could incur if you find yourself in that situation. Now on the other side of the coin, we are hearing there is no provision for the compensation for data subjects if you find yourself in a breach and there needs to be some compensation as it relates to your data being used without your consent or however that may come about. I am wondering if at any point, as we revise the legislation, and this is just to table it, if we can seriously look into having a part of this legislation that is reflective of those two elements - where there is some representation as it relates to the

size of companies, if you find yourself in a situation, and as it relates to data subjects and their compensations and the two of those areas being aligned so that there is some fairness in the proceedings in the legislation. I just wanted to table that comment for the Committee.

Mr. BARTLETT MORGAN: If I may just make a comment on that. Apart of why I chose to come here in a personal capacity is, I wear a number of different hats which, on the fact of it, to an onlooker, may seem to conflict so I did not want to take on this process, sort of carrying a grief, as they say. I attempted to look at the legislation just for what it is and what it is we are purporting to bring about in Barbados. The reality of it is, regardless of how you frame it, either business and perhaps larger businesses are going to be displeased, or smaller businesses are going to be displeased and then in the third sector, the data subjects are going to be displeased so you are not going to have any sort of ideal balance act, especially as regards the whole idea of which obligations you ought to comply with and so on. To my mind, the way usually the best place to start is at the beginning. What are we trying to do?

We are trying to secure the data related rights of everyday Barbadians. If that is the objective, then it stands to reason that a small business, by our standard definitions, who is passing lots of personal data should not get an exemption because there is no rule in the black hat hacker world that says we do not target small businesses with lots of valuable information and so, if the risk that we are guarding against is the personal data of Barbadians being misused, abused, and so on, then to my mind, necessarily tackling it head on from the perspective of well, big companies get big fines and smaller entities get small fines may not be the best way. Certainly not in the legislation itself. What I would suggest is that, on the face of it, as Ms. Belle would have pointed out, there is a built-in discretion with a lot of these penalties and so I have to believe that a fair-minded judicial officer of a court and even the Data Commissioner, when he is giving his administrative penalties, he would have to be mindful of the circumstances of the breach. If you are a large company, you have already breached the Act two times and you are still doing the wrong thing and it just so happens that you are hacked again - maybe a major insurance company, for example, just making something up - and thousands of Barbadian data is exposed, you probably deserve a larger penalty, closer to the half of million dollars, but if you are a small entity... This actually brings me to the other thing which, I think, is significant. The Bill does not seem to allow for reprimands. It cannot be that our only approach to getting people to do the right thing is to slap them with a big fine. If you committed a fairly mild breach I am sure a reprimand ought to be enough but perhaps let me... but I am not seeing this draft where the Data Commissioner has the power to reprimand someone because that may be appropriate in the cases of smaller perceived breaches.

MADAM CHAIRMAN: I believe that the time is up. I am going to extend it because I see that...

Bishop J. J. S. ATHERLEY: Thank you, Madam Chair, and thank you for your presentation. It is very insightful. Much of the legislation considered by the Parliament of Barbados in both Houses recently has been in a hurried context where the intention of coming into conformity compliance with international obligations. You made a reference to this and a relative EPA, define for me or describe for me the level of urgency which in your opinion now attaches to this, since you said it is a past due obligation. What is the level of urgency attaching to it or is there a level of urgency?

Mr. BARTLETT MORGAN: Four years, and by that I mean the particular article of the EPA mandated that we put legislation in place seven years after signing on to the EPA. We signed on it in 2008 so it means therefore that seven years hence would have brought us to 2015 and so it means we are four years out on the face of it and so there is that, but to my mind that ought not to be the only, at the basis of our urgency, in getting the document. I remember two years ago, I do not if you come to remember, an economist published a report two years ago that said that data is now the most valuable resource, it is no longer oil and so that in and of itself I think is sufficient reason for us to get about the business of getting this passed quickly in a fair manner.

MADAM CHAIRMAN: Thank you very much. I would like to mention at this time as well it is not simply catching up with our obligations, Barbados has certainly set itself on a path towards digital transformation, and even as we seek to implement the kiosks at the Airport we are recognising that there is some urgency in us ensuring that this legislation gets in place because it facilitates the exchange of information with some of our partners in the European Union and other places and so it is not just what we are playing catch up with - it is also what we need to accelerate towards in order to facilitate the transformation that we are seeking to bring on a digital level.

Mr. BARTLETT MORGAN: I am most grateful to the Committee, Ma'am.

MADAM CHAIRMAN: I see there is one more comment from Miss Belle, and I will commit because I think we have to be flexible at this time when people have meaningful contributions to make.

Miss SHAWN BELLE: Just to speak to the lack of reprimand mechanism, the enforcement notice gives the opportunity for the Commissioner to state his reasons for asking the Data Processor or the Data Comptroller to do something or to refrain from doing something, but is the mechanism of reprimand you are thinking of is a reprimand in and of itself in the league of perhaps, where you would be looking at like the recent juvenile justice legislation type set ups where the judge would be saying and you should do so and so because so and so is wrong, *et cetera*, for rehabilitation or some other type contemplative contemplation?

Mr. BARTLETT MORGAN: As I

conceptualised it, it is really that sort of light touch. In other words, to clarify the whole thing of what the enforcement notice encompasses and so on, the enforcement notices towards an end which is specified which is an administrative fine... for the course... so to my mind the reprimand is as I would call it a light touch where you are simply saying this is the end result, this is what you get for that breach, a slap on the wrist essentially, but simply saying you have done this thing wrong, refrain from doing this thing full stop but without any further recourse so to speak so it would be an ending of itself.

MADAM CHAIRMAN: Thank you very much. Sir, I would wish to request that you make that written submission as soon as possible, in fact the deadline is tomorrow. I believe that was communicated in the Press as well.

I would like to inform you as well as the other presenters that there may be some things that we were not responding to immediately. It is important for you to know that there being no written submissions ahead we will take the opportunity for those critical and substantive matters to be dealt with in matters arising at the next sitting of this Committee. Thank you.

Mr. BARTLETT MORGAN: Thank you, the Committee for having me.

MADAM CHAIRMAN: Colleagues, I have just been informed that the final presenter for today has informed that she will no longer be presenting and that said I am going to ask your permission to alter procedure as we would have established where we said we will do our oral presentations in the morning then we would break for lunch and come back to consider the written. I will ask your indulgence to take a suspension for approximately 15 minutes and then come back and do at least the first of the written submissions before we break for lunch. With your indulgence can we make that alteration in the procedures for today? I would like to invite a motion so that we can formalise this.

Senator K. J. BOYCE: I move that the Agenda be amended as proposed and that we break as suggested.

SUSPENSION

MADAM CHAIRMAN: Thank you, we will return at 12:05 p.m. to consider the first of the written submissions.

R
E
S
U
M
P
T
I
O
N

MADAM CHAIRMAN: First, Antonio Hollingsworth, next, Sherrine Flan, next, Shannon Clarke, and then Solutions Barbados. So we just do them in that order. Pardon me? Yes, Mr. Coppin, you seem to have a comment. Okay, could one of the... okay, the Clerk will assist you. That is because you would have been added after so, our apologies to you. The clerk will take care of it. The intention is that we will look at, I am assuming everyone has read at this stage. This by the way is a close section in that it is not being streamed. This is just, and the recordings is simply for Hansard purposes. The intention is to go through the critical recommendations in each one, and then have a discussion around them, and then determine how, if at all we would wish for it to impact the Bill. Is that a fair way to proceed committee?

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: The first one is from Soledad González, which is Quidguest, I believe is the name of that company. May I suggest to the Committee that this, from my reading of it, appears to be a sales pitch? That said, it does not gel with the terms of reference of this Committee, and so I would ask that we at this time defer this or disregard it completely? I would like a motion please. I would like to invite a motion that we either not consider this in the context of the Terms of Reference. Is there a Seconder?

Seconded by Senator Miss C. N. DRAKES.

MADAM CHAIRMAN: Thank you. The second submission is from S. Antonio Hollingsworth. This individual would have presented in the name of Bajan Digital Creations Inc., earlier this morning, an oral presentation. This individual would also have made a written presentation. You would have noticed that while his oral presentation would have differed in some ways from his written presentation there are, yes in a significant way. I would still recommend that the Committee consider the written as well. Here are some of the key considerations, and recommendations in this. Has everyone read? And can I just simply jump to the recommendations? You are comfortable with that? I am just flipping because the recommendations are all over the document.

If you look on page 4 number 2, as such I would like to make the following suggestions for your consideration. If we go first to number 2, to reduce the requirements of the Data Controller to fall within the established Article 4 of the Electronic Transaction Act until such time is the public aware, and fully understands the value of personal data? Pardon me?

Asides.

MADAM CHAIRMAN: Yes, it is Article 6, my apologies. Article 6 for the record. Miss Belle, can you speak to that?

Miss SHAWN BELLE: Madam Chairman,

just trying to find the place where we are.

MADAM CHAIRMAN: Page 4, the submission by Hollingsworth, number 2 at the bottom. With us?

Miss SHAWN BELLE: Yes. Madam Chairman, just to make the Committee aware that the framework that is set up under the Electronic Transactions Act, is confined to that sphere. So, Data Protection Controller for instance, has a different definition there. There are, and the regulation of Data Protection has specific relation to electronic transaction specifically. So that is one of the things that has to be understood. Now, it may be that at a later date you may want to incorporate those provisions into the Data Protection Bill. but for the time being because it is so specific then that, well rather part needs to be treated as operating in that specific sphere. Meaning the Electronic Transactions Legislation.

MADAM CHAIRMAN: Do any Committee Members need any clarification? Is there something specific you need understood?

Hon. C. S. V. HUSBANDS: The distinction that you are making in terms of what is required of the Data Controller versus how Mr. Hollingsworth had outlined what he saw as the things. I did not quite get that.

Miss SHAWN BELLE: For instance, the definition of a Data Controller in the context of the Electronic Transaction Act, does not have the same definition as in the Data Protection Legislation. Reason being is that those provisions are to be confined to regulating Data Protection in the context of electronic transactions. The data protection Legislation has a wider net, but that piece of legislation is very specific to electronic transactions. Particularly, if you look at the definition of say, the Data Protection Controller, it talks about looking at the certification of electronic signatures, which is not something that is addressed in the Data Protection Bill. So that is why it exist in parallel, but it is not the same, and it is that part dealing with Data Protection only deals with electronic transactions, I have to make that clear.

Senator Miss C. N. DRAKES: Madam Chairman, if I may, just for information purposes. Miss Belle, you are saying within the Electronic Transactions Act there are data controllers?

Miss SHAWN BELLE: Yes.

Senator Miss C. N. DRAKES: Are they registered?

Miss SHAWN BELLE: The registration regime as provided for under the Act, and regulated by their Minister, meaning the Ministers responsible for Electronic Transactions, wherever that may fall within the sphere. They have a different regulatory system, but it has not been. It has not ever been set up, it is done by regulations. So that is a completely different scheme, right. Now, there is no requirement yet for registration, because there are no regulations that have been drafted to regulate their registration. That is why I am saying that it is sphere of operation that is very, very limited.

Senator Miss C. N. DRAKES: Thank you.

MADAM CHAIRMAN: So if I may clarify, the definition in the Data Protection Act. is wider, broader, and differently applied.

Miss SHAWN BELLE: Yes, Madam Chairman.

Hon. C. S. V. HUSBANDS: My question would be, what is the implication of that, for what Mr. Hollingsworth, has outlined? My understanding is he is saying that what is required of a small business person needing a Data controller that that would be beyond the means of a lot of people who have data as a part of their...that was a little while back but everybody heard? I was just saying that I want to understand now given what, Mr. Hollingsworth, has placed on the table that the demand for small business is going to be great. What then would be the options or solutions to make it feasible for a business to be able to....

Miss SHAWN BELLE: Madam Chair, I am reticent to approach this because it gets into the elements of governance and matters that are ministry related or policy related, but the fact of the matter is that when you are setting up a business there are a number of requirements that have to be adhered to. So [that] for instance, if a hairdresser. If they decided that they needed to trade as a business they are going to have to register under the Businessman's Act; they are going to have to pay the fees for the name; they are going to have to deposit all the documentation related to that, as well as under the Health Act legislation; they are going to have to get licensing to operate. All of those things amount to a cost but all of those things are incidental to the running of your business. Now, in terms of anticipating, I understand the concern of the business community that you are adding onto the responsibilities that they would have, in terms of dealing with business but the fact of the matter is that I do not know that there is a streamlining of how you do business, and that is not something that the Office of the Chief Parliamentary Counsel can be asked to refine, you would have to tell us what you are contemplating. Another way, [let us] take the Electronic Filing Act, what that has done is that it allows for the filing of documents that would have been required under certain enactments to be submitted in electronic form. That is a form of streamlining but it only applies to certain Acts that are covered by the Electronic Filing Act, specifically those Acts that are administered by the Registrar, Corporate Affairs and Intellectual Property Office, that is a form of streamlining but you then cannot ask the Office of the Chief Parliamentary Counsel to kind of find a system to streamline the way that you do business. I do not know if you understand the trespass.

MADAM CHAIRMAN: I think one of the things we recognised is that there is some consideration for the micro, small, medium enterprises, the GDPR seeks to speak to that in its own way but we may very well have to deal with that either in the Regulations and that is where we are thinking we may very have to deal with that. I think at the same time too we have to recognise that we are operating in a different

environment and [that] therefore when you are operating in a different environment [that] there are going to be different things that are required in order to operate in that environment. And I think that there is a tremendous opportunity here for there to be some pooling of resources of some of the enterprises, and I will leave that to the Minister responsible for that, but basically my perspective is that there is an opportunity to create shared services in a way that makes sense for them. so [that] there are a number of different ways but I am sure [that] the Minister and his team will come up with how they would wish to do that but we are suggesting that we may consider something for that in the regulations.

So in terms of the reduced requirements of the Data Controller as a specific recommendation on page 4 (2), I am hearing that we wish to keep it as it and not necessarily reduce that but rather take into consideration the best way we can, if there is a case for micro and small enterprises. Is that correct, Committee? Or please correct me if you have a different understanding.

(The Committee concurred)

MADAM CHAIRMAN: So we can go on to the next one? We will say as of (2), there is no correction, that it will not have an impact on the Bill. Minister Sutherland.

Hon. D. G. SUTHERLAND: Madam Chair, one of the areas in (2) that I think that we ought to be aware of is this whole [issue of] public awareness. Mr. Hollingsworth's submission speaks to "until such time as the public is aware of, and fully understands the value...." Yes, indeed, the time is ripe and I heard you mentioned it, we need to explain to the public what is the role of a data controller or what is a data controller as it relates to these small businesses. I think that will bring some clarity. I do not think his main issue surrounds the small man, one or two individuals having a business and indeed having to employ the controller, the whole gambit, so that if we can explain that, because they are looking at a cost, the whole start-up cost for business, he indicated that businesses will not be able to thrive in an environment where we are imposing all of these restrictions. Indeed, the GDPR is a good point to reference because we have to be EU compliant as we do business because we are not doing business in a vacuum or within the 166 square miles because some of these companies also, whether they are digital or whatever type, they are indeed transacting business within the EU and that has to be put out there. In addition, the whole cost aspect, and I heard Miss Belle mentioned it, when you go to register a business these are the areas with which you have to comply, at Corporate Affairs and Intellectual Property Office depending on the business whether it is health or agriculture and the lowest or simplest cost is \$150, so we have to educate the public this is just a probably one-off cost and [that] it is not part of the business operation when you have to factor it in once a year or....

I do not know how often you would have to factor in this cost but these are some of the things we have to do, public education is very critical at this time and I myself am not aware whether or not it is a one-off cost, so it is very important at (2) the public awareness and the sensitisation explanation as it relates to micro, small and medium enterprises. I do not think [that] it is a big issue but when you do not give people information [then] it becomes a big issue.

Senator K. J. BOYCE: Madam Chair, through you, following on from the Minister's point, there is a slight variation from my perspective, the issue being, Ma'am, is that there are three positions that I am seeing under the legislation: the Data Controller, the Data Processor and the Data Privacy Officer. Those three titles in terms of accommodation, facilitation or creation within an organisation if you are sole business individual, a one-man shop, you could have your company under the Laws of Barbados but who is going to fill those roles and I think that it should be something that we consider as to what level. This is why I ask the question, what level does this obligation trigger, because there are going to be small and micro enterprises, as the Member of Parliament and Madam Minister had indicated, who would be impacted by this obligation, so [that] if we could perhaps set a threshold – I do not know – but just reading it in terms now that someone has to be defined, someone has to be stated. That is the first point, then when you turn to the obligation with regard to the binding corporate rules at section 25, it does indicate as though the concept is that it applies to a commercial or corporate entity but I do not know if we could perhaps clarify that.

Miss SHAWN BELLE: Madam Chair, a number of issues were raised there, let us talk about the Data Protection Controller and the Data Protection Processor. Now, the thing is, it is by virtue of your operation that it takes where you would be a processor or a controller *per se*, so it is not as if you are taking on some kind of profession or something like that. Most persons, legal and natural would be Data Controllers. The problem is whether they are also Data Processors. As to the data privacy officer.

Senator K. J. BOYCE: Sorry, can I just stop you there. Is it contemplated that you can be both the Data Controller and the Data Processor?

Miss SHAWN BELLE: It contemplates it, yes.

Senator K. J. BOYCE: Okay.

Miss SHAWN BELLE: But because for the most part, most would be Data Controllers and controlling their Data Processors is most likely that your operations would be at their core Data Controller.

MADAM CHAIRMAN: So my understanding is that you can be both in a situation.

Miss SHAWN BELLE: Yes. Now in terms of the Data Privacy Officer, that person is only designated in certain circumstances as explained in Clause 67. (1). When you are a public authority or body except for the Courts, where your core activities as a Data Controller or Data Processor consists of

operations that by virtue of their nature or scope, purposes, regular or systematic monitoring of data subjects, are on a large scale. Thirdly, the core activities are, processing on a large scale sensitive personal data. Now the problem is the interpretation of large scale. Now the GDPR does not actually explain what large scale is. What the guidance does not seem to be pointing to is a working party kind of meeting that came up with some guidelines in relation to what would be considered to be micro, small-medium sized, but they are linked to the number of employees and the revenue that is generated. The problem is that they are linked within the European context, so what would have to happen, is that the Ministry would then have to give instructions to make it locally right. That is why then the approach that was taken is because most would be Data Controllers and you would be handling the data, an obligation should be imposed on you to make sure that you protect person's right because that is the overarching policy, so you cannot be allowed to get away with it. But if it is that you want a straddling or a hierarchical type of treatment, then the Ministry is going to have to take the time to understand what that means. For instance, in the Barbadian context, you would be talking about small business and the Small Business Development Act. For instance, Section 3 goes into a breakdown of what it would mean, they referred to revenue, they referred to the type of business, the number of employees, *et cetera*. Some of you are familiar with the set up there. Is it that you want your concept of what a small business should be to be trained on existing legislation that defines a small business? Or should be looking at something else? This is the purview of the Ministry, so it requires policy directive, but what was the overarching thought process, is that all the persons that to whom responsibilities should be given, they should be given.

MADAM CHAIRMAN: May I recommend to the Committee, the Minister responsible is here and we are just talking about that and will ask what guidance he would wish to give us with regards to how we would deal with small business, micro and small business in the context of this.

Hon. D. G. SUTHERLAND: You are putting me on the spot. What I can say, I do not want to opt out of it, but give us until the next meeting and indeed that will be clarified. We may want to maintain what is in the Act because we have not done any other legislation since the Act, but we are indeed looking at a micro, small and medium enterprise strategy and then after that the Act. That is probably on the not so far horizon within next year. Give me until the next meeting and I will have that clarified for you.

Miss SHAWN BELLE: Madam Chair, just some other observations in relation to implementation.

MADAM CHAIRMAN: Are we still on the number 2

Indistinct Audio.

Miss SHAWN BELLE: Probably it may come

up again.

Senator Miss C. N. DRAKES: Madam Chair, I just want to interject here very quickly so that we can move on. It is in addition to the discussion about the size of the business, can we also look at the risk associated with the type of data. Because you may be a small business but the information that you have is extremely sensitive, so just to have that table in terms of also looking at the criteria by which you may have to have let us say the Data Privacy Officer.

Hon. Ms. C. S. V. HUSBANDS: Just one more thought if I think you would have mentioned it earlier. The workload or the requirements in terms of how much would need to be done, an assessment of it, so that you get a sense of how much demand it would put on a small business.

Asides (Indistinct Audio).

Hon. Ms. C. S. V. HUSBANDS: Right

MADAM CHAIRMAN: I am not sure you can get a definitive, you would need some clarification. I am not sure you would be able to get definitive, it would vary, so for example, I could be a company that does data and that is my core business. That might be different than a company that is selling books.

Hon. Ms. C. S. V. HUSBANDS: No sorry, I was thinking.....

MADAM CHAIRMAN: *(Indistinct Audio).*

Hon. Ms. C. S. V. HUSBANDS: Yes, which is true, but I was thinking more of the lower level one. I think somebody who is into handling a lot of data would recognise that they would have to do a fair amount to make sure that they are compliant, that they do what they need to do on a regular basis, but it was going back to the example that CPC put, the hairdresser. If we could get some kind of idea of how much demand it would put on that business to see how much load it really is, then it would present us with a better idea of if the Ministry of Commerce is going to make some recommendations and changes that it is doing that in relation to how much demand is likely to be put on the business in order to be compliant and stay compliant.

MADAM CHAIRMAN: Let me just make sure that I understand you. So you are saying perhaps we can identify a basket of businesses if you want to call it or a set of businesses. Here are hairdressers, a sampling of businesses, here is pharmacists.

Hon. Ms. C. S. V. HUSBANDS: That then would have a light load. Yes.

MADAM CHAIRMAN: Here is a coconut vendor, here are these various (persons that) have these different groupings of businesses and then come up for some costing for that

Hon. Ms. C. S. V. HUSBANDS: Highly like demand.

MADAM CHAIRMAN: Is that what you are saying.

Hon. Ms. C. S. V. HUSBANDS: Yes that way we can determine whether it is heavy, too heavy or what needs to be done, or if anything needs to be done.

Hon. D. G. SUTHERLAND: I heard Senator Drakes mention the point. Let us use the example of a hairdresser, a sole practitioner, with a database of 200 and so clients. What are the risks associated there? That database would have in it, the type of hair being used, I am just using examples, whether there are scalp issues. You have stuff in a database, even though it is a sole practitioner, it is still high risk in terms of taking that person's information out there, because you may not, Senator Drakes or Senator Wiggins, they might not want Minister Marshall to know about their scalp issue. Indeed, that is a risk and I am not sure how Minister Husbands in terms of the level that you want to put on it. It is a good point raised by Senator Drakes. You cannot only look at the number of employees but you have to look at the risk because you are dealing with information across borders and everything like that now so. I do not think we can just look at the size of a business as it relates to the risk because you are dealing with information across borders and such like now, so I do not think we can just look at the size of a business as it relates to how we are trying to classify micro, small and medium enterprises here. It becomes more tedious and technical.

Hon. Ms. C. S. V. HUSBANDS: Sorry, it is my misunderstanding. What I was suggesting was not so much quantity of data or anything like that. I accept the point about the risk but what I was asking was what would a small business like a hairdresser have to do be compliant, to stay compliant and keep the business safe? If there was a way to capture what demand it would put on the business, it would then make it easier now to determine what needs to be done or how to help a business like that, which would have less sophistication than a small data analytic company that has five people but who are really dealing with some stuff and know what they are doing. It is really about understanding the demand this will put on them so that we can determine how frequently they would have to do things if there is something that needs to be done. If they have to hire somebody, what is that going to look like? It is more that type of thing.

MADAM CHAIRMAN: Minister Husbands, I take your point in that there are going to be certain groups of businesses, a significant number of them, which will all need to be educated in a particular way. I think what we were talking about earlier – I think we discussed it at the last meeting – is that we have businesses, for example a pharmacist, which will have a very different level than the hairdresser, and the discussions we were having was that when we get to public education it cannot be a one-size-fits-all. It has to be where we are able to target the education to the particular business type, and it means then that we have to find a way to cluster the business types and then do public education that would be specific to that cluster. That was part of the conversation, so it still links to No. 2 which is how we do the public education. I think that

is further in terms of how we actually educate the public as opposed to determining whether or not we need to reduce the responsibility of the Data Controller, which is what the submission is actually asking us to do. What I am hearing people say is, "We do not need to reduce it. What we need to do is find ways in which we can support and help to mitigate the impact." I believe that is what I am hearing. Yes, Miss Belle.

Miss SHAWN BELLE: Madam Chair, just to make an observation now. In terms of how things work on the ground in various jurisdictions, a lot is placed on the Data Protection Commissioner to issue codes and to deal with certain areas that require guidance. For instance, let us suppose that people want to know how data protection would apply to installing surveillance cameras on their properties. The imagery would fall under the data protection, so then what the Data Protection Commissioner would do is issue a code to instruct businesses on how to be in compliance with the Act, so you have to notify the person that you are being surveilled and the purpose for which you are being surveilled. That kind of transparency has to be put into your policy in terms of implementing.

When you are putting this in place, it is really important for you to get the Data Protection Commissioner in place so that he or she can start generating the codes for guidance on these various areas. Even things like consent of children and that kind of thing. I do not want to digress but the point is that this person is very important in terms of the educational exercise.

Asides.

Mr. CHESTERFIELD COPPIN: I just want to add that whether a company is required to have the three officers was mentioned, but there is a model. There is a model existing in Europe where those things can be outsourced so maybe we could perhaps, in dealing with those small businesses, see how best we can incorporate a model like outsourcing as well as opposed to the small businesses taking on the three particular roles.

MADAM CHAIRMAN: Thank you very much for that submission. Senator Boyce?

Senator K.J. BOYCE: Finally, on this point, Madam Chair, I think Miss Belle has clarified. I am pretty comfortable with the concept that it can be both controller and processor. I was thinking that this is something again for yourself, Madam Chair, and the Attorney General to refer to this Bill. I believe the exemptions that are listed out in the Act set a framework if indeed there is a small business segment that you wish to consider in the future, and I think if that small business segment is then defined based on the criteria set out by Minister Husbands, as well as in consultation with the relevant Cabinet, you may find a solution to exempting the small business holders from the purview; the same way that you provide for the lawyers, the Government and for the parliamentary privilege that exists, Ma'am. I think that may be the

"out" that we can look at providing if it is to be considered for those businesses which you do not wish to put under the obligation.

MADAM CHAIRMAN: Thank you very much, Sir. Let me tell you what I understand with this and we can now move on from this. This is the final comment on it: We are not going to make any adjustments to the requirement for the Data Controller, as required. What will happen is that we will seek as part of the preparation before a Proclamation to get the Data Protection Commissioner in place ahead of time so that the necessary codes and all of the rest can be taken care of. The regulatory framework would have to be put in place ahead as well to help to guide some of these, including treatment regarding the small businesses. Is that what we all understand? Yes? Okay.

Asides.

MADAM CHAIRMAN: Let us move on then. The other point that was made here was the requirement of registration. We are at No. 3 on Page 5 of that same submission by Mr. Hollingsworth: That the registration and certification of the Data Controller be phased over a period of three years from enactment. Any discussion or comment on that? That is Page 5.

Asides.

MADAM CHAIRMAN: Is it necessary at this point?

Asides.

MADAM CHAIRMAN: There is no need therefore for us to address this for this to have any impact on the Bill at this point in time? Okay. The third is to clarify the term in writing as it relates to the Electronic Filing Act. My understanding from the submission from the representative of the Chief Parliamentary Counsel is that there are really different Acts altogether relating to very different things, and perhaps at this point in time we may wish to keep the definitions separate as they are, leave this definition to the particular Act and seek not to deal with it.

Miss SHAWN BELLE: Madam Chair, just for clarification. What you just spoke to was the Electronic Transactions Act. The Electronic Filing Act now is a completely different piece of legislation which he is asking about, so we need to clarify.

MADAM CHAIRMAN: Do we need to clarify this term in writing as it relates to it?

Miss SHAWN BELLE: In terms of having it in writing that is not really in that Act. What that Act is supposed to facilitate is the electronic filing of documents that would have been required under various pieces of legislation by the Registrar of CAIPO (Corporate Affairs and Intellectual Property Office). That is the central focus of that Act, so you would not find anything to do with having things in writing there so I do not know whether he needs to be asked for

clarification on it.

MADAM CHAIRMAN: This is irrelevant therefore to this Act.

Miss SHAWN BELLE: Yes.

MADAM CHAIRMAN: So if it is irrelevant we will not consider it as part of the Terms of Reference of this Committee. Okay? That is Number 04.

Number 5: The definition "profiling" which is on page 15. Part 1 of the current Bill, that the definition of "profiling" is not in sync with current technology trends. I have to understand that there is a difference ... in fact let me let Miss Belle speak to that because it is a legal question in terms of definition.

Miss SHAWN BELLE: Madam Chairman, just in terms of the definition of profiling, that definition is informed directly by reference to Article IV, 4 of the GDPR. What I am finding is that there is a perspective being put forward by the ITC and IT heavy constituency that is saying that the Act should take into consideration all of these very technical things that have to do with the working of technology and while I understand their concern, the overarching or the mischief that you are trying to address is how the use of technology makes your personal data vulnerable and so it is the backdrop with the focus being the protection of the data once it is put in electronic form. There may be nuances to that and I need to do more research to see what is the - I suppose this is colloquial - endgame of ICT and like industries because all the terms are informed by the GDPR and it has a specific focus and there is also an understanding of these terms in general data protection law. If we go and deviate then we are setting ourselves up to be in contradistinction to other jurisdictions that are trying to follow the same type of regime.

Senator K. J. BOYCE: Madam Chairman, the definitions are just ... following on from Miss Belle, she is absolutely correct. The definition is taking from the GDPR Article IV, 4. I do not think we need to touch it.

MADAM CHAIRMAN: If it was taken from the GDPR do we, as a Committee, believe that we need any adjustments to this as per number 5 on page 5? If not, let us just say no and move on.

The Committee answered a resounding "no".

MADAM CHAIRMAN: Are we unanimous? Is there anyone who is fundamentally opposed to us continuing the "profiling" definition as defined in this?

The Committee answered "no".

MADAM CHAIRMAN: Okay, then we will continue with the "profiling" definition as is with no adjustment to this Number 5.

Number 6, page 5, on that same submission, that there is no justification for sensitive data as defined by this Bill to be legitimately processed by political religious or philosophical bodies given that the Bill itself gives the data subject the right to migrate their data from one to the other. If you flip to page 6, it

continues that sensitive data should only be processed by persons who fall under implied or explicit confidentiality. If you look at page 65 - I know Mr. Attorney General you said you do not want a page, but that is how I had written it - Clause 58, (5)(b). This is the non-lawyer. I am just identifying where I would have seen reference to it when I went over these questions.

Miss SHAWN BELLE: Madam Chairman, just for clarification, because since it is ... yes. The protection of sensitive data is something that is required under the GDPR, Article IX and the reason for protecting such is revelatory through the understanding of the definition. If you are talking about biometric data, if you are talking about your medical records and even the associations that you make, being a member of a trade union, these are matters that should not be dealt with lightly and there is a responsibility that should be taken into account when you are dealing with such data. The GDPR specifies it and the various sections, one of the first Clauses within the Act, seeks to show how those things should be handled.

MADAM CHAIRMAN: Are you clear with that? You have a quizzical look on your face, Hon. Ms. Sandra Husbands?

Hon. Ms. C. S. V. HUSBANDS: I understood what she has said. I was awaiting.

MADAM CHAIRMAN: Any further comment on this section in terms of ...? Do we see that this concern that is raised having any significant impact on the Bill as it currently is?

Senator Miss C. N. DRAKES: Madam Chairman, correct me or please clarify for me. Is this submission related to Clause 9.(1)(e)? That is a Clause that I had some discomfort with myself and that is basically the processing of sensitive personal data and he said, the processing is carried out in the course of its legitimate activities by anybody or association with which exists for political, philosophical, religious or trade union purposes.

Miss Shawn BELLE: Madam Chairman, the thing is the construction is informed by the GDPR. The processing of sensitive personal data, this is Clause 9 that I am referring to, in the chapeau, "processing of sensitive personal data shall be prohibited unless" and then going into the paragraphs it lays it out and then going on in E. Now what I am saying is that formulation is informed by the GDPR. We are trying to become compliant with that. The only way then that you depart from it is if the Ministry or their submissions are saying that we should depart from that in some form because there is some interest that we are taking into account.

MADAM CHAIRMAN: The question is, is there some interest we are not taking into account or is there some harm that we believe we would be doing?

Senator Miss C. N. DRAKES: Madam Chairman, I raise the point and I understand Miss Belle's point as it relates to compliance, however, I will still state that that was actually one of the Clauses that I noted as it relates to the justification for why you would

allow for those entities or bodies to process sensitive data. That exists for political, philosophical, religious or trade union purposes.

Hon. D. D. MARSHALL: I am trying to understand what the Senator is saying. If you look at the categories at (a) and (b), not established or conducted for profit. Immediately that tells you that the information is not expected to be created to enter into anybody... We all go into things and our email address and everything goes out and then before we know it we start getting emails and unsolicited calls so by eliminating the profit motive you narrow the scope, and then secondly, it exists for political, philosophical, religious or trade unions purposes all of which are publicly recognised and legitimate purposes that are in fact protected under every known democratic constituent. I think what this is therefore trying to do, if we go back to the chapeau, is that nobody is allowed to process sensitive personal data. Remember what sensitive personal data is, it is defined in the definition section, that is the rule, but then the exceptions are created at the next Clause, the exceptions are that if a person is carrying out... by anybody or association that is not established for profit, so I think that is a box we can tick, but then exists for political, philosophical, religious or trade union purposes, and then it goes through the other things, so we still need to look at 2, 3, and 4.

Appropriate safeguards for the rights and freedoms of data subjects must be guaranteed. It was ... relate to individuals who are either members or have regular contact with the body for its purposes, and (4) it does not involve the storage of the personal data to any third party without the consent of the data subject, so taken as a whole I would like to say that I do not think that there is any reasonable challenge that could be mounted in those circumstances so I would like to ask the Senator if she would accept the Clause as it stands.

Senator Miss C. N. DRAKES: Madam Chairman, thank you and I would like to also thank the Attorney-General for his clarification.

MADAM CHAIRMAN: My understanding then is that we will accept the Clause as it stands.

Can we move on then to number 7 still on Page 6 of the Mr. Hollingsworth's submission, where automated decision needs to be clearly defined? Do we need to further define this with such specificity as it is being defined here?

Hon. D. D. MARSHALL: My problem, Madam Chairman, is that I do not understand what Mr. Hollingsworth is saying and if I cannot understand what he is saying then I have a little bit of difficulty trying to process the direction that he is trying to orient my mind in. Perhaps that is the beauty of a Committee like this because it is precisely for these reasons that we need to meet in caucus and try to go through what is happening, but I cannot usefully comment on it because I do not understand what Mr. Hollingsworth is saying. He might have been better off coming to sit here and give us an explanation.

Senator K. J. BOYCE: Madam Chairman,

through you, can I ask Ms. Belle if the definition from the GDPR is utilised in terms of that section. Is the GDPR the source for the definition?

Miss SHAWN BELLE: Madam Chairman, the automated decision is not specifically defined. What happens in the language is that it connects itself to profiling and so what is understood as automated decision-making has to do with the "profiling", so if you look at the "profiling" definition you would then be talking about the use of personal data to evaluate certain personal aspects of the individual analysing and predicting aspects concerning the individual's performance at work, economic situation, *et cetera*, so you read those there. The concern then is with that sort of. I guess, action, is that it could promote discriminatory treatment.

Madam Chairman, when you refer back to Clause 18 though, it is stated in a way that is similar to the constitutional provision so there is a declaration in Clause 1 that speaks to, you should not be engaging in solely automated processing including filing but then when you go to subsection 2, then subsection 1 would not apply in certain circumstances and then you have to take into account those circumstances. Additionally, it speaks to subsection 2 not applying where the sensitive personal data is concerned unless it is in the public's interest and suitable safeguards are in place to protect the data subject rights, freedoms and legitimate interest, so it gives an operation within which it is, I guess, to be implemented if you put it that way and the provision again is informed by reference to the GDPR.

Hon. Miss C. S. V. HUSBANDS: Just a question. I am just trying to understand the parameters of that particular profiling action. This might be a bridge too far but I am just asking to find out if it extends out here where for example an employer is looking to employ persons and they do the psychological testing and profiling and they are going to use this information for example to make a decision about employment, would it extend out there or that is cut off at people using information for marketing or something?

Miss SHAWN BELLE: Madam Chairman, that would be triggered if the inputted information were then used to create an automatic decision, so based on the fact that you are black and you are disabled then that creates a profile that maybe you are poor and so maybe you are not supposed to be entitled to a certain loan or things like that so that is where that becomes discriminatory and that is what they are trying to target and protect against.

Senator Miss C. N. DRAKES: Madam Chairman, if I can try to frame it differently so that we can possibly get some clarification, for example, an automated decision is for instance, if you go for a line of credit, the bank has certain parameters, criteria and the algorithm likely makes a decision for the bank and the teller says your loan is declined, is that the type of automated decision-making that we are talking about?

That being, I then take Mr. Hollingsworth's concern regarding the lack of definition behind what we

are including and not including given Minister Husband's, introduction as well. In terms of what are we deciding is automated decision making, given that is a very central part of data processing and anything technologically driven at the moment. A lot of the information is used by machines, artificial intelligence. So, I am not sure if there is a best practice or a general definition that is used for automated decision making in legislation at the moment.

Miss SHAWN BELLE: Like I said, the automated decision-making is tacked onto the profiling, so and then what we probably need to understand is that this regulation, the GDPR, just came out into 2016 and then came into force in 2018. So the jurisprudence that would lead to an understanding or interpretation of these provisions has not actually been generated, so it is working. There are several working parties, it seems in the European Union that are dealing with different issues that would inform interpretations. So, for instance, if it went to Court then the Courts take into account that as an intrinsic instrument for interpretation of this legislation.

Senator K. J. BOYCE: Madam Chairman, I do not think there need be any change since it fits with the definition currently held in the GDPR, and leaving it wide just allows for the wider interpretation. I do not see it as an issue to stop the progress of the legislation.

MADAM CHAIRMAN: If I may be permitted to add my opinion here, what I see him define is specific types of technologies, and if you leave automated decision open then it becomes technology neutral. So when you get new technologies this is technologies we know of right now, there may be others coming in the future, I think that we are wise to not limit it to naming specific technologies, but leaving technology neutral, and keeping broad in mind. So are we in agreement therefore that we leave it as is?

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Fine. I believe that, that is the final submission on this particular paper for our consideration. Have I missed any? Number 1 sparks out ???of clarify legal??? (*inaudible audio*), how is it or supersedes Article 6 of Electronic Transactions Act. That we no longer need....

Miss SHAWN BELLE: Madam Chairman, we did actually cover it when I spoke to the fact that the Electronic Transactions Act, one Act. Electronic Transactions Act, one Act. Electronic Filing Act is another Act. His point dealt with the Electronic Transactions Act, and that there is a part that deals with Data Protection. What I was saying is that part is confined within that particular Act.

MADAM CHAIRMAN: So if I can say now in conclusion, we are looking at this paper that while we take for instance consideration while we are grateful for the submission at this point these recommendations particularly with respect to public education will certainly be taken on board for some consideration.

How we will be able to treat to the micro, small, and medium enterprises perhaps using models that, Mr. Coppin would have suggested could be considered and dealing with the matter within the context of regulations as Mr. Sutherland, would have also dealt with this is what arises from that. Other than that they will be no further impact on the Bill based on this submission.

If at this point it is now approximately 20 after 1. May I invite the motion for us to suspend for lunch and return at 3:00 p.m. or at 2:30 p.m.? At 2:30 p.m. or do you wish to resume sooner? We have four more submissions right now to consider. Do you wish to try to do one more at this point or do you wish to break for lunch? What is your preference Committee? Okay we will break. I just would like to invite a motion then for us to break for lunch and return and return at 2:30 p.m.

RESUMPTION

MADAM CHAIRMAN: Good afternoon. Honourable Members, this Sitting is resumed. Members, the submission that we are going to review at this time is the Barbados International Business Association. There are three major recommendations or suggestions for consideration that are put forward:

- (a) to incorporate cognitive technologies as part of the definition of data processor;
- (b) to set up a local agency that provides shared services to enable micro, small and medium enterprises, which I do not think falls within the purview of this Terms of Reference but we can discuss it;
- (c) Use a percentage of income versus a fixed sum as it relates to penalties.

Members, those are the three things being considered, let us consider the first, the case for that is placed on the very first page of the Barbados International Business Association submission under Item 1. Do we see here a need for the incorporation of cognitive technologies as part of the definition of data processor, and what would be the implications for that? If we could get Miss Belle to speak to the definition, that would help us.

Miss SHAWN BELLE: Madam Chair, in relation to the definition of data processor, that definition is informed by Article IV of the GDPR. The inclusion of the ICT's industries understanding of data processor is noted but if you include those considerations, again it would set us apart from others who are trying to implement the regime and what you would not be wanting to do is having set that up, then have to explain why you would not be providing the same protections or the same flexibility as in other jurisdictions, so that is my main problem in terms of incorporating what their understanding is of data processor.

MADAM CHAIRMAN: So you are saying [that] this would provide less flexibility if we were to do this?

Miss SHAWN BELLE: I believe so and as I would have observed earlier, the ICT's constituency has a particular understanding that is rooted in more technical things having to do with technology rather than focusing on the protection of persons' data which is what data protection is about. But I mean, I could be corrected if it is that there are some learning that say to me that we should take that into consideration but I looked at the legislation from various jurisdictions and they all take their cue from the GDPR.

MADAM CHAIRMAN: Does any other members on the committee have a different perspective on how we should treat to the incorporation of this element in the definition?

The Committee responded in the negative.

MADAM CHAIRMAN: Are we in agreement therefore that we will allow that definition to stand as is without the incorporation of these cognitive technologies? Are we in agreement?

The Committee agreed in the positive.

MADAM CHAIRMAN: Okay. Excellent. We now move onto the second consideration. Local agency that provides shared services to micro, small and medium enterprises to implement data protection requirement. I think one of the things we acknowledged earlier is that there may be some need for us to look at this and see what kind of support should be put there. I am not convinced that it needs to be placed in the legislation at this point in time and therefore that that should be a consideration but not necessarily to be incorporated into the legislation.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I would suggest that it makes a good opportunity for people to start a service to provide, you know, for five or ten people to give them that coverage, so that it could generate potential business opportunities for others.

(indistinct response)

Senator Ms. A. M. WIGGINS : Madam Chair, the consideration I would like to say here that would incorporate discussion that went on this morning. it would be in addition to what I said in reaching out to the different groups of organisations out there. I know that Minister Husbands was associated with the Small Business Association but I do not know if Senator Holder can make, or if you can make her part of the Committee, because a lot of this legislation seems to be directly impacting on the small business people and I think [that] they should have a voice and given that we have the Senator here who is the Chief Executive Officer of the Small Business Association I would say, with respect, Ma'am, that either make her a part of the Committee or let her come in and make a presentation on behalf of the Small Business Association. Ma'am, to continue what I said before, then they would say, well, you see, they did this and we were never consulted. With respect, Ma'am.

MADAM CHAIRMAN: Mr. Coppin, you were involved over the last several years with the consultations. To your recollection was there representation by the small business community as inputs to the Bill that is drafted at this time.

Mr. Chesterfield COPPIN: Yes, Madam Chair, we would have had consultation with Lynette Holder and all stakeholders with regards to the drafting of legislation and so on, but the thing about this is that we are saying small businesses because we have maybe an affinity and a feeling but it applies to all businesses, just that we think that because they are small [that] they are vulnerable and I do agree with the vulnerability, but the pieces of legislation pertains to all businesses.

MADAM CHAIRMAN: I think what I am gathering from that is that there are different client/groups or stakeholder groups that we wish to engage. As part of this now, I would have to be guided by the experts, the Clerks of Parliament but my understanding is that the Committee as constituted is the Committee as constituted, that the Committee will then consider what it needs to consider in Committee and once we have made the decision, we can then engage other stakeholder groups as we start moving towards implementation. And I would wish to make sure that we have that level of input, so thank you for that. Would the Committee agreed that that is the way that we go forward?

(The Committee responded in the affirmative.)

MADAM CHAIRMAN: In support I would say that, yes, we do this, I agree that this is a business opportunity and I also would wish to state that it is not the Government's place necessarily to take up this opportunity on its own. I think that we also would need to encourage the private sector to take this up as a business opportunity, rather than Government do it all at this stage.

The final consideration was the use of a percentage of income versus using a fixed sum as it relates to penalties. What is the Committee's perspective on that?

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I agree with this recommendation here. As it rightly pointed out, large companies with very deep pockets can make provision for accidental or deliberate violation of the legislation without skipping a beat, whereas that same fine on a small business would put it out of business altogether and therefore a percentage, I think, would be better with a floor minimum, if you want, a reasonable \$1 000 or \$2 000, something that a small business would feel but it is not going to put them out of business to have to pay the fine.

Senator Ms. A. M. WIGGINS: Madam Chair, I think that discussion went on this morning at some point where I think they were saying a judge has discretionary powers, in terms of whether they are going to charge company X zero dollars or half-million dollars, so I think we more or less would have....

Asides (Indistinct

Audio).

Senator Ms. A. M. WIGGINS: Yes we would have covered that this morning. I think Miss Belle spoke about it also.

Asides

Senator Ms. A. M. WIGGINS: Yes the Judge has discretionary powers, so she would not charge somebody..... because you see and then we talk about the whole question of small businesses and information because lawyers might, as sole traders might be viewed as a small business but they might be holding a lot of sensitive information and my favourite group of persons, doctors, that they might be small but they handle exceedingly sensitive information. Are you going to then impose a fine on the doctor who has the

more sensitive information, the harsher should be the fine rather than looking at it in terms of the amount of clients that the small business itself holds?

Miss SHAWN BELLE: Madam Chair just to raise the fact that another one of the submissions, it mentions the setting of minimum penalties. Now that has been struck down by the Court of Appeal as unconstitutional because it fetters the discretion of the Judge to tailor the punishment to the particular offence, so that just to state again, in legislation the expression of the penalty is at its maximum. The Judge will have the discretion to impose no penalty or the highest threshold, depending on the circumstances of the case, whether there are any mitigating factors, whether the person is a frequent person who contravenes on more than one occasion, those kinds of factors. I just wanted to say that once again.

MADAM CHAIRMAN: Any other member would wish to say in terms of setting whether percentage or flat range.

Mr. Chesterfield COPPIN: Madam Chair, I would prefer it to stay as is in terms of a flat amount. As I mentioned before, in dealing with percentages especially with the landscape of our small business structure, it might be in terms from an operative level it might be difficult and onerous, so because of the bookkeeping mechanisms that some do small businesses have in place. My opinion is that we stay as is for the current moment.

MADAM CHAIRMAN: With the option to review at some later stage if we so choose.

Senator Miss C. N. DRAKES: Madam Chair, just thinking it through, because you have the options of either the percentage or a maximum of the \$500 000.00, is there any room for the inclusion of both? I mean, that is under the guidance of obviously CPC, as she has quietly stated previously that the GDPR speaks to percentages.

Miss Shawn BELLE: Madam Chair, just to say that if you go into that, it is okay to impose that kind of dual regime, but what would end up happening is that the Ministry as the pilot Ministry would have to then get into what constitutes a small business, as opposed to what constitutes a large business, should a medium size business also be dealt with on a different regime. Our tradition in terms of penalties is basically the expression of the maximum penalty, so to introduce this type of a system now actually requires more consultation, more time to look into how it would actually function.

Senator Miss C. N. DRAKES: Thank you.

MADAM CHAIRMAN: In light of these discussions in bringing to close, the three major considerations let me recap what I understand it to be. That with regards to item one which is the incorporation of cognitive technologies as part of the definition of Data Processor, at this point in time we will not change it as we do not want to distance ourselves from the very regulation that informs this Bill. Two, with regards to local agency that provide shared services, it is outside of the scope of the terms of reference and at the same

time while we understand that this is a good thing to do let us encourage it as a good business opportunity for the private sector, not necessarily for Government, but there would be no additional change, no impact on the Bill. Third, use of a percentage of income versus a fixed sum, that rather than either several options were put on that table, either what exists now, a percentage or some combination of the two, and my understanding from the Committee is that you would prefer at this time to keep it as is and review it, and if anything we can make the adjustments at a later stage. Committee is that all complete in terms of what.

Senator R. J. H. ADAMS: Sorry Madam Chair and excuse me for arriving late after the break. I just have a comment on that percentage one, number three there. We said at some point earlier today that it is one thing to talk about percentages of revenue and another thing to talk about the gravity of the data that has been breached. What do we do in that case of a serial offender for example, large or small, possibly cannot afford whether it is a percentage or a flat fee but it is still a serial offender? What other sanctions beyond the financial are available for someone who just persistently, for example, I do not know, let us say it is a small business and they are driven out of business because they cannot pay the fine and the principles just start another business and do the same thing in a recidivist manner. I believe we can find an example of that perhaps not with data breaches but in other areas of the law. I am not sure if the bill can capture this sort of case, but it does seem to me that it could be an escape patch in some cases. I do not have the answer, but sometimes it might mean the disqualification of directors for example from doing the same thing in that business or in another business that is subsequently incorporated. Do we think that perhaps that is something we should consider or is that already been considered?

Miss SHAWN BELLE: Madam Chair, just to intervene, there is the mechanism of the imposition of the administrative penalties under Clause 94, so that the Commissioner can after a hearing where they have contravened certain provisions in the legislation and the Commissioner considers it to be in the public's interest they can make an order for the person to pay to the Crown a penalty of an amount not exceeding \$50 000.00. We put that threshold because it is an admin penalty meaning that the Commissioner or functionary is actually imposing it and not the Court, so there needs to be a threshold on that. In imposing that, the factors that the Commissioner will also take in apart from the public interest, is the nature and gravity of the offence, the intentional or negligent character of contravention, previous contraventions of the Data Controller or the Data Processor in relation to offences. Those are the kinds of factors that can be taken into account in terms of imposing an administrative penalty. Remember too that there is also the enforcement notice, which compels or ask persons to refrain from certain behaviours so that the Commissioner's resources in relation to dealing with persons who may be frequent offenders.

MADAM CHAIRMAN: Your question asked about financial penalties and then you asked about others.

Senator R. J. H. ADAMS: Thank you Madam Chair, it may do, I just want to be clear. Let us say we have a case, because this is something I have seen in Europe. The cases I have seen in Europe involved fraud. Someone creates a company, runs a deliberate fraud and the company is disqualified but the directors, because there is an absence of sanction stopping them, will reconstitute another company and do the same thing again. This is really what I am getting at. Can you stop a persistent offender restructuring under a different type of corporate entity and just doing the same thing again?

Miss SHAWN BELLE: No, Sir, we do not have anything like that but perhaps you need to take that into account in terms of the regulatory framework. The tradition is usually to impose penalties, fines and so on. That has usually been the case but in terms of going into specific administrative consequences like suspending the licence and so on, those are things we would have to work on and articulate fully. Maybe we need to look into it; the pilot Ministry.

Senator Ms. A. M. WIGGINS: Madam Chair, I was just wondering, in terms of what Senator Adams alluded to, if that would not be coming under the Companies Act in terms of the treatment of directors. When companies go bankrupt, as you know, the directors are individually and severally liable for all the liabilities of the company so I am just wondering if you could not cross-reference the Companies Act there.

Miss SHAWN BELLE: Madam Chair, it is true that you can have legislation on similar areas interpreted together. The problem here is that you are looking at a different functionary who is imposing a penalty for different reasons. What you would have to do is create the capacity for there to be regulation in that vein, because it is not regulated under CAIPO. It is regulated under a different regime in this Bill.

MADAM CHAIRMAN: Are you saying therefore that it can be addressed in the regulations as well?

Miss SHAWN BELLE: Madam Chair, this is not a matter that you should deal with in regulations. It is a matter that would have to be incorporated into the Bill. The question is whether the pilot Ministry would be in favour of employing those kinds of methods in order to deal with something like that. Remember too that even if you are talking about suspension and cancellation, you still have to have a right to appeal and a right to be heard and all of that. Those kinds of mechanisms would still be put in place in order to protect the rights of persons, because once they get the registration aspect dealt with then there is a question of going to livelihood and their operations.

MADAM CHAIRMAN: That said, may I suggest to the Committee that we take this one away for further consideration and get back to the Committee at our next meeting before we conclude the Report? How does the Committee feel about this?

Miss SHAWN BELLE: Madam Chair, it is still a question of who would get back to the Committee. Certainly the Chief Parliamentary Counsel is not going to put forward anything.

MADAM CHAIRMAN: No, it would not. This would have to be a consideration among the Ministries that would be involved and we would speak to it in the proper context to get back to you on that.

Asides.

MADAM CHAIRMAN: Okay, then it seems as if we have concluded this one Paper. There are three questions in the back but I think we can answer them quite simply. They are speaking to what is the registration fee for the Data Processor and the Data Controller. Those will be dealt with in regulations. The final question is why does the Data Protection Commissioner have to be an attorney-at-law? Simply because of the functions of the Data Protection Commissioner, he or she really needs to know the law. They need to be versed in the law. These are simple questions to be answered. We have now concluded the third of these. There are two others to go.

I now want to move onto the submission which was the third in line, from Mr. Shannon Clarke with regard to the recommendations. We want to make sure that we give the fullest consideration to all of the persons and entities that have taken the time to submit their submissions. Let us move to the penultimate page, the one before the last, under 'Suggestions for improving the Bill'. Let us go through these considerations very quickly and determine whether or not they would have an impact on the Bill. It reads as follows:

"The requirements for the compliance for the business should match the level of access that the company has to customers' private information, such that the company deals with sensitive information."

I believe that is part of what Senator Drakes was saying earlier. Are there any further comments on this? Should this necessarily impact the Bill as it is now?

Senator R. J. H. ADAMS: Madam Chair, just a couple of comments. I think the answer is "no" because to lay out a different set of requirements for different levels of access really requires a lot of consideration business by business by business, and it is sure to open a can of worms when something goes wrong. I think this is one instance where a blunt instrument is better than trying to wield a scalpel across the ten thousand businesses that are in this country.

MADAM CHAIRMAN: Are we all in agreement with Senator Adams and the fact that this suggestion should not impact the Bill at this time?

Asides.

MADAM CHAIRMAN: Okay, good. We move on to No. 2. I believe we have covered No. 2 with regard to using a percentage for the fines versus the flat range or fee so we will move onto No. 3.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I am glad that this has come up again.

MADAM CHAIRMAN: Which one? Are we referring to No. 2? Okay.

Hon. Ms. C. S. V. HUSBANDS: I think it links back to No. 1. I agree that if you start trying to change up the compliance requirements it gets really hairy. The thing would be that when it comes to penalties, this is where the differences between the operators now would become important. I still think that large service providers are not going to be deterred because they will factor that in. The access to people's data for marketing purposes is so major for everybody, and if half of the people are like me when they ask me if I want to receive things, I say no. To have this database of people is going to be a temptation and many companies that need access to that market will say, I will pay the \$500 000. I am not sure that we would get the deterrent that we are looking for. My other concern is, I heard the issue that the Commissioner – Is it the Commissioner that has the power to impose the fine?

Miss SHAWN BELLE: Administrative penalties.

Hon. Ms. C. S. V. HUSBANDS: Sorry, let me get it technically and legally correct, the administrative penalties, the Commissioner can decide between \$0 to ...

Miss SHAWN BELLE: No.

Hon. Ms. C. S. V. HUSBANDS: No. Okay. I have it wrong. Help me there.

Miss SHAWN BELLE: Okay. They are different regimes. In terms of criminal offences, when the penalty provision is constructed the penalty is expressed at the maximum threshold. The judge, in that case, can impose no penalties or the highest penalty based on the case and what the circumstances are but what I am drawing to the attention of the Committee is that the Commissioner has within his toolbox of enforcement the facility to impose administrative penalties and those administrative penalties have a cap necessarily because he is the one imposing them and they also can only apply to certain sections. That is really what I was talking about.

Hon. Ms. C. S. V. HUSBANDS: Okay. The point I was going to raise is that my concern would be if the person imposing the penalty or determining what level to apply, should we assume that they have a good understanding of businesses and business' sensitive and so on. That is my main concern. The same way how we are going to spend time educating the businesses, educating the public about this so that people can transition on to it, should we not make sure that whoever, whether it is the judges, then we should not assume that they have enough knowledge. What sometimes happens because we are all human is that somebody may be brought before the Court, they committed an average offence, it is nothing huge but because sometimes some people do not know how to handle being wrong, they might have a little attitude in front of the judge and the judge decides, "um-hum, see you, \$20 000 in your bosom" and the small business

closed down. That is my concern. I do not know how we can address it but I feel that some education and guidance for the persons who have to impose penalties should have a clear understanding of some of the things to consider when imposing the penalties as a kind of a guideline or something because you are asking somebody to make a judgment call who is not necessarily an expert in business or small business matters. That is my main concern with the penalty as it stands. I feel some attention could be given to looking at it.

Miss SHAWN BELLE: Madam Chairman, just in relation to the administrative penalties, 94(2) sets out the factors. Apart from the public interest, sets out the factors that would guide the judge in terms of what penalty they would impose. That is the Commissioner who would be an expert in the field of data protection.

In relation to the judges, the thing is that in imposing penalties you are not also only taking into account the construction of the penalty itself but you are also taking in the account the jurisprudence that has developed around imposing the sentence so that there would be circumstances which the Courts have already litigated and have found that in this particular circumstance, this particular penalty is appropriate. I take the point that the jurisprudence in data protection may not have the depth of that yet, but there are a number of working studies and so on that the judges can have a look at to inform how they approached things. I think too that you have to give credit to our judges. They are not incompetent and they understand what is serious and what is not. I think you need to differentiate them.

MADAM CHAIRMAN: Senator Wiggins.

Senator Ms. A. M. WIGGINS: Thank you, Madam Chairman. I just wanted to make three points and one may fit into penalties. Speaking with respect to the whole question of the harvesting of the personal data because sometimes when you log into a hotspot your information is automatically captured by the particular company and then you start receiving emails, you see it on your Facebook page and you did not subscribe *per se* to the company or you did not say yes, you did not tick any box, you just logged into the person's Wi-Fi, be it a hotel, because as you, as soon as you check into a hotel you start getting all the confusion that you do not want, all the information about coming back and a year later I am still getting emails inviting me back to hotels. I am saying that sometimes, because you have to log into other people's Wi-Fi you are going to get the unsolicited emails and everything coming at you. This information can be shared and you are totally unaware that somebody has captured your personal information and it is being shared and you do not know. Of course, when you are going on Amazon and those places and logging in, that information too is shared and then not only is your personal data in terms of whatever, but your financial data is also shared with other companies. Again, as I am speaking to financial data and that is why I wanted the Bankers' Association here because they already capture a lot of personal data.

As I said, they have an integrated system and I want to speak to you off the record about something Senator Adams. They already have an integrated system. If you apply at one bank and say you do not have any loans any other place, they know that you do. That system already exists in Barbados. The question is, did you give Bank A permission to share your personal financial data with Bank B? So then there should be cases where the injured party should be able to get some kind of redress especially from a banking institution for sharing your data without your permission because as far as I know, Senator Adams can correct me here, a lot of the information that we take for granted here in Barbados you cannot easily share in the European Union.

Senator R. J. H. ADAMS: Yes, thanks for putting me on the spot. For the avoidance of doubt I want to make it clear, I have none of Senator Wiggins' personal or financial data anywhere. I am not sure I have the answer to the European Union's part of the question but as you were talking what struck me was not so much the enforcement but the fact that many people will ignore the legislation and it is hard to catch them in the net and I think we have to accept that. Any piece of legislation that has a punitive section to it is going to encounter that I think.

From those examples you gave, what often strikes me from a prior job is that you have no way of knowing who breached your data. You may know somebody is misusing it but you do not know how they got it or who is the original offender in that, so that is not really an answer but a supplementary comment.

Miss SHAWN BELLE: Madam Chairman, I just want to say that in the scenarios that Senator Wiggins would have drawn out, you have the right to have your information restricted, you also have the right to erasure and you have the right to access, so within the sections that they are dealt with, your first recourse would be to make the Data Controller know that this is your desire. If then there is a problem then you resort to enforcement from the Data Protection Commissioner, so those are matters that can be dealt with there. If it is in the situation that Senator Adams outlined where there is not a knowledge of who would have disseminated, the Data Protection Commissioner under the information notice could seek out the information because there would have to be an electronic trail and so in investigating then they would try to find who would be the party that needs to be targeted in terms of providing redress.

MADAM CHAIRMAN: Does that address the matter that was raised? Okay.

Hon. Ms. C. S. V. HUSBANDS: Senator Wiggins raised a very important question and I have a slightly different one. I know that the 'on the surface answer' would be "well just don't go there" but there are so many service providers who make it mandatory for you to tick off yes and that they have cookies that they will trail you and yes we will be giving it out to third party persons but in a responsible manner and it is a service that you have to access so for me as a

consumer I often feel cornered by those companies because it is an issue. If I travel and I go into a hotel I have to have the Wi-Fi to do what I have to do because I am travelling on business, I am not joyriding to say well look I do not mind being without my connection for a week or whatever.

Asides.

Hon. Ms. C. S. V. HUSBANDS: Well, who wants to do that? Madam Chairman, I am just wondering if there is anything that can be done about those attempts to corner the consumer in a way that you are obligated to thing if you want to transact.

Miss Shawn BELLE: The Bill will not address that directly but what is happening is that an environment is being created because of the introduction of the GDPR, General Data Protection Regulations, so that you probably would have received notification from even Google to say to you that they have to perform in certain ways and you provide this information or you do not provide this information, but that is not because a jurisdiction went after Google. What they are recognising is that if they do not comply the sphere for operation, it then starts to close. So it is an environment that is being created because several countries are getting together to say this needs to be handled. It is the same way with like treaties. I mean you can go to international courts and all of that but the main form of enforcement is actually peer pressure so that is what is eventually going to happen in relation to the GDPR because even though it started out as an European Union standard because of the size of the European Union it might as well be an international standard. I do not know if people understand.

MADAM CHAIRMAN: Are there any further comments on that at this time? Okay. Then, is it fair and correct for me to say that we have exhausted the discussion on Number 2 and that we stand by the original decision that had been made with regards to the fines but we do take into account that there are other areas such as those pointed out by Minister Husbands, Senator Adams and Senator Wiggins that we would need to take into account.

Can we move on then to Item Number 3, the enactment of the Data Protection Bill needs to be delayed. I believe that this matter was addressed by Miss Belle earlier when she said that it will be done by proclamation and basically you can proclaim the Bill at whatever time you choose to proclaim the Bill, well if it is an Act then it would become an Act, giving yourself enough room to take care of whatever internal matters would need to be put in place in order to facilitate its implementation, so I believe we have dealt with Number 3 and therefore no further impact on the Bill.

With regards to Numbers 4 and 5, one speaks of public education campaign and business training sessions. I do not think that they necessarily relate to the Terms of Reference of this Committee but we did say that there is some consideration that we would have to give to these matters. With that said, based on our

conversations we will note this submission and it would have no further impact on the Bill as it stands.

The final submission for today we can consider is that from Solutions Barbados and I would just ask for you to follow on from one page to the other, there are four pages of submission. I know that certain parts interrelate and so we may very well be able to deal with several parts at once, so let us start with Number 1, the preamble to the page, grammatical errors. I believe errors happened and they will be corrected, that is why this is in a Bill format and so when it is finalised basic errors will be corrected, and indeed we are grateful for some that are pointed out.

Section 9 deals with the non-consistent processing of sensitive information by political parties, and they are suggesting that this should not be permitted. Is there anyone who has a specific perspective on this? In other words, should this at this point in time impact the Bill in any way. Yes/No.

Miss SHAWN BELLE: Madam Chairman, this actually links back to a discussion that we had earlier and the Attorney-General provided clarification as to why it needed to be included so I would defer to the Attorney-General.

MADAM CHAIRMAN: Correct. So we will move past 9.(1) which would have no further impact. Section 10.(3), that the Data Controller shall provide a copy of the personal data undergoing processing to the data subject. The concern here being that when it gets to the point where the Data Controller has reasonable doubts, Section 21 suggest that they may request the provision of additional information necessary to confirm the identity of the subject. My understanding is that this provision was put here to give the controller flexibility in terms of confirming identity as it.... There may be many different ways other than directly with the subject to confirm identity. So, if this Committee is in agreement that, that flexibility should remain for the Data Controller.

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Therefore this one shall have no impact on the Bill either.

Section 15.(3), page 31, in exercising his or her right to Data portability. The concern here was that there are gender references one part of the Bill deals with "his", some say "hers" *et cetera*. For consistency certainly, we agree that it is proper form and we will seek to have that consistency throughout the Bill. So can we move on now to Section 22, to which this reference is made. It is suggesting that we try to define adequate, and appropriate safeguards as it relates to section 22, which says that Personal Data should not be transferred to a Country or territory outside of Barbados unless that Country or territory provides for an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data and appropriate safeguards. On condition that the rights of the data subject are enforceable and there are

available effective legal remedies for data subjects. It asking that we further define adequate and appropriate safeguards *et cetera*. It further suggest that it should be a list. Well, let us deal with that one first before we go on to the next one. Is there some concern here, any comment from the Committee?

Senator R. J. H. ADAMS: Madam Chairman, I guess I have comment. I understand the desire to make everything schematic and box ticking. Did I do this, and did I do that. I cannot help thinking that context is always going to defeat that approach and you have to leave something for if it goes before a Judge for them to interpret. I have some sympathy for this, but I just cannot see it working... the maintenance of a list. We know all about blacklist, and grey list. I am not sure that is a business that I want us to get into just from the maintenance point of view. I think, I would rather we spoke about the, and I am not sure I am making an appropriate, we spoke about the confidence of judges and so on. I think we have to rely on their confidence in this one to define what is adequate and so on and so forth.

MADAM CHAIRMAN: I would certainly agree that for us to start putting Countries on negative list and positive list as this recommended will really create a level of activity on the part of Government that could certainly not be something that we can handle. Plus it is impractical because the list would have, if we put this in the legislation, the list would have to be changing constantly and we would have to bring some kind of legislation by order or some other form. Each time that it has to be changed. I am not sure that currently this is something we want to impose on our system as it is. Therefore, I would say with regards to section 22, it seems that there is consensus around the table that it does not have an impact on the Bill as drafted. Is that correct? Agreed.

Section 50(4), page 59. A person who operates as a Data Controller without being registered will receive a fine. The question raised here is that Data Controller is anyone who is responsible for processing data, which can include every employer, and this needs clarification. I am going to ask Miss Belle, to speak to this matter with regards to any confusion.

Miss SHAWN BELLE: In terms of clarification, the sure answer is that it will apply to legal and natural persons. So, yes it could apply to every employer. In relation to an educational institution, usually there are run by boards, and that would be the legal entity then that would be liable. So it does not need clarification, when you use a person it applies to the natural or to the legal person.

MADAM CHAIRMAN: Now that there is that simple clarification it is an inclusive Bill, so all are included here. Section 55(1). A person shall not operate as a Data Processor unless he is registered in the register of Data Processors, and the point here I make is if there is no separate Registration Act for the new profession should it then be included in the Profession Trade and Business Registration. I believe Miss Belle, spoke to that a little bit earlier, and the reality is that a

new profession is not being created that is not the intention of this Bill. I would let Miss Belle provide a further perspective on that.

Miss SHAWN BELLE: Madam Chairman, yes, just to explain. This is not a new profession in the lane of, oh this is regulating lawyers, and this is regulating accountants. The nature of your activities will dictate whether you are a processor or whether you are a controller. Your registration requirements that come out from that. So that is why then you would only require to register under this Bill. There would be no need to refer or go under the Profession Trade and Business Registration Act.

Senator Miss C. N. DRAKES: Madam Chairman, just thinking this through a bit more as well. We stated earlier that a Data Controller can also be a Data Processor, and a Data Controller needs to be registered. Given that, that may be onerous on businesses, we also spoke about having the possibility of that being outsourced. If that is outsourced from a business what mechanism do we have in place then and this is just thinking it through, because of the conversations that we have had. How does a company then make itself compliant if it outsourced the services of the Data Controllers and the Data Processor?

Miss SHAWN BELLE: Madam Chairman, what would happen is most entities are most likely going to be Data Controllers. The question is whether they are also Data Processors, and the decision to outsource may be there. They may also have to go through the debate as to whether they would register as Data Processors although what I would argue is that there are core activities would suggest where the meaning lies. So that if you are for the most part doing what would be considered the functions of the data controller, you register as a controller particularly, because the Data Controller has responsibilities over the Data Processor. That is how I would, and that is applying a purposive approach to interpretation to make things function. Sometimes everything cannot be put in legislation in terms of how things work, but you cannot interpret the legislation to render it absurd.

Senator Ms. A. M. WIGGINS: Madam Chairman, my concern here in terms what he has if there is no separate legislation then it should be included in the Professions Act. I think again because we are dealing with a small society like Barbados that we must consider the additional persons who will now have our confidential information, and there must be some way of policing them, and I think he is suggesting here that they should be registered because if they are registered [then] they [would] have a higher obligation to be confidential.

Miss SHAWN BELLE: Madam Chair, through you, just to say that [the] profession, trade and business registration is targeted to regulate professions, basically lawyers, doctors and the like. This is not creating a profession, this is basically identifying what this company does and then if you do that activity, then you should be registered as a data controller or a data processor, whatever is applicable to you, and the

registration regime would already control what is required.... Well, okay, I am rambling, sorry.

Senator Miss C. N. DRAKES: Madam Chair, I understand what Mrs. Belle is saying, in terms of not creating a new profession but I am speaking to the very critical issue of accountability.

Miss SHAWN BELLE: Madam Chair, again, the application for registration goes to the Data Protection Commissioner, so [that] the Data Protection Commissioner is going to be the person who has responsibility for maintaining the register and for dealing with the applications, so [that] he is the regulator.

MADAM CHAIRMAN: The question is, can a person, whether legal or human, register as both processor and controller or would they have to choose one?

Miss SHAWN BELLE: It is possible that they may have to do both if they are doing two functions, but I would say that you would lean to the core activities that you are performing and that that informs how you register.

Senator Miss C. N. DRAKES: Madam Chair, so [that] I can recap and make sure I am clear, if my core, let us say for instance, a doctor – bad example – and I outsourced the information to a data controller who is registered, what would happen is [that] the doctor, by virtue of his job, in collecting the information is a controller, because he then organises and distributes that process. He might outsource, which means that he would be outsourcing the processing issue, [would also mean] that processor needs to be regulated.

Miss SHAWN BELLE: Okay.

Senator Miss C. N. DRAKES: Madam Chair, if I can continue to seek clarity, if that doctor outsources that service and the information is then breached, who is responsible?

Miss SHAWN BELLE: The data processor, if you have me having that arrangement, the data processor is accountable to the data controller under the provisions of the Act, so you cannot process without the data controller, meaning the doctor's authorisation and the doctor then, as the data controller, if there was a breach under the Act, the doctor has the responsibility to report it to the Data Commissioner and the Data Subject, particularly where it is infringing that person's rights and there has to be time limits within which to report.

Senator Miss C. N. DRAKES: Thank you, Chair, this is an extremely insightful exercise.

MADAM CHAIRMAN: [Let us] remember that the data controller is responsible, [he is the person] who has the authority to tell you what is the purpose for which your data will be used later on, but then the data processor is the one [who is] doing the manipulation of it, whether it is distributing, et cetera, so [that] you have to separate the data controller who is focused on the purpose, from the data processor who then has control over actually manipulating and using that data. Does that clarify it now, in that regard?

Senator Miss C. N. DRAKES: Yes, Chair.

MADAM CHAIRMAN: If we are to move along from 55(1) with the conclusions we have come to, it then makes the section 55(4) the concern that is at the bottom of page 2. It just makes that null and void because they are not creating professions, therefore, that one is not relevant. Again, we are at the top of page 3, section 68(3) and (4). Where the concession is that there appears to make the Data Privacy Officer the Commissioner's spy, but paid for and maintained by a company. No, this is not the case, the Data Controller designates their own privacy officers and it is to facilitate core operation in the Data Subject's interest, so that, for example, the Privacy Officer is working for the Data Controller but in the interest of the data subject, so [that] the Privacy Officer is really there to take care of the Data Subject's privacy interest, and also they work with the data controller because they are making sure that the data controller's interests are served by complying, so [that] you have to distinguish between the data controller, the data privacy officer and the data processor, so [that] the data controller deals with purpose; the data processor is dealing with the manipulation of information, and the data privacy officer is there to make sure that the data subject's rights are served and to make sure that there is compliance with the Act. Does that now make sense to everyone?

(The Committee responded in the affirmative)

MADAM CHAIRMAN: That said, therefore, section 68(3) the comment made there does not have an impact on the Bill. Is that the understanding of the entire Committee?

Senator R. J. H. ADAMS: Madam Chair, that is my understanding but I do not know if that is helpful but when we wrote back and explained our reasoning to each submission, it struck me [from] reading this that there is a parallel to a compliance officer running KYC AML in a business and the data privacy officer is fairly strong parallel to that norm. I know when you give people these kinds of analogies that they immediately start to open a can of worms and so on but that is the way I set it up in my mind. I know I do not want to drag this out but that does seem to be fairly fair and it might be something that people can more easily grasp when we give them the explanation.

MADAM CHAIRMAN: Thank you. Now we move to section 73(1), that again is the section just below the middle of page 3. The contention here is that the last sentence appears to be glaring loopholes for mischief. If the Commissioner instructs his employees to release someone's personal information to one of their competitors, then, while it is clearly unethical, this clause appears to make it legal, and it is the clause they are referring to above, which I believe all of you [would] have read. I am going to ask Ms. Belle to speak to this matter.

Miss SHAWN BELLE: Madam Chair, this particular provision is very common when you are

dealing with functionaries, to impose upon them a specific obligation to keep things confidential, but you give them some leeway in relation to circumstances where they may have to, in this case, release information. Now, that is not to say that you interpret it to mean, and a court would see it this way, that he can do anything. He has to have in his mind the Bill itself and also other enactments, as well as any common law jurisprudence that has developed on the matter, as well as any customs and practice that may be relevant. It is not that the discretion is unfettered, he has to take all of those things into account and if he does not he can be challenged and disciplined under the Public Service Act because he is a public officer. I just wanted to make that point.

MADAM CHAIRMAN: With that said can we therefore, agree that this Section 73.1 as presented in this submission would have no impact on the Bill as drafted currently. That is agreed? Okay agreed.

Section 73.3, it speaks to, "A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or imprisonment for a term of 12 months, or to both." What is being suggested here is that there will be a minimum fine of \$500 000.00 submitted for this. I believe that this was discussed earlier and the fact that the law really and truly does not allow us to do a minimum penalty on anything and therefore this recommendation would not have an impact on the Bill if the Committee is an agreement with that. Agreed.

Now we are at Section 74, "The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act." Now again the suggestion here is that this seems to be an excuse for professional negligence and my perspective is certainly the idea of in good faith that that is the measuring stick and where that officer would act outside of good faith then they would be subject again as Ms. Belle said earlier to the Public Service Act as a public servant. Therefore I would say that this submission regarding Section 74 should not have an impact on the Bill as drafted. What says the Committee?

Senator Ms. A. M. WIGGINS: The only thing I would say there is what Senator Adams spoke of earlier serial offenders. What then would be the penalty if the person can be suspended or something of that matter? He wants to say that these persons should not be penalised because they are doing their job in faith, but sometimes people's information can fall off the back of a truck and as he said earlier a serial offender. I do not think you should give just like that, it should be built in mechanisms to protect people's data.

Senator R. J. H. ADAMS: Madam Chair I was just going to say in contrast to my prior comment about blunt instruments and scalpels, this seems to be a

processed question, and I am just wondering what is the legal test for good faith. I guess I am asking would a judge for example not look back and say did this person follow the process. Is that the test or does it have a special definition in the eyes of the law?

Miss SHAWN BELLE: Madam Chair, just to say that this is a common provision again that is put in place in terms of functionaries, because sometimes it is anticipated that functionaries can make errors, but they are acting in good faith and the good faith meaning they were following the proper procedure, they were following the Act as set out, they were following all of the relevant rules that pertain to the execution of their job, and so the Judge then would look at those factors to determine whether they are acting in good faith should it come before a Court. In terms of the Public Service Act, though, there are several mechanisms for disciplining a civil servant. Now the vernacular, I might be getting wrong, but there is the concept of like a lesser type of infraction versus a more serious type of infraction and the lesser types of infractions may attract a reprimand or whereas a more serious may go to the point of even rendering the person to have to be dismissed. There are a gam..... or toolbox of ways in which the Commissioner can be disciplined.

MADAM CHAIRMAN: Anything further on this item? Does that answer the question? Then again it appears then that Section 74 as we have just explained it should have no further impact on the Bill as drafted. Is that correct Committee?

Section 75.(1). *"The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct."*

MADAM CHAIRMAN: The question raised here is there a penalty for not submitting that report. I believe that was just answered. The Commissioner would be subject to the Public Service Act with regard to not executing their duties, and that then would apply in this situation and therefore this suggestion would have no further impact on the Bill. Is that correct Committee? We are in agreement.

With regards to Section 79.(1) and Section 85.(2). These are typos, and as we said typos happen and they will be fixed in the final Bill. It also speaks to copies of documents, sorry, that is Section 79.(1) in particular. Section 85.(2) however, speaks to copies of documents may be seized but the person should be allowed to make copies of materials seized is unrelated to the charge and as part of this business. Now, this is taken in the context of a warrant having been issued by a Judge, and I will let Ms. Belle speak to that, but if a warrant has been issued by a Judge, this idea that you get to take back things and photocopy them is not something that we would wish to do at this stage or at any stage.

Miss SHAWN BELLE: Madam Chair, the thing is that context matters, so the power to inspect and seize is within the context of a warrant. A warrant is a

special document, you have to go before a Judge and you have to lay out a compelling case for him to sit down and it allows the Commissioner or his staff and Police to come to the premises to search, to seize, and inspect the different part. Those are things that ordinarily would not be allowed to do, and so the copying of documents, I understand that maybe it is that there was a thought that maybe you need to retain something. But the fact of the matter is for it to get to that stage, this would have been a very serious infraction in terms of not cooperating with the investigative functions of the Commissioner. Note also that the Commissioner has within their toolbox the capacity to issue an information notice if it is that they need information. The thing is then at that point the person would not be in cooperation and that is why the Commissioner would then resort to seeking a warrant from the Judge. I just wanted to say that.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, while that is so, for it to reach a stage where a warrant has to be issued, the person would have to be not complying. I think the issue being raised here, is that the documents unnecessary for the continued function of the business or they are holding information belonging to a different...

Miss SHAWN BELLE: ... Madam Chair, again this is a lack of knowledge of how warrants function. When you go before the judge, you cannot be asking for information that is not related. It is going to be very specific as to what you are looking for and why, so this concept that you would be seizing just any material; no, that is not the case. You have to understand how warrants work.

Asides.

Miss SHAWN BELLE: They would be looking for specific materials and the parameters would be carefully set out in the warrant.

MADAM CHAIRMAN: Given that education on the way warrants work and the fact that this may not necessarily be a major concern, before I continue let me give Senator Drakes the Floor before I wrap up, because it seems that you have a comment to make.

Senator Miss C. N. DRAKES: No, Madam Chair. I understand the concern which the submission has and I am wondering what the precedence is in terms of warrants period. I do not know if a lawyer in the room such as Senator Sands can explain. What is the precedence as it relates to warrants? What can and cannot be taken, and would that then speak directly to this section of the Bill?

Senator D. R. SANDS: Miss Belle actually spoke to it. All a warrant does is specify what the actual officer or commission is looking for, so in a practical sense let us base it on what this gentleman has put in the submission. If the person had all of their information on one sheet of paper, and I want information at Line 7 but all of my information is on this one sheet of paper, then we have a practical issue here which we have to deal

with. I cannot cut out the middle part and leave the balance; I want the document as a whole, so in a situation like that which is peculiar then we may find ourselves in an area of some confusion. However, in the normal course of things if it is File A or File B or File C, the officer would have a warrant speaking to the specific file which he or she is seeking to seize or inspect.

Senator Miss C. N. DRAKES: Madam Chairman, on that note what we are primarily talking about is soft copy. With soft copy you just need access, a password, where you then more than likely have access to all of the information. We are thinking of it in a very physical sense but given you were talking about data, if you need to seize information from my laptop, I have to give you the password to my laptop which then gives you access to all of my information. How does the warrant then apply?

Miss SHAWN BELLE: That is so extreme. A judge will not sit down and fling them like candy like that. You have to establish a case.

Asides.

Miss SHAWN BELLE: And there is an understanding of the fact that you are dealing with electronic information. Okay? This Clause comes from the United Kingdom, the Cayman Islands and those, so there is an understanding that it is electronic information but I just need to stress again: Extreme. Right? So a judge in order to give that type of an order would have to be persuaded by counsel or the Commissioner that there really is a case and there is really an infraction. Also, part of the warrant is almost like an injunction. You would have to say there is an urgency because the person might spirit away the evidence, so there is an urgency attached to that too. I just need to emphasise those points.

Senator Miss C. N. DRAKES: Madam Chair, thank you. I think Miss Belle is giving me more faith in the justice system.

Asides.

Senator Ms. A. M. WIGGINS: Madam Chair, can I say something possibly off the record?

MADAM CHAIRMAN: On the record for Hansard at this point in time.

Senator Ms. A. M. WIGGINS: I was just saying that she spoke to electronic issues, and everyone knows....

MADAM CHAIRMAN: If you want this to be off the record, then turn off your microphone.

Asides.

MADAM CHAIRMAN: That was Section 85.2. Given the extensive discussion and explanation we have had with regard to how warrants really work, do we see this Section having any impact on the Bill as it is drafted currently?

Asides.

MADAM CHAIRMAN: I believe that answer is "no", therefore we move on to Section 85.3, where it reads:

"A judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism, or for artistic or literary purposes unless the determination by the Commissioner has taken effect."

The question here is: What about educational institutions processing student records? Would they fall under that? I am again going to ask Miss Belle to speak to that.

Miss SHAWN BELLE: Madam Chair, it would not apply to educational purposes but just to say that Section 81 deals with the determination of the Commissioner as for the purposes of journalism or artistic or literary purposes. That exception – remember it is under an exception – is the one that is one that is going to cause the greatest challenge because persons are going to want to use the information for those purposes and you may need to drill down to make sure that they really fall within the exception. In short, it does not deal with the educational institutions and I would have to say that there would have to a directive to say that or a reason why you should also cover processing of student records. I do not recall it being something that other legislation dealt with.

MADAM CHAIRMAN: Any further questions on this? It seems as if it would not in any way substantively change the Bill as it is drafted currently. Is that the concurrence of the Committee?

Senator Miss C. N. DRAKES: Madam Chairman, if it was not under this Bill and this same scenario applied, would they be guilty of an obstruction?

MADAM CHAIRMAN: Yes.

Senator Miss C. N. DRAKES: Therefore, I think we can readily move on at your discretion, Madam Chairman.

Senator R. J. H. ADAMS: No dissenting voice, but I wonder again and I think about the response that we offer to these submissions and this just seems to be one where we say, we may say, we can revisit these levels of trying. If there are not deterrents then we will go back and look at it again but at this stage, why would \$500 000 be more of a deterrent than \$100 000, that part is not clear to me. It is a comment and I think we should respond carefully, except to that one about the ladder when we do reply.

MADAM CHAIRMAN: There are submissions, as we have been told - my apology, my microphone was not on – that we are expecting from the Bar Association and perhaps Barbados Association of Medical Practitioners (BAMP). I believe BAMP has already come and also the Bankers' Association and they are already here. I believe the Parliamentary team will send that out to us tonight as we would have agreed in procedure on Monday. We will reveal those on Monday and I would propose that we reconvene on Monday at 11:00 a.m. as opposed to 10:00 a.m. and at that time, whatever submissions would have been

received from all of the above, and I believe tomorrow is their deadline, again if I may repeat, then they will send it to us electronically. We can then review those on Monday and then prepare for the final report after that.

MADAM CHAIRMAN: Committee, thank you for your indulgence. I was having a conversation with regards to the submissions that have already been received. I believe the Bankers' Association have already submitted. The Parliamentary team will make a request of the others. Would they wish only to make a written submission or would they wish to make an oral submission on Monday as well. The Parliamentary team will get back to us because we are fine with a written and some may be open to also making an oral submission. If that is satisfactory to the Committee we will leave that option also for oral presentations on Monday.

Miss SHAWN BELLE: Madam Chairman. I am partial to just considering the written submissions. Remember that Chief Parliamentary Counsel if there are things that we have to follow up on, we have to do the work and if I am here, then it will be a problem.

MADAM CHAIRMAN: What is the word of the Committee? Please, everyone, make your voice heard.

Senator Miss C. N. DRAKES: Madam Chairman, I would also like to second that because, I think, even though given the experience this morning with the oral submissions, for instance, Mr. Morgan, he had some very good points, however, a written submission would have been better to sit down and analyse. If any amendments needed to be made there is a document you can refer to and if you are serious about the submission and if you are serious about any amendments that needed to be made to the legislation, I would rather us request written submissions.

MADAM CHAIRMAN: Are there any other voices? I really want to hear the other voices on the Committee.

Senator K. J. BOYCE: Madam Chairman, I would request the written submission.

Senator D. R. SANDS: I agree with both of my colleagues, I would require the written submission as well, Madam Chairman.

Senator Ms. A. M. WIGGINS: Madam Chairman, with great respect. Unless the Ministers have House of Assembly on Tuesday, I was just wondering if we could defer the Monday's session until Tuesday.

MADAM CHAIRMAN: There are other things on our schedules other than that and for me in particular I know that there is a major project that I have to work on that day.

Hon. Ms. C. S. V. HUSBANDS: Madam Chairman, I take the point that you need a written submission because when the person gets up and leaves, you want to have the information set out. My only thing, I did not hear a lot of it. All of you had the experience so you can say but I was wondering if it was not helpful having the person explain more of what they

meant because sometimes you may read something and you think of it in a particular way but when the person explains you get an understanding of what they are trying to get at but still have it in written so you can refer.

MADAM CHAIRMAN: There is one person for oral and written.

Senator R. J. H. ADAMS: Thank you, Madam Chairman, I am glad I got to speak last. I needed time to think about it. I think where if we know a submission is going to be a little contentious, for example, that Solutions Barbados submission, if Mr. Phillips was here and could explain...

Asides.

Senator R. J. H. ADAMS: I do not know Mr. Phillips but, for example, on the fines where a lot of misinterpretation has gone on, and we set out that no, actually that is not the way it works, I think we shut down the wrong expression, we satisfy the inquiry. I am tended to say that if it is contentious it is nice to give the person a chance to hear us out but it is not very good use of time overall. I mean if they do put in a written submission, I will hear you but I think they should express themselves pretty clearly and we can give them a response and if they want to come back again and open that up with a different question I guess we could respond again but that takes a certain amount of effort on their part that should focus their mind on getting it right the first time, so I think on balance I would go for the written.

MADAM CHAIRMAN: Okay. I as Chair certainly am open to written so I believe that the Committee... all except one is...

Senator Miss C. N. DRAKES: Madam Chairman, if we can have a middle ground, is there any way they can provide the written submission and there is an invitation update if they want to come and sit in on the closed session, is that allowed?

Miss SHAWN BELLE: Madam Chairman, I get it, you want to give people as much opportunity to express themselves but it was advertised several times on the radio and if you have a material in chest you would be here, and that is my view. The Chief Parliamentary Counsel wants to be cooperative but I am one person and I have to go back and analyse all of the information that I have received. Yes, you all have worked with me before with Public Finance Management Bill and it was like, *snap, snap, snap*, but I am one person.

Senator Miss C. N. DRAKES: Madam Chairman, if I could.

MADAM CHAIRMAN: I beg the Committee's indulgence for one second please, I am just getting a clarification on process. Okay, in terms of seeing how we might be able to have a middle ground, one consideration is that when we have the written submission for Monday, we go through that submission as a Committee and if in going through the submission we discovered that there are some things that we

definitely need to invite the submitters for, then we would have to consider how we might be able to do that. Would that work better for the team in terms of a middle ground?

The Committee in unison answered yes.

MADAM CHAIRMAN: Well, I think if I am to go the democratic route the majority has said let us take a written submission and only if there is need for us then to invite the persons or organisations making the submission, that we do that only then off record. I think the Committee has made its decision and the collective responsibility of all of us to say we are in. That said, is there anything further before we conclude?

Senator Miss A. M. WIGGINS: I would like to put forward a motion for this session to be adjourned and to compliment you, Madam Chairman, on your excellent chairmanship. I will also say, and it happens within the Senate when you are leading as well, that you always sum up so concise and so perfect. You summarise what people say very well. Can I say I admire you for that, and that is my motion?

Senator Miss C. N. DRAKES: Madam Chairman, I would like to say I second that motion.

THE AUDIO FEED ENDED AT THIS TIME AND THE MEETING WAS SUBSEQUENTLY ADJOURNED TO JULY 01, 2019 AT 11:00 A.M.

ENDS TRANSCRIPT OF THE SECOND MEETING OF THE JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, HELD ON JUNE 26, 2019, IN THE SENATE CHAMBER.

**SECOND MEETING
OF THE
JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, 2018
HELD IN
THE HONOURABLE THE SENATE**

WEDNESDAY, JUNE 26, 2019

First SESSION 2018-2023

PRESENT:

Senator the Hon Miss K. S. McCONNERY
(Madam Chairman)
Hon. D. D. MARSHALL, Q.C., M.P.
Bishop the Hon. J. J. S. ATHERLEY, M.P. (Leader of
the Opposition)
Hon. Ms. C. S. V. HUSBANDS
Hon. D. G. SUTHERLAND, M.P.
Senator R. J. H. ADAMS
Senator Miss A. M. WIGGINS
Senator K. J. BOYCE
Senator Miss C. N. DRAKES
Senator D. R. SANDS

Also in Attendance:

Miss SHAWN BELLE *(Senior Parliamentary Counsel,
Office of the Chief Parliamentary Counsel)*
Mr. CHESTERFIELD COPPIN *(E-Commerce
Development Officer, Ministry of Small Business,
Entrepreneurship and Commerce)*
CLERK OF PARLIAMENT Mr. Pedro E. Eastmond
DEPUTY CLERK Mr. Nigel R. Jones
DEPUTY CLERK Miss Beverley S. Gibbons
Miss Suzanne Hamblin, (LIBRARY ASSISTANT)
PROCEDURAL OFFICER TO THE COMMITTEE
(Ag.)

ABSENT WERE

Mr. N. G. H. ROWE, M.P.

CALL TO ORDER/WELCOME

The Chairman called the meeting to order at 10:32 a.m. and welcomed those present.

MADAM CHAIRMAN: Recognising that there are five members of the Committee here which, according to procedures established in our first meeting, constitutes a quorum, we will get started with the quorum that is here currently. For all of those members who were unable to make it to the first meeting we want to welcome you to this meeting. Thank you very much for coming.

In moving to the second item on the Agenda which is the Minutes, I would like to invite a motion for the deferral of those Minutes given that we would have met only Monday and they are not yet quite prepared.

On the motion of Senator K. J. BOYCE, seconded by Senator Miss C. N. DRAKES, the Minutes of the last meeting were deferred.

MADAM CHAIRMAN: Thank you. The third item on the Agenda is Matters Arising from the Minutes. I would propose that there are no matters arising as we have deferred those Minutes.

The fourth item on the Agenda is Oral Submissions. For those members who were not present, we had established in procedures at our first meeting with regards to oral presentations that persons who had expressed an interest in presenting to us today orally. There were presentations that were written and some were oral. There were five requests for oral presentations for today. We had received notice that one of those persons will not be here and so we can expect four oral presentations so far based on the information we have to-date.

What we agreed on in the procedures on Monday at our first meeting is that each person would have the opportunity to present for about 10 minutes and then there will be 15 – 20 minutes of questions and answers that we can pose as a Committee and altogether no more than half an hour and we can show some flexibility given reason in that regard. We had also asked that Mr. Chesterfield Coppin, who would not have been named properly on the Committee would serve as a resource person, as he would have been the officer that was most intensely involved in the consultations with stakeholders in bringing this Bill to the next level and so I would ask the permission of the Committee to permit Mr. Chesterfield Coppin to sit as a technical resource as part of this Committee today. Are there any objections?

The Committee answered with a unanimous no.

MADAM CHAIRMAN: With that said, I think we have been able to move with dispatch to the submissions based on the speed with which we get through these submissions today, the thinking, again according to procedure we agreed, is that we would have heard the oral presentations in the morning, then we would break for lunch, and then after we would go through the written presentations with the intention by the end of the day of determining how those

submissions would or might impact the Bill and what adjustments, if any, would need to be made as required. Are there any other thoughts? Yes, Sir.

Bishop J. J. S. ATHERLEY: Madam Chairman, what time are we going to today?

MADAM CHAIRMAN: It depends on how fast we get through the presentations. Some presentations may take the full ten minutes, but the intention is to cover all today. Just let me use this opportunity to give notice too that following the request that was made for some groups to be reached out to directly that the Clerk of Parliament and the team did indeed reach out to those groups and we are now understanding that they maybe two additional submissions. So far, we have been notified that the Bar Association would also wish to make a submission as well as the Barbados Bankers' Association Inc.

According to the procedures which we established on Monday, we said that we would extend that deadline until Thursday, meaning tomorrow, for those submissions and then we will seek to hear those submissions if there is a request for oral presentations on Monday. If there is no request for oral presentations, we will then consider the written presentations on that day. Anything further?

Without further ado, I would recommend that we now go to the consideration of oral submissions. What we will do for ease, with your permission, of course, is to invite all of the presenters in and simply call them one at a time so that they can see the presentations of the others.

At 10:37 a.m., the presenters were ushered into the Senate Chamber to commence oral submissions.

Hon. D. G. SUTHERLAND joined the meeting at 10:38 a.m.

MADAM CHAIRMAN: I wish to acknowledge the presence of those persons and organisations that have requested to make an oral presentation before this Joint Select Committee. We will simply call you in the order in which your submissions were received and what we will ask is that, as you are called, you take your seat directly opposite, ensure that the green light is on so that we can hear your presentation. It will be a presentation from sitting. You have 10 minutes to make your presentation with about a 15 to 20 minutes for questions and comments from the Joint Select Committee. We want you to be aware that your presentation is being streamed live and you may begin when you are ready.

The very first person we would wish to call is Miss Cynthia Wiggins. When you come, kindly identify yourself and the organisation, if one, you are representing.

Miss Cynthia WIGGINS: Good morning. My name is Cynthia Wiggins. I am here as a user of data, an individual and a small business owner as well. May I begin?

I would first like to thank Madam Chairman and the members of the Joint Select Committee for

allowing the public to provide submissions on the Data Protection Bill, 2019.

Secondly, although I believe the Bill is an important one, I also believe that the amendments may be necessary to ensure that it facilitates:

1. The provision of a framework that allows companies to have the flexibility to target individuals, gain a competitive advantage through the utilisation of data and data analysis while ensuring the privacy of individuals.
2. Consideration of the new methods in which data can be captured, generated and analysed. For example, through retail transactions, online methods, block chain, *et cetera*.
3. Viewing the protection of data more so from the standpoint of the data use itself, than from the classification of the activities and the tasks in the data process.

For conciseness and clarity in the preceding paragraphs or discussion, my submission points will be addressed under six main headings with either page or section references where required. The main headings are as follows: Data and Data Element; Content; Privacy and Security; Monitoring and Compliance; Costs; and Others where I believe the points were important but did not fit under any of the above.

In relation to Data and Data Element, I believe the Bill in most instances does not seem to take into consideration the nuances of online and transactional data or the issues that would accompany such data types. For example, on Page 12, Accessible Records: I believe online transactions records do not technically fall within any of the record types listed. On Page 16, Sensitive Personal Data or Data in Page 13 does speak to photographs, videos, comments, *et cetera* that does not include personal purchasing information. Page 79 (r) does not include transactional or online data. Page 18, 4(1)(c) would limit social media or other business ability to utilise data as part of their competitive advantage.

On Page 25 (1), the point speaks to deceiving or misleading of individuals, however, businesses often collect data for purposes other than what they are proposed and change the reasons that they are collecting the data. For example, on Facebook you are connecting with your friends but, however, they actually analyse the data to advertise and gain revenue, *et cetera*. It is not necessarily for malicious reasons, it is just the nature of the business.

2. Under the same heading, online data by its very nature may be onerous to describe making the registration requirement on Page 60, 51 (2)(1)(c) difficult to comply with. For example, meta data, time stamps, information, location, landing pages, *et cetera* in general will be difficult to describe but may be captured for analysis reasons. Additionally, data captured requirements may change to assist with online visitors analysis as the need arise which would potentially hinder the innovation of a business if notification regarding the description is required.
3. In the normal course of business, data can be

collected and used for profit or as a tool to gain a competitive advantage, so consideration would have to be given to the following points: Page 25 (e), (i), (a), data can be collected for profit in relation to social media; Page 33, 18 (1)(4) could limit an organisation's use of data modelling, algorithm and profiling which may be how the company ensures its competitive advantage, for example, Social Media, Facebook, Instagram *et cetera*; Page 27 (10)(1) to provide the logic for profiling methods could impact on the company's competitive advantage. I do not see a reference to the sales and transaction or other data regarding the sale of actually companies. So whether or not when you sell a company it is the data that refers and relates to individuals may become part of the sale. Is that fine? Or do they need to actually inform the Commissioner?

The definition of direct marketing on Page 33 (3) does not seem to take into consideration telemarketing or online marketing since there are no restrictions specific to telemarketing or content marketing within the points on direct marketing. For example, where the company may initially call... I have had this where I would have gotten a call from one of the telecommunications companies under the pretence that they were informing me of a service problem and they started to upsell. That sometimes happened. I have had numerous calls at 7:30 in the night which I complained about and told them to place me on a do not call list, but there are loopholes within our legislation yes that allows for such things so it becomes difficult for an individual to actually say that this is a problem. Where individuals may be targeting within the content that does not seem as though it is an advertisement, so we often get things that are not classified as advertisements and it may just seem as though it is a normal conversation for BuzzFeed or YouTube funny videos but really and truly it is an advertisement. So how do we classify those things and what do we do about those things?

Although part of the general data protection regulations for small business, it seems as though the financial requirement would be a little bit onerous for small businesses to have data privacy officer (Pages 74, 75 and 76) and will hinder small businesses seeking to utilise data as a competitive advantage.

Just a note, I believe that we do not use data as much as we can or should as a competitive advantage. There are bigger businesses that are trying to seek to do that. Telecommunications companies tend to do that. Financial companies although they have the data do not use it as much, but they more than likely should.

Consent: Number 1- There is the need to specify in the Bill that consent needs to be explicitly given by opting in for utilising transfer or processing of the data therefore consideration would have to be given to certain points.

MADAM CHAIRMAN: Miss Wiggins, you do have two more minutes.

Miss. C. WIGGINS: Yes, that is fine. For utilising transfer or utilising of data, therefore

consideration would have to be given to certain points.

The Bill should seek to specify that individuals must notify on accidental disclosure, disruption or breaches which I do not think is currently there. Where an individual is no longer a user or a customer they should be able to ask for the removal of the data providing that it is not historical records or there is no legal ramifications.

Under Monitoring and Compliance, in the Bill, although there is no obligation to comply, there are loopholes which would allow individuals to circumvent the requirements. There is a need to specify time frame or frequency in which some of the activities should occur, Page 77 and 79.

I want to speak a little bit with the last minutes that I probably have with the cost issues which I think would come up for a lot of business owners. If there is a cost associated either legal administrative or otherwise with individuals requesting information or trying to ensure compliance via the tribunal or a quote, it may become a deterrent for individuals. For example, on Page 28 (3), I am not sure a data subject should be made to pay a fee in retrieving information that the data collector should have as part of their general service and their general operational costs. For example, you go to a bank and you want something printed from your account they are pressing print and that is about it and you are charged \$5.00.

I can see that being a loophole for persons to place cost to things that they do not need to place cost to.

Other issues, page 10. Financial Institutions may not fall under credit referencing agency according to the definition, but they also have information regarding credit standing. I will take for example, The Student Revolving Loan Fund that has on a number of occasions send information to your sureties only informing you that they will send information to your sureties, but they actually would have provided your sureties with your financial standing, technically. I see that as an issue. I am not sure of the minutes I have, if I have any more minutes, but I will stop here. I can always provide a written document as well.

MADAM CHAIRMAN: Thank you very much, Miss Wiggins. We really would have appreciated having at least the written document ahead, because it would have meant we could follow you more closely.

Senator Ms. A. M. WIGGINS: Yes.

MADAM CHAIRMAN: So thank you very much. I think that was very comprehensive as you touched on a number of the areas, which you thought you saw some loopholes there that you thought should be addressed, and that you saw some cost issues. You also need some clarification on definitions and a number of other important contributions that you made there.

Are there any questions from the committee at this point in time?

Senator Ms. A. M. WIGGINS: Or comments?

MADAM CHAIRMAN: Or comments?

BISHOP J. J. S. ATHERLEY: Madam Chairman, thank you, and thank you for your presentation, Miss Wiggins. I really would love to get a copy....

Miss. C. WIGGINS: Yes that is fine. Time constraints. I would not want something that I have not proofed properly out there. It is just a time constraint issue. Yeah, that is fine. I will send it.

Senator Miss C. N. DRAKES: Madam Chairman, just one question for Miss Wiggins. Thank you very much for your presentation. You noted that you are a small business owner without giving the name of your business, but could you tell us the type of business you own?

Miss C. WIGGINS: I am in content marketing and social media advertisement, *et cetera*.

Senator Miss C. N. DRAKES: Thank you.

Miss C. WIGGINS: Yes, you are welcome.

MADAM CHAIRMAN: Thank you very much. We would simply ask that electronically, you submit your presentation to the Clerk of Parliament as you would have your initial.

Miss C. WIGGINS: Yes, sure.

MADAM CHAIRMAN: I would like now to call. Mr. S Antonio Hollingsworth, to present to the Joint Select Committee. Identify yourself, and who you are representing, and then please continue as soon as you are ready.

Mr. S. ANTONIO HOLLINGSWORTH: Good morning Madam Chairman, Members of the Joint Select Committee. First of all, my name is S Antonio Hollingsworth. I represent myself personally, and I am the founder of Bajan Digital Creation Inc. We are a company that deals with conversational artificial intelligence and virtual reality content. I believe that you have received a copy of my written submission?

MADAM CHAIRMAN: Yes, we did.

Mr. S. ANTONIO HOLLINGSWORTH: Right. What I am about to say is to put everything that I would have written in context. This is a story of a Bajan who returned home to heal, his hands trembling, and his body ill. A shell of a man who left Barbados thirteen years ago. This Bajan returned at a time where jobs were scarce, and his thirteen years of educational experience in Mathematics meant little. He had to survive, so this industrious Bajan like every other proud Bajan used what he had to do and what had to be done. He used his skill set, will power, sweat and tears to build a business from a piece of drift wood to a digital entity with global reach in less than a year, bootstrapped. No loan because he had nothing, no political affiliation, he is the average Bajan from a working class family who lives by modest means in a Christ Church village. He was willing to work hard and build in a time when building was difficult and resources extremely scarce.

That story is familiar to most small to medium enterprises that would be affected by this current version of the Bill, they need to survive. The artist selling her art online, she needed to survive. The taxi driver hustling to collect one of his clients who called,

he needed to survive. The homeowner who runs an Airbnb to make extra, she needed to survive. The 60 plus year old seamstress who collects measurements on persons, she needed to survive. The start-ups that are still in gestation, they need to survive. These may not have the resources for another specialist employee called a Data Privacy Officer. They may not have the time or resources to go through a certification or registration process. It is already difficult enough to start or do business in Barbados, and this Bill in its current form makes it harder for small to medium enterprises to be profitable when money is scarce. Worse yet, under this Bill to take a chance with noncompliance is not only the end of whatever small business you may have, but the tarnishing of your reputation by incarceration of three years. I do not think that the Government has educated its constituents thoroughly enough to enforce such draconian measures that cannot be the reward for entrepreneurs at this time when the Country needs more entrepreneurs. Under this Bill the Government has introduced penalties that create a hostile environment for the average Bajan to enjoy his property, his business and his network that he has cultivated. In my most humble opinion this treads uncomfortably close to the spirit of the Constitution, which may stymie the growth of Small Business Enterprises due to fear of the increased liability. In my opinion, and others', the Government should delay the implementation of penalties until the public is fully aware or sensitised to the importance of Data Protection, and the inherent responsibilities of a Data Controller. For your consideration:

1. a suggested period of three years to prepare before penalties are incurred. That penalties be scaled to be commensurate with the revenue of the Data Controller or the Data Processor.

Also, we request that:

2. the registration and certification of the Data Controller be waived to reduce bureaucracy and also facilitate the proper execution of the duties of the Commissioner. A middle ground where the privacy may be maintained in terms of security.

According to Article 6 of the Electronic Transaction Act, and that only in the case where the Data Controller or Data Processors, Data Privacy Policy is unreasonably inefficient that a data privacy officer is required for oversight. Data Privacy is of utmost importance and I commend the Government for such swift move to protect the interest of their constituents. However, to make it onerous on the average Bajan to start and operate a small to medium enterprise is not in keeping with the resounding mandate that the constituents of this great nation, in full confidence, entrusted to the custodians of this Government. I thank you.

MADAM CHAIRMAN: Thank you very

much, Sir. Are there any questions at this stage? Sir, we reserve the right to ask you questions both on your oral presentation, as well as the written submission that you would have made.

Senator K. J. BOYCE: Through you, Madam Chair. Sir, I think your presentation was quite profound. I understand the perspective of where you are coming from in relation to the small business owner, and also as well the skill set which you bring to the table, [you] being a practitioner within the field. At the end of the day, however, the Government is obliged to balance its obligations with regard to generating business, while seeking to bring itself in a more compliant state, recognising that information and data being the new currency, that there are several external and even internal pressures to make sure that relevant legislation is in place. Recognising the need for that balance, and I have noted your suggestions with regard to delay of the implementation of the enforcement provision, as well as the other suggestions, but assuming you had a magic wand – and I am purely hypothetical – but how would you, in an ideal world, what would be the mechanism that you would suggest that would allow the Government to balance its obligations to ensure [that] the legislative framework is in place to provide the protection of the data, as well as to still encourage and facilitate small businesses which for better or worse have to find themselves in a position whereby they are able to comply with these new requirements, but may not have the resources to do so?

Mr. S. ANTONIO HOLLINGSWORTH: The suggestion on how small to medium enterprises might be able to meet the requirement, basically.

Senator K. J. BOYCE: [To] meet the requirement, and this is an ideal world scenario so you are not limited by any form of practicality, it is just that how they can meet the requirements, [while] recognising that the Government does have an obligation to the same citizens, with regards to the protection mechanisms that are being proposed in the legislation.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you. I will deal within the realm of practicality because within the realm of practicality what is defined as data, according to this Bill, goes beyond electronic, it implies written information that is filed in a filing cabinet; it implies information that may be stored in an app on a cell phone; it implies information that may be stored within a cell phone, and I am going to present a real world situation whereby I had a conversation recently with an individual who is running a small Airbnb and I had to sit down and go through with her the importance of compliance, that she should encrypt her phone, that she should lock the app. These are things that I may know because of my skill set but the average Bajan may not know. I would not be willing to bet, because this is not the place for that, but most Bajans or individuals who may have the latest smartphones may not know or may not be aware that [that] phone has passive listening, waiting for someone to say a key phrase, and they may not have trained it to

recognise their own voice, so that if you are going to bring a Bill into play that essentially could make every citizen a data controller, then the necessary sensitisation should occur before there is any debate. The fact that there are so few of us here to represent orally is an indication of how many people [who] do not understand these 104 pages and the implications of that Bill. So in terms of the practical application, the Government should not place into legislation any Bill that becomes an absurdity because you cannot enforce it. So I would go with a systematic education of the public on how important data is, the value of their data, how they can protect their data. I am just going to ask the question, if I may. How many Members in the room uses two-factor authentication?

(silence)

That is an indication, there are lots of Barbadians who do not know what two-factor authentication is. They may just be people [who are] trying to make a living, they would have lost their job, they might have just been laid off, [they might just be] trying to find a way to make a living and along comes this Bill that requires them to register. My concern is that it bears much similarity with [the] Jamaican Act which requires registration and an annual registration, which is not clarified in this Bill. So [that] for me, the average Barbadian seeing that I must register as a data controller and [that] in that registration there are fees that the Commissioner may impose, and those fees may be annual, [for me] essentially that is a tax.

Senator K. J. BOYCE: Just one follow-up question. Madam Chairman. If you were able then to suggest a delineation between the average person with a smartphone running an Airbnb's, the example that you gave, and the interpretation as to whether that would fall under this regime will be determined, what level do you think the test, what level do you think this legislation should apply for? In other words, do you believe there should be some prescription as to the amount of revenue, [be there] some type of prescription as to specific industries? You will note that there are specific areas which are excluded.

Mr. S. ANTONIO HOLLINGSWORTH: Yes, I know there are specific areas.

Senator K. J. BOYCE: So then, of course, that then raises an implication as to what is included. Would you be able to suggest, then, if we do not want to catch everyone in this net, what areas perhaps the Government should be trying to focus on, to be clear that this legislation should explicitly affect?

Mr. S. ANTONIO HOLLINGSWORTH: Thank you for the question. Maybe we might want to start at the general data protection legislation. It starts off speaking and addressing data controllers on a large scale, it is repeated on a large scale. Of course, that is relative to what is large, the European Union is much larger than Barbados so [that what is] large for the European Union might not be large for Barbados, so what I would recommend is that you look at maybe

the.... Well, that you look at the annual revenue and also you look at the impact that a data breach may have, because if I have ten telephone numbers or ten clients, a data breach of that magnitude could be significant to them in terms of a civil situation, but not necessarily to the extent that they incur half-million dollars and three years in prison. However, a large telecom company that maybe running data for all of Barbados, a breach in that magnitude is a significant breach or if the State has a breach [and] that [would] be a significant breach. Would that be required to be made public? One of the things that I would like to recommend that you also consider, is that while you have a Data Privacy Protection Act that you also have within the legislation or in another Bill, a Freedom of Information Act, if one does not exist. Because if I am surrendering my data to the Government of Barbados, let us say TAMIS, the TAMIS privacy policy is woefully inadequate, and I would like to know that if there is any breach that has occurred that the public authority is held to notify the public that a breach has occurred.

Senator K. J. BOYCE: No further questions. Thank You, Sir. No further questions from me Madam Chairman.

MADAM CHAIRMAN: Any other questions from the Committee? Senator Adams.

Senator R. J. H. ADAMS: Thank you Madam Chairman. This is more a comment. When we had our closed session we talked about the penalties, three years imprisonment or \$500 000.00, and it was my understanding, and I am open to correction here that that is really a question, legal presentation but any Judge would have a discretion to do some of the things you are talking about. Recognise the scale of the breach, the context of the breach and so on, but I wonder if, I think Madam Chairman or Ms. Belle could just lend some comment to that because I would hate to give you misinformation, but I think a discretion is built into that and I know that from your presentation and the way you have written an oral, the way you talked to it that it is of concern. But I believe that is recognised implicitly.

MADAM CHAIRMAN: I am going to ask Ms. Shawn Belle, who is the Senior Parliamentary Counsel who would have worked on the drafting of this Bill to respond to that comment.

Miss SHAWN BELLE: Thank you. Madam Chairman through you, just to speak to how penalty regimes usually work in Barbados by reference to the Interpretation Act Chapter 1. When you speak to penalties, there are expressed at their maximum. When you see \$500 000.00 and then three years in prison, that is the maximum that the Judge can impose for the particular offence that is identified. However, the Judge would have a discretion to impose their role or no penalty to the maximum threshold that is set out in the legislation. Within that discretion then the Judge would then look at the circumstances of the case and then consider the seriousness of the infraction, any mitigating factors before he would impose that penalty. What needs to be recognised is that it would not be a

fixed penalty as I see certain persons interpreting it, but more, that it is an expression of a maximum of that penalty.

Mr. S. ANTONIO HOLLINGSWORTH: May I respond?

MADAM CHAIRMAN: Sure.

Mr. S. ANTONIO HOLLINGSWORTH: I understand what you are saying. Again looking at it from a small business approach, the discretion of a Judge could be one dollar, it could be ten dollars, it could be \$100.00, legal fees to a small business can be the entire revenue of that small business for a month.

Miss SHAWN BELLE: Madam Chairman through you. Just to say that when you are going through civil proceedings, the cost, if it is that you are then the party that is I suppose it falls in favour of that you will be compensated by the other persons. Those are facilities that are provided for by the Supreme Court Rules, those are things that are provided for. I do appreciate that there would cost in starting civil proceedings or things like that but there are provisions for that. Additionally, I also need to point that according to the GDPR, you must take these breaches seriously, and so the State is under a mandate to make sure that they impose penalties that are sufficiently of notice to the public that it is serious. With that in mind, that is why the penalties appear in that form, so I just wanted to speak to that.

Mr. S. ANTONIO HOLLINGSWORTH: May I respond?

MADAM CHAIRMAN: Yes.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you for your submission. Based on what you have just said, I appreciate the benefit that would come for a small to medium enterprise that maybe taken to Court if they have sufficiently justified what has gone on. But, in so doing you have also opened up the door where a large entity who might have been in breach, maybe able to have all of the legal machinations to work against a private citizen, whereby the private citizen loses the case.

Miss SHAWN BELLE: Madam Chair, through you. Just to say there were some submissions in relation to liability insurance and so on, so the question is, whether there is actually a development in the insurance industry for covering the potential liability that you may incur. Now that part is something that would need to be developed maybe outside the sphere of this legislation, because for instance with Attorneys, if they are service providers, they are required to get insurance set up to cover such things where they may find themselves liable for certain actions or infractions of legislation, and that requirement works throughout certain industries or professions. I am just making that observation.

MADAM CHAIRMAN: I believe your time is up now. Thank you very much for your presentation and your contribution. Thank you especially for your comment about public education as we move forward, that certainly is a significant part of the work that has to be done in preparing the country for the implementation

of this particular Bill once it becomes an Act.

Mr. S. ANTONIO HOLLINGSWORTH: Thank you Madam Chair. Thank you for the opportunity.

MADAM CHAIRMAN: The third presenter, I would like to invite, is Mr. Bartlett Morgan, who is representing Lex Caribbean. Please take this opportunity Sir to make any correction with regards to either your name or the organisation you represent for the record.

Mr. BARTLETT MORGAN: Thank you, Minister. Good morning Senators, Members of Parliament, to the Clerks present. First of all, I thank you very much for this opportunity. I think it is a positive signal as to the state of our democracy; it can only allow persons, members, citizens all to have some sort of input into important legislative developments like this. I do not know if clarification is the word, but I am here ostensibly in a personal capacity and with perhaps good reason that I can get into later, but to the extent that I have ten minutes to make my submissions, I would much prefer to sort of dive right in and then we can perhaps deal with those other matters later.

Mr. BARTLETT MORGAN: Now I must say just in the way of framing that I think it is clearly high time that we got about the business of passing legislation like this. I do not say that in the whimsical sense that we always thought it was a good idea and now have got around to it, but I say it in perhaps the more legalistic sense which is that we have passed due obligations to get this ball rolling. I say that among other things with reference to our obligations under the Economic Partnership Agreement (EPA), which we would have signed onto in 2008. I refer to that one specifically because, among the hundreds of Articles which we agreed to, when you read almost to the bottom of it one of the primary things was that we would pass comprehensive data protection legislation within seven years. We signed onto that in 2008, and so literally we are past due on a very serious international obligation, as it were, under the EPA to pass this legislation.

Madam Chairman, the other reason why I mentioned that is because it flows into my first set of submissions. To the extent that I have ten minutes, I suspect that I may not get past the first set and so I will get to the point of it really quickly. To my mind, there are four "big fish issues" which this Committee needs to be mindful of. I had a look at the Order Paper this morning, and I noted that it says that the purpose is really to consider the legislation and the degree to which, when passed, it will allow for the protection of personal data while allowing for transparency and accountability. I am mindful of that in my comments, and so to my mind the major big fish that we need to tackle is the whole question of the independence of the regulator, which is the Data Protection Commissioner. That is the first thing that jumps out at me on reading this latest iteration of the Bill. The other thing is the question of compensation for Data Subjects. Thirdly, is the framework for the Data Protection Commissioner to

actually audit Data Controllers and Processors. That framework may need some re-jigging.

In the main, what I want to start off with is a point which was addressed earlier. I was thinking of not mentioning it but it is the whole question of the implementation periods and the timelines for implementation. I think those are perhaps the four biggest ones. To start off with the whole question of independence, a part of the reason why I would have mentioned the EPA was that in Article 197, I believe, it obligates us to not just implement a regulator for a data protection regime but that the regulator has to be independent. It cannot simply be a sort of spawn of the Government and taking directions from the Government in the usual course of things. It has to operate in a truly independent sense. On review of this draft, I note that even though there are many functions listed under what the Data Protection Commissioner ought to do, there is nothing that speaks in detail to any sort of staffing or human resource-type independence in terms of the Commissioner's ability to impact who is selected, how many persons are selected and so on. There is no sort of budgetary independence that is outlined there. So effectively you have a regulator who will be in a real sense beholden to the Minister to whom he will report. To the extent that this Bill purports to have a regime that also encompasses the Government and Government agencies and so on. I am hard-pressed to see in a situation where, with all of those factors and also no security of tenure, a Data Protection Commissioner would readily and gladly step into a Government agency to audit them and to turn up negative findings.

Therefore, to my mind, if we are to consider this in the context of accountability, transparency and a regime that is effective in the main, unless that is tackled and those issues are tackled then I think it is quite likely that we may end up with a regime that looks really good on paper and looks good to our international partners, but in terms of actually protecting the data-related rights of Barbadians and persons in Barbados, we may not be setting up ourselves to actually achieve that in a real sense. I can perhaps go into more detail but given the time constraints, I will move on to the whole question of compensation.

Madam Chair, if we see this purely in the context of incentives – this is human nature – and if this Act is set up to protect the rights of persons in Barbados who are Data Subjects but there is no mechanism in the Act for Data Subjects to be compensated when their rights are breached, I am hard-pressed to imagine that very many persons would actually go about the hassle of seeking to enforce or to vindicate their rights pursuant to this Bill as drafted. I said that by the way to note that if you look at the legislation that is considered the gold standard nowadays, the GDPR (General Data Protection Regulations), they have that right and it is expressly and clearly stated. If we look at even the prior draft of this very Bill, it had that right to compensation, and so I would suggest that unless that is in place, again we are lessening the likelihood that this Bill when passed into law, will actually meet the test which we set

out for it.

The other question which I think requires some attention is the whole sort of auditing framework that is present in the Bill. As it stands right now and as I read the Bill, it is a process whereby in effect, yes, you can give an assessment notice but you cannot actually go in to assess the Data Controller or Data Processor until you have gotten a warrant from the Courts. That is going to be a very time-consuming and expensive process for the Data Protection Commissioner himself, and with whatever budget the Commissioner may have and however limited it may be, that is more expense and time incurred to simply get a warrant to go and investigate essentially. It would seem to me that, again in line with prevailing best practices globally, we ought to have within the Bill some provision whereby there can be at the very least what I would refer to as a consensual audit process. The Data Protection Commissioner, for whatever reason, may say, "I would like to investigate you", or even of your own volition as a Data Controller you may think your systems are up to muster and so you would want to ensure that they pass the test outlined in the Bill. You can therefore invite the Data Protection Commissioner in to have a look. There needs to be some mechanism to allow for that process because otherwise it becomes an unnecessarily expensive process for even the Data Protection Commissioner himself to partake in.

Madam Chair, as time goes I literally have two minutes left and therefore I will move right on to the whole question of the grace period for implementation. To me, this is a practical issue more than anything else. If we were to quickly pass the Bill into law as an Act in its entirety then most Barbadian entities would be in default or in breach. That is the simple reality of it, and so having a timeframe within which persons can get their houses in order, I think, is just a practical thing that we ought to be mindful of and to legislate for. Also, there is the other added benefit which is that it allows the Data Protection Commissioner to begin his work of awareness because that is one of his obligations. It would, therefore, seem to me that perhaps the best approach may be to pass those sections of the Bill into law that enliven or give power to the Data Protection Commissioner to, first of all, exist so that he can get about the business of sensitisation and awareness and also putting practical mechanisms in place for his own office to operate first before we actually get about the business of enforcing the Act.

In my last minute, I just want to quickly run past that to outline some other matters which I think....

MADAM CHAIRMAN: You are very creative with your time, Sir, but that is okay.

Mr. BARTLETT MORGAN: If my time is up then, that is fine, Ma'am.

MADAM CHAIRMAN: Go ahead. It is your minute.

Mr. BARTLETT MORGAN: Just very quickly, there are a number of other things and first of all I should perhaps apologise because, as I understood, the invitation was sort of to present orally, or otherwise

if you are not minded then to do written submissions. I would be happy to put together written submissions to articulate my position because there are a number of other things that are more like bread-and-butter matters but they need addressing. First things first, the provisions that deal with... Subsection 2, for example, the definition of data controller and data processor. To my mind, simply by using the word "person" it remains unnecessarily vague especially to the extent that this Bill purports to capture data controller and processors who are also governmental agencies and so on, simply using "person" as the definition of a data controller or a processor, to my mind, it may arguably miss the mark. My suggestion is that we actually spell it out. Do not leave it up to chance. Say a data controller is "a person or a corporate entity or a Governmental entity, *et cetera*." If you go beyond that quickly, Section 4.(1) which is sort of like the foundation of the entire Bill because that outlines that actually fundamental principles that a data controller and a processor would have to abide by. It requires the use of the word "and" in there somewhere because you have to abide by all of these obligations and so at some point, perhaps before, at the end of the second to last, the penultimate provision, there needs to be an "and" in there so that it is clear that you have to comply with of them as opposed to cherry-picking one and going well, I am transparent but you know, the whole data minimisation thing. I did not do that.

If you keep it going along those lines, another major one which needs to be addressed is Section 5, Subsection 3 and 4. That has to do with the whole question of fairness. The idea is, if you are being fair in how you collect data then one of your obligations is that at a very minimum tell the person you are collecting the data from here is what I am doing with it, here is who I am going to share it with, here is how I plan to store it, here is how I plan to process it, that kind of a thing. Those matters are outlined in Subsection 3 and 4 of Section 5 but the problem is, when you read through the Bill you realise that essential the same provisions, but in far greater detailed are outlined at Sections, I believe, 18 and 19. In other words, we are basically repeating ourselves and to no good purpose. Especially in a context where this Bill will be used not just by lawyers but lots of everyday business persons. You would have seen that lots of the persons who have presented already are business people, small businesses and so on. They are going to be reading this Bill themselves and so, I think, it is upon us to be as clear as possible about what it is we are doing and what the obligations are and so on.

MADAM CHAIRMAN: Thank you for your submission.

Mr. BARTLETT MORGAN: Thank you very much for having me, Madam Chair.

MADAM CHAIRMAN: I am going to ask Ms. Belle to speak to a couple things because I think it is important that we have clarification as we go into our questions and answers session. There was the question of the definition of the data controller and the data

processor and whether there is a legal person as well as human person, *et cetera*. Number 1, can you speak to that? And then I will ask the second one after.

Miss SHAWN BELLE: Madam Chair, through you, when the use of the word "person" is used in legislation, well, at least, our legislation; it contemplates the inclusion of the individual as well as legal persons so that there would be no need then to specify companies, or other entities that have corporate or legal personality so from that point of view you can take what you can.

Hon. Ms. C. S. V. HUSBANDS joined the meeting at 11:34 a.m.

MADAM CHAIRMAN: There was also the reference to a consensual audit process preceding the need to go for warrants, *et cetera*, I wonder whether or not you wish to comment on that at this stage or you may defer it and we can come back later.

Miss SHAWN BELLE: Madam Chair, if we can defer so I can look more closely or maybe I need clarification in relation to what you mean by that.

Mr. BARTLETT MORGAN: Do you need that clarification now?

Miss SHAWN BELLE: Madam Chairman, through you, if it is that in your written presentation if you are planning to submit then you can write it out so I can see what you mean by it. That would be appreciated.

Mr. BARTLETT MORGAN: Very well.

MADAM CHAIRMAN: I will open the Floor to the rest of the Committee to ask any questions at this stage.

Hon. Ms. C. S. V. HUSBANDS: Sorry. Before you do, my apologies and good morning to everyone. I really enjoyed what I heard and what you had to say so I am looking forward to this engagement.

Mr. BARTLETT MORGAN: Thank you.

MADAM CHAIRMAN: Thank you Honourable Sandra Husbands. Senator Drakes?

Senator Miss C. N. DRAKES: Yes, Madam Chairman, thank you. First of all, Mr. Morgan, thank you very much for your presentation. I thought it was quite insightful. You made some interesting points as it relates to where the legislation lacks clarity on some issues and one of those things that I want to ask you and possibly put it out to the Committee is, we keep hearing this issue of one discrepancy between possibly the size of the company, the revenue it makes and the potential for the penalties that it could incur if you find yourself in that situation. Now on the other side of the coin, we are hearing there is no provision for the compensation for data subjects if you find yourself in a breach and there needs to be some compensation as it relates to your data being used without your consent or however that may come about. I am wondering if at any point, as we revise the legislation, and this is just to table it, if we can seriously look into having a part of this legislation that is reflective of those two elements - where there is some representation as it relates to the

size of companies, if you find yourself in a situation, and as it relates to data subjects and their compensations and the two of those areas being aligned so that there is some fairness in the proceedings in the legislation. I just wanted to table that comment for the Committee.

Mr. BARTLETT MORGAN: If I may just make a comment on that. Apart of why I chose to come here in a personal capacity is, I wear a number of different hats which, on the fact of it, to an onlooker, may seem to conflict so I did not want to take on this process, sort of carrying a grief, as they say. I attempted to look at the legislation just for what it is and what it is we are purporting to bring about in Barbados. The reality of it is, regardless of how you frame it, either business and perhaps larger businesses are going to be displeased, or smaller businesses are going to be displeased and then in the third sector, the data subjects are going to be displeased so you are not going to have any sort of ideal balance act, especially as regards the whole idea of which obligations you ought to comply with and so on. To my mind, the way usually the best place to start is at the beginning. What are we trying to do?

We are trying to secure the data related rights of everyday Barbadians. If that is the objective, then it stands to reason that a small business, by our standard definitions, who is passing lots of personal data should not get an exemption because there is no rule in the black hat hacker world that says we do not target small businesses with lots of valuable information and so, if the risk that we are guarding against is the personal data of Barbadians being misused, abused, and so on, then to my mind, necessarily tackling it head on from the perspective of well, big companies get big fines and smaller entities get small fines may not be the best way. Certainly not in the legislation itself. What I would suggest is that, on the face of it, as Ms. Belle would have pointed out, there is a built-in discretion with a lot of these penalties and so I have to believe that a fair-minded judicial officer of a court and even the Data Commissioner, when he is giving his administrative penalties, he would have to be mindful of the circumstances of the breach. If you are a large company, you have already breached the Act two times and you are still doing the wrong thing and it just so happens that you are hacked again - maybe a major insurance company, for example, just making something up - and thousands of Barbadian data is exposed, you probably deserve a larger penalty, closer to the half of million dollars, but if you are a small entity... This actually brings me to the other thing which, I think, is significant. The Bill does not seem to allow for reprimands. It cannot be that our only approach to getting people to do the right thing is to slap them with a big fine. If you committed a fairly mild breach I am sure a reprimand ought to be enough but perhaps let me... but I am not seeing this draft where the Data Commissioner has the power to reprimand someone because that may be appropriate in the cases of smaller perceived breaches.

MADAM CHAIRMAN: I believe that the time is up. I am going to extend it because I see that...

Bishop J. J. S. ATHERLEY: Thank you, Madam Chair, and thank you for your presentation. It is very insightful. Much of the legislation considered by the Parliament of Barbados in both Houses recently has been in a hurried context where the intention of coming into conformity compliance with international obligations. You made a reference to this and a relative EPA, define for me or describe for me the level of urgency which in your opinion now attaches to this, since you said it is a past due obligation. What is the level of urgency attaching to it or is there a level of urgency?

Mr. BARTLETT MORGAN: Four years, and by that I mean the particular article of the EPA mandated that we put legislation in place seven years after signing on to the EPA. We signed on it in 2008 so it means therefore that seven years hence would have brought us to 2015 and so it means we are four years out on the face of it and so there is that, but to my mind that ought not to be the only, at the basis of our urgency, in getting the document. I remember two years ago, I do not if you come to remember, an economist published a report two years ago that said that data is now the most valuable resource, it is no longer oil and so that in and of itself I think is sufficient reason for us to get about the business of getting this passed quickly in a fair manner.

MADAM CHAIRMAN: Thank you very much. I would like to mention at this time as well it is not simply catching up with our obligations, Barbados has certainly set itself on a path towards digital transformation, and even as we seek to implement the kiosks at the Airport we are recognising that there is some urgency in us ensuring that this legislation gets in place because it facilitates the exchange of information with some of our partners in the European Union and other places and so it is not just what we are playing catch up with - it is also what we need to accelerate towards in order to facilitate the transformation that we are seeking to bring on a digital level.

Mr. BARTLETT MORGAN: I am most grateful to the Committee, Ma'am.

MADAM CHAIRMAN: I see there is one more comment from Miss Belle, and I will commit because I think we have to be flexible at this time when people have meaningful contributions to make.

Miss SHAWN BELLE: Just to speak to the lack of reprimand mechanism, the enforcement notice gives the opportunity for the Commissioner to state his reasons for asking the Data Processor or the Data Comptroller to do something or to refrain from doing something, but is the mechanism of reprimand you are thinking of is a reprimand in and of itself in the league of perhaps, where you would be looking at like the recent juvenile justice legislation type set ups where the judge would be saying and you should do so and so because so and so is wrong, *et cetera*, for rehabilitation or some other type contemplative contemplation?

Mr. BARTLETT MORGAN: As I

conceptualised it, it is really that sort of light touch. In other words, to clarify the whole thing of what the enforcement notice encompasses and so on, the enforcement notices towards an end which is specified which is an administrative fine... for the course ... so to my mind the reprimand is as I would call it a light touch where you are simply saying this is the end result, this is what you get for that breach, a slap on the wrist essentially, but simply saying you have done this thing wrong, refrain from doing this thing full stop but without any further recourse so to speak so it would be an ending of itself.

MADAM CHAIRMAN: Thank you very much. Sir, I would wish to request that you make that written submission as soon as possible, in fact the deadline is tomorrow. I believe that was communicated in the Press as well.

I would like to inform you as well as the other presenters that there may be some things that we were not responding to immediately. It is important for you to know that there being no written submissions ahead we will take the opportunity for those critical and substantive matters to be dealt with in matters arising at the next sitting of this Committee. Thank you.

Mr. BARTLETT MORGAN: Thank you, the Committee for having me.

MADAM CHAIRMAN: Colleagues, I have just been informed that the final presenter for today has informed that she will no longer be presenting and that said I am going to ask your permission to alter procedure as we would have established where we said we will do our oral presentations in the morning then we would break for lunch and come back to consider the written. I will ask your indulgence to take a suspension for approximately 15 minutes and then come back and do at least the first of the written submissions before we break for lunch. With your indulgence can we make that alteration in the procedures for today? I would like to invite a motion so that we can formalise this.

Senator K. J. BOYCE: I move that the Agenda be amended as proposed and that we break as suggested.

SUSPENSION

MADAM CHAIRMAN: Thank you, we will return at 12:05 p.m. to consider the first of the written submissions.

R
E
S
U
M
P
T
I
O
N

MADAM CHAIRMAN: First, Antonio Hollingsworth, next, Sherrine Flan, next, Shannon Clarke, and then Solutions Barbados. So we just do them in that order. Pardon me? Yes, Mr. Coppin, you seem to have a comment. Okay, could one of the... okay, the Clerk will assist you. That is because you would have been added after so, our apologies to you. The clerk will take care of it. The intention is that we will look at, I am assuming everyone has read at this stage. This by the way is a close section in that it is not being streamed. This is just, and the recordings is simply for Hansard purposes. The intention is to go through the critical recommendations in each one, and then have a discussion around them, and then determine how, if at all we would wish for it to impact the Bill. Is that a fair way to proceed committee?

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: The first one is from Soledad González, which is Quidguest, I believe is the name of that company. May I suggest to the Committee that this, from my reading of it, appears to be a sales pitch? That said, it does not gel with the terms of reference of this Committee, and so I would ask that we at this time defer this or disregard it completely? I would like a motion please. I would like to invite a motion that we either not consider this in the context of the Terms of Reference. Is there a Seconder?

Seconded by Senator Miss C. N. DRAKES.

MADAM CHAIRMAN: Thank you. The second submission is from S. Antonio Hollingsworth. This individual would have presented in the name of Bajan Digital Creations Inc., earlier this morning, an oral presentation. This individual would also have made a written presentation. You would have noticed that while his oral presentation would have differed in some ways from his written presentation there are, yes in a significant way. I would still recommend that the Committee consider the written as well. Here are some of the key considerations, and recommendations in this. Has everyone read? And can I just simply jump to the recommendations? You are comfortable with that? I am just flipping because the recommendations are all over the document.

If you look on page 4 number 2, as such I would like to make the following suggestions for your consideration. If we go first to number 2, to reduce the requirements of the Data Controller to fall within the established Article 4 of the Electronic Transaction Act until such time is the public aware, and fully understands the value of personal data? Pardon me?

Asides

MADAM CHAIRMAN: Yes, it is Article 6, my apologies. Article 6 for the record. Miss Belle, can you speak to that?

Miss SHAWN BELLE: Madam Chairman,

just trying to find the place where we are.

MADAM CHAIRMAN: Page 4, the submission by Hollingsworth, number 2 at the bottom. With us?

Miss SHAWN BELLE: Yes. Madam Chairman, just to make the Committee aware that the framework that is set up under the Electronic Transactions Act, is confined to that sphere. So, Data Protection Controller for instance, has a different definition there. There are, and the regulation of Data Protection has specific relation to electronic transaction specifically. So that is one of the things that has to be understood. Now, it may be that at a later date you may want to incorporate those provisions into the Data Protection Bill, but for the time being because it is so specific then that, well rather part needs to be treated as operating in that specific sphere. Meaning the Electronic Transactions Legislation.

MADAM CHAIRMAN: Do any Committee Members need any clarification? Is there something specific you need understood?

Hon. C. S. V. HUSBANDS: The distinction that you are making in terms of what is required of the Data Controller versus how Mr. Hollingsworth had outlined what he saw as the things. I did not quite get that.

Miss SHAWN BELLE: For instance, the definition of a Data Controller in the context of the Electronic Transaction Act, does not have the same definition as in the Data Protection Legislation. Reason being is that those provisions are to be confined to regulating Data Protection in the context of electronic transactions. The data protection Legislation has a wider net, but that piece of legislation is very specific to electronic transactions. Particularly, if you look at the definition of say, the Data Protection Controller, it talks about looking at the certification of electronic signatures, which is not something that is addressed in the Data Protection Bill. So that is why it exist in parallel, but it is not the same, and it is that part dealing with Data Protection only deals with electronic transactions, I have to make that clear.

Senator Miss C. N. DRAKES: Madam Chairman, if I may, just for information purposes. Miss Belle, you are saying within the Electronic Transactions Act there are data controllers?

Miss SHAWN BELLE: Yes.

Senator Miss C. N. DRAKES: Are they registered?

Miss SHAWN BELLE: The registration regime as provided for under the Act, and regulated by their Minister, meaning the Ministers responsible for Electronic Transactions, wherever that may fall within the sphere. They have a different regulatory system, but it has not been. It has not ever been set up, it is done by regulations. So that is a completely different scheme, right. Now, there is no requirement yet for registration, because there are no regulations that have been drafted to regulate their registration. That is why I am saying that it is sphere of operation that is very, very limited.

Senator Miss C. N. DRAKES: Thank you.

MADAM CHAIRMAN: So if I may clarify, the definition in the Data Protection Act, is wider, broader, and differently applied.

Miss SHAWN BELLE: Yes, Madam Chairman.

Hon. C. S. V. HUSBANDS: My question would be, what is the implication of that, for what Mr. Hollingsworth, has outlined? My understanding is he is saying that what is required of a small business person needing a Data controller that that would be beyond the means of a lot of people who have data as a part of their...that was a little while back but everybody heard? I was just saying that I want to understand now given what, Mr. Hollingsworth, has placed on the table that the demand for small business is going to be great. What then would be the options or solutions to make it feasible for a business to be able to....

Miss SHAWN BELLE: Madam Chair, I am reticent to approach this because it gets into the elements of governance and matters that are ministry related or policy related, but the fact of the matter is that when you are setting up a business there are a number of requirements that have to be adhered to. So [that] for instance, if a hairdresser, if they decided that they needed to trade as a business they are going to have to register under the Businessman's Act; they are going to have to pay the fees for the name; they are going to have to deposit all the documentation related to that, as well as under the Health Act legislation; they are going to have to get licensing to operate. All of those things amount to a cost but all of those things are incidental to the running of your business. Now, in terms of anticipating, I understand the concern of the business community that you are adding onto the responsibilities that they would have, in terms of dealing with business but the fact of the matter is that I do not know that there is a streamlining of how you do business, and that is not something that the Office of the Chief Parliamentary Counsel can be asked to refine, you would have to tell us what you are contemplating. Another way, [let us] take the Electronic Filing Act, what that has done is that it allows for the filing of documents that would have been required under certain enactments to be submitted in electronic form. That is a form of streamlining but it only applies to certain Acts that are covered by the Electronic Filing Act, specifically those Acts that are administered by the Registrar, Corporate Affairs and Intellectual Property Office, that is a form of streamlining but you then cannot ask the Office of the Chief Parliamentary Counsel to kind of find a system to streamline the way that you do business. I do not know if you understand the trespass.

MADAM CHAIRMAN: I think one of the things we recognised is that there is some consideration for the micro, small, medium enterprises, the GDPR seeks to speak to that in its own way but we may very well have to deal with that either in the Regulations and that is where we are thinking we may very have to deal with that. I think at the same time too we have to recognise that we are operating in a different

environment and [that] therefore when you are operating in a different environment [that] there are going to be different things that are required in order to operate in that environment. And I think that there is a tremendous opportunity here for there to be some pooling of resources of some of the enterprises, and I will leave that to the Minister responsible for that, but basically my perspective is that there is an opportunity to create shared services in a way that makes sense for them, so [that] there are a number of different ways but I am sure [that] the Minister and his team will come up with how they would wish to do that but we are suggesting that we may consider something for that in the regulations.

So in terms of the reduced requirements of the Data Controller as a specific recommendation on page 4 (2), I am hearing that we wish to keep it as it and not necessarily reduce that but rather take into consideration the best way we can, if there is a case for micro and small enterprises. Is that correct, Committee? Or please correct me if you have a different understanding.

(The Committee concurred)

MADAM CHAIRMAN: So we can go on to the next one? We will say as of (2), there is no correction, that it will not have an impact on the Bill, Minister Sutherland.

Hon. D. G. SUTHERLAND: Madam Chair, one of the areas in (2) that I think that we ought to be aware of is this whole [issue of] public awareness. Mr. Hollingsworth's submission speaks to "until such time as the public is aware of, and fully understands the value..." Yes, indeed, the time is ripe and I heard you mentioned it, we need to explain to the public what is the role of a data controller or what is a data controller as it relates to these small businesses. I think that will bring some clarity, I do not think his main issue surrounds the small man, one or two individuals having a business and indeed having to employ the controller, the whole gambit, so that if we can explain that, because they are looking at a cost, the whole start-up cost for business, he indicated that businesses will not be able to strive in an environment where we are imposing all of these restrictions. Indeed, the GDPR is a good point to reference because we have to be EU compliant as we do business because we are not doing business in a vacuum or within the 166 square miles because some of these companies also, whether they are digital or whatever type, they are indeed transacting business within the EU and that has to be put out there. In addition, the whole cost aspect, and I heard Miss Belle mentioned it, when you go to register a business these are the areas with which you have to comply, at Corporate Affairs and Intellectual Property Office depending on the business whether it is health or agriculture and the lowest or simplest cost is \$150, so we have to educate the public this is just a probably one-off cost and [that] it is not part of the business operation when you have to factor it in once a year or....

I do not know how often you would have to factor in this cost but these are some of the things we have to do, public education is very critical at this time and I myself am not aware whether or not it is a one-off cost, so it is very important at (2) the public awareness and the sensitisation explanation as it relates to micro, small and medium enterprises. I do not think [that] it is a big issue but when you do not give people information [then] it becomes a big issue.

Senator K. J. BOYCE: Madam Chair, through you, following on from the Minister's point, there is a slight variation from my perspective, the issue being, Ma'am, is that there are three positions that I am seeing under the legislation: the Data Controller, the Data Processor and the Data Privacy Officer. Those three titles in terms of accommodation, facilitation or creation within an organisation if you are sole business individual, a one-man shop, you could have your company under the Laws of Barbados but who is going to fill those roles and I think that it should be something that we consider as to what level. This is why I ask the question, what level does this obligation trigger, because there are going to be small and micro enterprises, as the Member of Parliament and Madam Minister had indicated, who would be impacted by this obligation, so [that] if we could perhaps set a threshold – I do not know – but just reading it in terms now that someone has to be defined, someone has to be stated. That is the first point, then when you turn to the obligation with regard to the binding corporate rules at section 25, it does indicate as though the concept is that it applies to a commercial or corporate entity but I do not know if we could perhaps clarify that.

Miss SHAWN BELLE: Madam Chair, a number of issues were raised there, let us talk about the Data Protection Controller and the Data Protection Processor. Now, the thing is, it is by virtue of your operation that it takes where you would be a processor or a controller *per se*, so it is not as if you are taking on some kind of profession or something like that. Most persons, legal and natural would be Data Controllers. The problem is whether they are also Data Processors. As to the data privacy officer.

Senator K. J. BOYCE: Sorry, can I just stop you there. Is it contemplated that you can be both the Data Controller and the Data Processor?

Miss SHAWN BELLE: It contemplates it, yes.

Senator K. J. BOYCE: Okay.

Miss SHAWN BELLE: But because for the most part, most would be Data Controllers and controlling their Data Processors is most likely that your operations would be at their core Data Controller.

MADAM CHAIRMAN: So my understanding is that you can be both in a situation.

Miss SHAWN BELLE: Yes. Now in terms of the Data Privacy Officer, that person is only designated in certain circumstances as explained in Clause 67. (1). When you are a public authority or body except for the Courts, where your core activities as a Data Controller or Data Processor consists of

operations that by virtue of their nature or scope, purposes, regular or systematic monitoring of data subjects, are on a large scale. Thirdly, the core activities are, processing on a large scale sensitive personal data. Now the problem is the interpretation of large scale. Now the GDPR does not actually explain what large scale is. What the guidance does not seem to be pointing to is a working party kind of meeting that came up with some guidelines in relation to what would be considered to be micro, small-medium sized, but they are linked to the number of employees and the revenue that is generated. The problem is that they are linked within the European context, so what would have to happen, is that the Ministry would then have to give instructions to make it locally right. That is why then the approach that was taken is because most would be Data Controllers and you would be handling the data, an obligation should be imposed on you to make sure that you protect person's right because that is the overarching policy, so you cannot be allowed to get away with it. But if it is that you want a straddling or a hierarchical type of treatment, then the Ministry is going to have to take the time to understand what that means. For instance, in the Barbadian context, you would be talking about small business and the Small Business Development Act. For instance, Section 3 goes into a breakdown of what it would mean, they referred to revenue, they referred to the type of business, the number of employees, *et cetera*. Some of you are familiar with the set up there. Is it that you want your concept of what a small business should be to be trained on existing legislation that defines a small business? Or should be looking at something else? This is the purview of the Ministry, so it requires policy directive, but what was the overarching thought process, is that all the persons that to whom responsibilities should be given, they should be given.

MADAM CHAIRMAN: May I recommend to the Committee, the Minister responsible is here and we are just talking about that and will ask what guidance he would wish to give us with regards to how we would deal with small business, micro and small business in the context of this.

Hon. D. G. SUTHERLAND: You are putting me on the spot. What I can say, I do not want to opt out of it, but give us until the next meeting and indeed that will be clarified. We may want to maintain what is in the Act because we have not done any other legislation since the Act, but we are indeed looking at a micro, small and medium enterprise strategy and then after that the Act. That is probably on the not so far horizon within next year. Give me until the next meeting and I will have that clarified for you.

Miss SHAWN BELLE: Madam Chair, just some other observations in relation to implementation.

MADAM CHAIRMAN: Are we still on the number 2

Indistinct Audio.

Miss SHAWN BELLE: Probably it may come

up again.

Senator Miss C. N. DRAKES: Madam Chair, I just want to interject here very quickly so that we can move on. It is in addition to the discussion about the size of the business, can we also look at the risk associated with the type of data. Because you may be a small business but the information that you have is extremely sensitive, so just to have that table in terms of also looking at the criteria by which you may have to have let us say the Data Privacy Officer.

Hon. Ms. C. S. V. HUSBANDS: Just one more thought if I think you would have mentioned it earlier. The workload or the requirements in terms of how much would need to be done, an assessment of it, so that you get a sense of how much demand it would put on a small business.

Asides (Indistinct Audio).

Hon. Ms. C. S. V. HUSBANDS: Right

MADAM CHAIRMAN: I am not sure you can get a definitive, you would need some clarification. I am not sure you would be able to get definitive, it would vary, so for example, I could be a company that does data and that is my core business. That might be different than a company that is selling books.

Hon. Ms. C. S. V. HUSBANDS: No sorry, I was thinking.....

MADAM CHAIRMAN: *(Indistinct Audio).*

Hon. Ms. C. S. V. HUSBANDS: Yes, which is true, but I was thinking more of the lower level one. I think somebody who is into handling a lot of data would recognise that they would have to do a fair amount to make sure that they are compliant, that they do what they need to do on a regular basis, but it was going back to the example that CPC put, the hairdresser. If we could get some kind of idea of how much demand it would put on that business to see how much load it really is, then it would present us with a better idea of if the Ministry of Commerce is going to make some recommendations and changes that it is doing that in relation to how much demand is likely to be put on the business in order to be compliant and stay compliant.

MADAM CHAIRMAN: Let me just make sure that I understand you. So you are saying perhaps we can identify a basket of businesses if you want to call it or a set of businesses. Here are hairdressers, a sampling of businesses, here is pharmacists.

Hon. Ms. C. S. V. HUSBANDS: That then would have a light load. Yes.

MADAM CHAIRMAN: Here is a coconut vendor, here are these various (persons that) have these different groupings of businesses and then come up for some costing for that

Hon. Ms. C. S. V. HUSBANDS: Highly like demand.

MADAM CHAIRMAN: Is that what you are saying.

Hon. Ms. C. S. V. HUSBANDS: Yes that way we can determine whether it is heavy, too heavy or what needs to be done, or if anything needs to be done.

Hon. D. G. SUTHERLAND: I heard Senator Drakes mention the point. Let us use the example of a hairdresser, a sole practitioner, with a database of 200 and so clients. What are the risks associated there? That database would have in it, the type of hair being used, I am just using examples, whether there are scalp issues. You have stuff in a database, even though it is a sole practitioner, it is still high risk in terms of taking that person's information out there, because you may not, Senator Drakes or Senator Wiggins, they might not want Minister Marshall to know about their scalp issue. Indeed, that is a risk and I am not sure how Minister Husbands in terms of the level that you want to put on it. It is a good point raised by Senator Drakes. You cannot only look at the number of employees but you have to look at the risk because you are dealing with information across borders and everything like that now so. I do not think we can just look at the size of a business as it relates to the risk because you are dealing with information across borders and such like now, so I do not think we can just look at the size of a business as it relates to how we are trying to classify micro, small and medium enterprises here. It becomes more tedious and technical.

Hon. Ms. C. S. V. HUSBANDS: Sorry, it is my misunderstanding. What I was suggesting was not so much quantity of data or anything like that. I accept the point about the risk but what I was asking was what would a small business like a hairdresser have to do be compliant, to stay compliant and keep the business safe? If there was a way to capture what demand it would put on the business, it would then make it easier now to determine what needs to be done or how to help a business like that, which would have less sophistication than a small data analytic company that has five people but who are really dealing with some stuff and know what they are doing. It is really about understanding the demand this will put on them so that we can determine how frequently they would have to do things if there is something that needs to be done. If they have to hire somebody, what is that going to look like? It is more that type of thing.

MADAM CHAIRMAN: Minister Husbands, I take your point in that there are going to be certain groups of businesses, a significant number of them, which will all need to be educated in a particular way. I think what we were talking about earlier – I think we discussed it at the last meeting – is that we have businesses, for example a pharmacist, which will have a very different level than the hairdresser, and the discussions we were having was that when we get to public education it cannot be a one-size-fits-all. It has to be where we are able to target the education to the particular business type, and it means then that we have to find a way to cluster the business types and then do public education that would be specific to that cluster. That was part of the conversation, so it still links to No. 2 which is how we do the public education. I think that

is further in terms of how we actually educate the public as opposed to determining whether or not we need to reduce the responsibility of the Data Controller, which is what the submission is actually asking us to do. What I am hearing people say is, "We do not need to reduce it. What we need to do is find ways in which we can support and help to mitigate the impact." I believe that is what I am hearing. Yes, Miss Belle.

Miss SHAWN BELLE: Madam Chair, just to make an observation now. In terms of how things work on the ground in various jurisdictions, a lot is placed on the Data Protection Commissioner to issue codes and to deal with certain areas that require guidance. For instance, let us suppose that people want to know how data protection would apply to installing surveillance cameras on their properties. The imagery would fall under the data protection, so then what the Data Protection Commissioner would do is issue a code to instruct businesses on how to be in compliance with the Act, so you have to notify the person that you are being surveilled and the purpose for which you are being surveilled. That kind of transparency has to be put into your policy in terms of implementing.

When you are putting this in place, it is really important for you to get the Data Protection Commissioner in place so that he or she can start generating the codes for guidance on these various areas. Even things like consent of children and that kind of thing. I do not want to digress but the point is that this person is very important in terms of the educational exercise.

Asides

Mr. CHESTERFIELD COPPIN: I just want to add that whether a company is required to have the three officers was mentioned, but there is a model. There is a model existing in Europe where those things can be outsourced so maybe we could perhaps, in dealing with those small businesses, see how best we can incorporate a model like outsourcing as well as opposed to the small businesses taking on the three particular roles.

MADAM CHAIRMAN: Thank you very much for that submission. Senator Boyce?

Senator K.J. BOYCE: Finally, on this point, Madam Chair, I think Miss Belle has clarified. I am pretty comfortable with the concept that it can be both controller and processor. I was thinking that this is something again for yourself, Madam Chair, and the Attorney General to refer to this Bill. I believe the exemptions that are listed out in the Act set a framework if indeed there is a small business segment that you wish to consider in the future, and I think if that small business segment is then defined based on the criteria set out by Minister Husbands, as well as in consultation with the relevant Cabinet, you may find a solution to exempting the small business holders from the purview; the same way that you provide for the lawyers, the Government and for the parliamentary privilege that exists, Ma'am. I think that may be the

"out" that we can look at providing if it is to be considered for those businesses which you do not wish to put under the obligation.

MADAM CHAIRMAN: Thank you very much, Sir. Let me tell you what I understand with this and we can now move on from this. This is the final comment on it: We are not going to make any adjustments to the requirement for the Data Controller, as required. What will happen is that we will seek as part of the preparation before a Proclamation to get the Data Protection Commissioner in place ahead of time so that the necessary codes and all of the rest can be taken care of. The regulatory framework would have to be put in place ahead as well to help to guide some of these, including treatment regarding the small businesses. Is that what we all understand? Yes? Okay.

Asides

MADAM CHAIRMAN: Let us move on then. The other point that was made here was the requirement of registration. We are at No. 3 on Page 5 of that same submission by Mr. Hollingsworth: That the registration and certification of the Data Controller be phased over a period of three years from enactment. Any discussion or comment on that? That is Page 5.

Asides

MADAM CHAIRMAN: Is it necessary at this point?

Asides

MADAM CHAIRMAN: There is no need therefore for us to address this for this to have any impact on the Bill at this point in time? Okay. The third is to clarify the term in writing as it relates to the Electronic Filing Act. My understanding from the submission from the representative of the Chief Parliamentary Counsel is that there are really different Acts altogether relating to very different things, and perhaps at this point in time we may wish to keep the definitions separate as they are, leave this definition to the particular Act and seek not to deal with it.

Miss SHAWN BELLE: Madam Chair, just for clarification. What you just spoke to was the Electronic Transactions Act. The Electronic Filing Act now is a completely different piece of legislation which he is asking about, so we need to clarify.

MADAM CHAIRMAN: Do we need to clarify this term in writing as it relates to it?

Miss SHAWN BELLE: In terms of having it in writing that is not really in that Act. What that Act is supposed to facilitate is the electronic filing of documents that would have been required under various pieces of legislation by the Registrar of CAIPO (Corporate Affairs and Intellectual Property Office). That is the central focus of that Act, so you would not find anything to do with having things in writing there so I do not know whether he needs to be asked for

clarification on it.

MADAM CHAIRMAN: This is irrelevant therefore to this Act.

Miss SHAWN BELLE: Yes.

MADAM CHAIRMAN: So if it is irrelevant we will not consider it as part of the Terms of Reference of this Committee. Okay? That is Number 04.

Number 5: The definition "profiling" which is on page 15, Part I of the current Bill, that the definition of "profiling" is not in sync with current technology trends. I have to understand that there is a difference ... in fact let me let Miss Belle speak to that because it is a legal question in terms of definition.

Miss SHAWN BELLE: Madam Chairman, just in terms of the definition of profiling, that definition is informed directly by reference to Article IV, 4 of the GDPR. What I am finding is that there is a perspective being put forward by the ITC and IT heavy constituency that is saying that the Act should take into consideration all of these very technical things that have to do with the working of technology and while I understand their concern, the overarching or the mischief that you are trying to address is how the use of technology makes your personal data vulnerable and so it is the backdrop with the focus being the protection of the data once it is put in electronic form. There may be nuances to that and I need to do more research to see what is the - I suppose this is colloquial - endgame of ICT and like industries because all the terms are informed by the GDPR and it has a specific focus and there is also an understanding of these terms in general data protection law. If we go and deviate then we are setting ourselves up to be in contradistinction to other jurisdictions that are trying to follow the same type of regime.

Senator K. J. BOYCE: Madam Chairman, the definitions are just ... following on from Miss Belle, she is absolutely correct. The definition is taking from the GDPR Article IV, 4. I do not think we need to touch it.

MADAM CHAIRMAN: If it was taken from the GDPR do we, as a Committee, believe that we need any adjustments to this as per number 5 on page 5? If not, let us just say no and move on.

The Committee answered a resounding "no".

MADAM CHAIRMAN: Are we unanimous? Is there anyone who is fundamentally opposed to us continuing the "profiling" definition as defined in this?

The Committee answered "no".

MADAM CHAIRMAN: Okay, then we will continue with the "profiling" definition as is with no adjustment to this Number 5.

Number 6, page 5, on that same submission, that there is no justification for sensitive data as defined by this Bill to be legitimately processed by political religious or philosophical bodies given that the Bill itself gives the data subject the right to migrate their data from one to the other. If you flip to page 6, it

continues that sensitive data should only be processed by persons who fall under implied or explicit confidentiality. If you look at page 65 - I know Mr. Attorney General you said you do not want a page, but that is how I had written it - Clause 58, (5)(b). This is the non-lawyer. I am just identifying where I would have seen reference to it when I went over these questions.

Miss SHAWN BELLE: Madam Chairman, just for clarification, because since it is ... yes. The protection of sensitive data is something that is required under the GDPR, Article IX and the reason for protecting such is revelatory through the understanding of the definition. If you are talking about biometric data, if you are talking about your medical records and even the associations that you make, being a member of a trade union, these are matters that should not be dealt with lightly and there is a responsibility that should be taken into account when you are dealing with such data. The GDPR specifies it and the various sections, one of the first Clauses within the Act, seeks to show how those things should be handled.

MADAM CHAIRMAN: Are you clear with that? You have a quizzical look on your face, Hon. Ms. Sandra Husbands?

Hon. Ms. C. S. V. HUSBANDS: I understood what she has said. I was awaiting.

MADAM CHAIRMAN: Any further comment on this section in terms of ...? Do we see that this concern that is raised having any significant impact on the Bill as it currently is?

Senator Miss C. N. DRAKES: Madam Chairman, correct me or please clarify for me. Is this submission related to Clause 9.(1)(e)? That is a Clause that I had some discomfort with myself and that is basically the processing of sensitive personal data and he said, the processing is carried out in the course of its legitimate activities by anybody or association with which exists for political, philosophical, religious or trade union purposes.

Miss Shawn BELLE: Madam Chairman, the thing is the construction is informed by the GDPR. The processing of sensitive personal data, this is Clause 9 that I am referring to, in the chapeau, "processing of sensitive personal data shall be prohibited unless" and then going into the paragraphs it lays it out and then going on in E. Now what I am saying is that formulation is informed by the GDPR. We are trying to become compliant with that. The only way then that you depart from it is if the Ministry or their submissions are saying that we should depart from that in some form because there is some interest that we are taking into account.

MADAM CHAIRMAN: The question is, is there some interest we are not taking into account or is there some harm that we believe we would be doing?

Senator Miss C. N. DRAKES: Madam Chairman, I raise the point and I understand Miss Belle's point as it relates to compliance, however, I will still state that that was actually one of the Clauses that I noted as it relates to the justification for why you would

allow for those entities or bodies to process sensitive data. That exists for political, philosophical, religious or trade union purposes.

Hon. D. D. MARSHALL: I am trying to understand what the Senator is saying. If you look at the categories at (a) and (b), not established or conducted for profit. Immediately that tells you that the information is not expected to be created to enter into anybody... We all go into things and our email address and everything goes out and then before we know it we start getting emails and unsolicited calls so by eliminating the profit motive you narrow the scope, and then secondly, it exists for political, philosophical, religious or trade unions purposes all of which are publicly recognised and legitimate purposes that are in fact protected under every known democratic constituent. I think what this is therefore trying to do, if we go back to the chapeau, is that nobody is allowed to process sensitive personal data. Remember what sensitive personal data is, it is defined in the definition section, that is the rule, but then the exceptions are created at the next Clause, the exceptions are that if a person is carrying out... by anybody or association that is not established for profit, so I think that is a box we can tick, but then exists for political, philosophical, religious or trade union purposes, and then it goes through the other things, so we still need to look at 2, 3, and 4.

Appropriate safeguards for the rights and freedoms of data subjects must be guaranteed. It was ... relate to individuals who are either members or have regular contact with the body for its purposes, and (4) it does not involve the storage of the personal data to any third party without the consent of the data subject, so taken as a whole I would like to say that I do not think that there is any reasonable challenge that could be mounted in those circumstances so I would like to ask the Senator if she would accept the Clause as it stands.

Senator Miss C. N. DRAKES: Madam Chairman, thank you and I would like to also thank the Attorney-General for his clarification.

MADAM CHAIRMAN: My understanding then is that we will accept the Clause as it stands.

Can we move on then to number 7 still on Page 6 of the Mr. Hollingsworth's submission, where automated decision needs to be clearly defined? Do we need to further define this with such specificity as it is being defined here?

Hon. D. D. MARSHALL: My problem, Madam Chairman, is that I do not understand what Mr. Hollingsworth is saying and if I cannot understand what he is saying then I have a little bit of difficulty trying to process the direction that he is trying to orient my mind in. Perhaps that is the beauty of a Committee like this because it is precisely for these reasons that we need to meet in caucus and try to go through what is happening, but I cannot usefully comment on it because I do not understand what Mr. Hollingsworth is saying. He might have been better off coming to sit here and give us an explanation.

Senator K. J. BOYCE: Madam Chairman,

through you, can I ask Ms. Belle if the definition from the GDPR is utilised in terms of that section. Is the GDPR the source for the definition?

Miss SHAWN BELLE: Madam Chairman, the automated decision is not specifically defined. What happens in the language is that it connects itself to profiling and so what is understood as automated decision-making has to do with the "profiling", so if you look at the "profiling" definition you would then be talking about the use of personal data to evaluate certain personal aspects of the individual analysing and predicting aspects concerning the individual's performance at work, economic situation, *et cetera*, so you read those there. The concern then is with that sort of, I guess, action, is that it could promote discriminatory treatment.

Madam Chairman, when you refer back to Clause 18 though, it is stated in a way that is similar to the constitutional provision so there is a declaration in Clause 1 that speaks to, you should not be engaging in solely automated processing including filing but then when you go to subsection 2, then subsection 1 would not apply in certain circumstances and then you have to take into account those circumstances. Additionally, it speaks to subsection 2 not applying where the sensitive personal data is concerned unless it is in the public's interest and suitable safeguards are in place to protect the data subject rights, freedoms and legitimate interest. so it gives an operation within which it is, I guess, to be implemented if you put it that way and the provision again is informed by reference to the GDPR.

Hon. Miss C. S. V. HUSBANDS: Just a question. I am just trying to understand the parameters of that particular profiling action. This might be a bridge too far but I am just asking to find out if it extends out here where for example an employer is looking to employ persons and they do the psychological testing and profiling and they are going to use this information for example to make a decision about employment, would it extend out there or that is cut off at people using information for marketing or something?

Miss SHAWN BELLE: Madam Chairman, that would be triggered if the inputted information were then used to create an automatic decision, so based on the fact that you are black and you are disabled then that creates a profile that maybe you are poor and so maybe you are not supposed to be entitled to a certain loan or things like that so that is where that becomes discriminatory and that is what they are trying to target and protect against.

Senator Miss C. N. DRAKES: Madam Chairman, if I can try to frame it differently so that we can possibly get some clarification, for example, an automated decision is for instance, if you go for a line of credit, the bank has certain parameters, criteria and the algorithm likely makes a decision for the bank and the teller says your loan is declined, is that the type of automated decision-making that we are talking about?

That being, I then take Mr. Hollingsworth's concern regarding the lack of definition behind what we

are including and not including given Minister Husband's, introduction as well. In terms of what are we deciding is automated decision making, given that is a very central part of data processing and anything technologically driven at the moment. A lot of the information is used by machines, artificial intelligence. So, I am not sure if there is a best practice or a general definition that is used for automated decision making in legislation at the moment.

Miss SHAWN BELLE: Like I said, the automated decision-making is tacked onto the profiling, so and then what we probably need to understand is that this regulation, the GDPR, just came out into 2016 and then came into force in 2018. So the jurisprudence that would lead to an understanding or interpretation of these provisions has not actually been generated, so it is working. There are several working parties, it seems in the European Union that are dealing with different issues that would inform interpretations. So, for instance, if it went to Court then the Courts take into account that as an intrinsic instrument for interpretation of this legislation.

Senator K. J. BOYCE: Madam Chairman, I do not think there need be any change since it fits with the definition currently held in the GDPR, and leaving it wide just allows for the wider interpretation. I do not see it as an issue to stop the progress of the legislation.

MADAM CHAIRMAN: If I may be permitted to add my opinion here, what I see him define is specific types of technologies, and if you leave automated decision open then it becomes technology neutral. So when you get new technologies this is technologies we know of right now, there may be others coming in the future, I think that we are wise to not limit it to naming specific technologies, but leaving technology neutral, and keeping broad in mind. So are we in agreement therefore that we leave it as is?

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Fine. I believe that, that is the final submission on this particular paper for our consideration. Have I missed any? Number 1 sparks out ???of clarify legal??? (*inaudible audio*), how is it or supersedes Article 6 of Electronic Transactions Act. That we no longer need....

Miss SHAWN BELLE: Madam Chairman, we did actually cover it when I spoke to the fact that the Electronic Transactions Act, one Act. Electronic Transactions Act, one Act. Electronic Filing Act is another Act. His point dealt with the Electronic Transactions Act, and that there is a part that deals with Data Protection. What I was saying is that part is confined within that particular Act.

MADAM CHAIRMAN: So if I can say now in conclusion, we are looking at this paper that while we take for instance consideration while we are grateful for the submission at this point these recommendations particularly with respect to public education will certainly be taken on board for some consideration.

How we will be able to treat to the micro, small, and medium enterprises perhaps using models that, Mr. Coppin would have suggested could be considered and dealing with the matter within the context of regulations as Mr. Sutherland, would have also dealt with this is what arises from that. Other than that they will be no further impact on the Bill based on this submission.

If at this point it is now approximately 20 after 1. May I invite the motion for us to suspend for lunch and return at 3:00 p.m. or at 2:30 p.m.? At 2:30 p.m. or do you wish to resume sooner? We have four more submissions right now to consider. Do you wish to try to do one more at this point or do you wish to break for lunch? What is your preference Committee? Okay we will break. I just would like to invite a motion then for us to break for lunch and return and return at 2:30 p.m.

RESUMPTION

MADAM CHAIRMAN: Good afternoon. Honourable Members, this Sitting is resumed. Members, the submission that we are going to review at this time is the Barbados International Business Association. There are three major recommendations or suggestions for consideration that are put forward:

- (a) to incorporate cognitive technologies as part of the definition of data processor;
- (b) to set up a local agency that provides shared services to enable micro, small and medium enterprises, which I do not think falls within the purview of this Terms of Reference but we can discuss it;
- (c) Use a percentage of income versus a fixed sum as it relates to penalties.

Members, those are the three things being considered, let us consider the first, the case for that is placed on the very first page of the Barbados International Business Association submission under Item 1. Do we see here a need for the incorporation of cognitive technologies as part of the definition of data processor, and what would be the implications for that? If we could get Miss Belle to speak to the definition, that would help us.

Miss SHAWN BELLE: Madam Chair, in relation to the definition of data processor, that definition is informed by Article IV of the GDPR. The inclusion of the ICT's industries understanding of data processor is noted but if you include those considerations, again it would set us apart from others who are trying to implement the regime and what you would not be wanting to do is having set that up, then have to explain why you would not be providing the same protections or the same flexibility as in other jurisdictions, so that is my main problem in terms of incorporating what their understanding is of data processor.

MADAM CHAIRMAN: So you are saying [that] this would provide less flexibility if we were to do this?

Miss SHAWN BELLE: I believe so and as I would have observed earlier, the ICT's constituency has a particular understanding that is rooted in more technical things having to do with technology rather than focusing on the protection of persons' data which is what data protection is about. But I mean, I could be corrected if it is that there are some learning that say to me that we should take that into consideration but I looked at the legislation from various jurisdictions and they all take their cue from the GDPR.

MADAM CHAIRMAN: Does any other members on the committee have a different perspective on how we should treat to the incorporation of this element in the definition?

The Committee responded in the negative.

MADAM CHAIRMAN: Are we in agreement therefore that we will allow that definition to stand as is without the incorporation of these cognitive technologies? Are we in agreement?

The Committee agreed in the positive.

MADAM CHAIRMAN: Okay. Excellent. We now move onto the second consideration. Local agency that provides shared services to micro, small and medium enterprises to implement data protection requirement. I think one of the things we acknowledged earlier is that there may be some need for us to look at this and see what kind of support should be put there. I am not convinced that it needs to be placed in the legislation at this point in time and therefore that that should be a consideration but not necessarily to be incorporated into the legislation.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I would suggest that it makes a good opportunity for people to start a service to provide, you know, for five or ten people to give them that coverage, so that it could generate potential business opportunities for others.

(indistinct response)

Senator Ms. A. M. WIGGINS : Madam Chair, the consideration I would like to say here that would incorporate discussion that went on this morning, it would be in addition to what I said in reaching out to the different groups of organisations out there. I know that Minister Husbands was associated with the Small Business Association but I do not know if Senator Holder can make, or if you can make her part of the Committee, because a lot of this legislation seems to be directly impacting on the small business people and I think [that] they should have a voice and given that we have the Senator here who is the Chief Executive Officer of the Small Business Association I would say, with respect, Ma'am, that either make her a part of the Committee or let her come in and make a presentation on behalf of the Small Business Association. Ma'am, to continue what I said before, then they would say, well, you see, they did this and we were never consulted. With respect, Ma'am.

MADAM CHAIRMAN: Mr. Coppin, you were involved over the last several years with the consultations. To your recollection was there representation by the small business community as inputs to the Bill that is drafted at this time.

Mr. Chesterfield COPPIN: Yes, Madam Chair, we would have had consultation with Lynette Holder and all stakeholders with regards to the drafting of legislation and so on, but the thing about this is that we are saying small businesses because we have maybe an affinity and a feeling but it applies to all businesses, just that we think that because they are small [that] they are vulnerable and I do agree with the vulnerability, but the pieces of legislation pertains to all businesses.

MADAM CHAIRMAN: I think what I am gathering from that is that there are different client/groups or stakeholder groups that we wish to engage. As part of this now, I would have to be guided by the experts, the Clerks of Parliament but my understanding is that the Committee as constituted is the Committee as constituted, that the Committee will then consider what it needs to consider in Committee and once we have made the decision, we can then engage other stakeholder groups as we start moving towards implementation. And I would wish to make sure that we have that level of input, so thank you for that. Would the Committee agreed that that is the way that we go forward?

(The Committee responded in the affirmative.)

MADAM CHAIRMAN: In support I would say that, yes, we do this, I agree that this is a business opportunity and I also would wish to state that it is not the Government's place necessarily to take up this opportunity on its own. I think that we also would need to encourage the private sector to take this up as a business opportunity, rather than Government do it all at this stage.

The final consideration was the use of a percentage of income versus using a fixed sum as it relates to penalties. What is the Committee's perspective on that?

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I agree with this recommendation here. As it rightly pointed out, large companies with very deep pockets can make provision for accidental or deliberate violation of the legislation without skipping a beat, whereas that same fine on a small business would put it out of business altogether and therefore a percentage, I think, would be better with a floor minimum, if you want, a reasonable \$1 000 or \$2 000, something that a small business would feel but it is not going to put them out of business to have to pay the fine.

Senator Ms. A. M. WIGGINS: Madam Chair, I think that discussion went on this morning at some point where I think they were saying a judge has discretionary powers, in terms of whether they are going to charge company X zero dollars or half-million dollars, so I think we more or less would have....

Asides (Indistinct Audio).

Senator Ms. A. M. WIGGINS: Yes we would have covered that this morning. I think Miss Belle spoke about it also.

Asides

Senator Ms. A. M. WIGGINS: Yes the Judge has discretionary powers, so she would not charge somebody..... because you see and then we talk about the whole question of small businesses and information because lawyers might, as sole traders might be viewed as a small business but they might be holding a lot of sensitive information and my favourite group of persons, doctors, that they might be small but they handle exceedingly sensitive information. Are you going to then impose a fine on the doctor who has the

more sensitive information, the harsher should be the fine rather than looking at it in terms of the amount of clients that the small business itself holds?

Miss SHAWN BELLE: Madam Chair just to raise the fact that another one of the submissions, it mentions the setting of minimum penalties. Now that has been struck down by the Court of Appeal as unconstitutional because it fetters the discretion of the Judge to tailor the punishment to the particular offence, so that just to state again, in legislation the expression of the penalty is at its maximum. The Judge will have the discretion to impose no penalty or the highest threshold, depending on the circumstances of the case, whether there are any mitigating factors, whether the person is a frequent person who contravenes on more than one occasion, those kinds of factors. I just wanted to say that once again.

MADAM CHAIRMAN: Any other member would wish to say in terms of setting whether percentage or flat range.

Mr. Chesterfield COPPIN: Madam Chair, I would prefer it to stay as is in terms of a flat amount. As I mentioned before, in dealing with percentages especially with the landscape of our small business structure, it might be in terms from an operative level it might be difficult and onerous, so because of the bookkeeping mechanisms that some do small businesses have in place. My opinion is that we stay as is for the current moment.

MADAM CHAIRMAN: With the option to review at some later stage if we so choose.

Senator Miss C. N. DRAKES: Madam Chair, just thinking it through, because you have the options of either the percentage or a maximum of the \$500 000.00, is there any room for the inclusion of both? I mean, that is under the guidance of obviously CPC, as she has quietly stated previously that the GDPR speaks to percentages.

Miss Shawn BELLE: Madam Chair, just to say that if you go into that, it is okay to impose that kind of dual regime, but what would end up happening is that the Ministry as the pilot Ministry would have to then get into what constitutes a small business, as opposed to what constitutes a large business, should a medium size business also be dealt with on a different regime. Our tradition in terms of penalties is basically the expression of the maximum penalty, so to introduce this type of a system now actually requires more consultation, more time to look into how it would actually function.

Senator Miss C. N. DRAKES: Thank you.

Madam CHAIRMAN: In light of these discussions in bringing to close, the three major considerations let me recap what I understand it to be. That with regards to item one which is the incorporation of cognitive technologies as part of the definition of Data Processor, at this point in time we will not change it as we do not want to distance ourselves from the very regulation that informs this Bill. Two, with regards to local agency that provide shared services, it is outside of the scope of the terms of reference and at the same

time while we understand that this is a good thing to do let us encourage it as a good business opportunity for the private sector, not necessarily for Government, but there would be no additional change, no impact on the Bill. Third, use of a percentage of income versus a fixed sum, that rather than either several options were put on that table, either what exists now, a percentage or some combination of the two, and my understanding from the Committee is that you would prefer at this time to keep it as is and review it, and if anything we can make the adjustments at a later stage. Committee is that all complete in terms of what.

Senator R. J. H. ADAMS: Sorry Madam Chair and excuse me for arriving late after the break. I just have a comment on that percentage one, number three there. We said at some point earlier today that it is one thing to talk about percentages of revenue and another thing to talk about the gravity of the data that has been breached. What do we do in that case of a serial offender for example, large or small, possibly cannot afford whether it is a percentage or a flat fee but it is still a serial offender? What other sanctions beyond the financial are available for someone who just persistently, for example, I do not know, let us say it is a small business and they are driven out of business because they cannot pay the fine and the principles just start another business and do the same thing in a recidivist manner. I believe we can find an example of that perhaps not with data breaches but in other areas of the law. I am not sure if the bill can capture this sort of case, but it does seem to me that it could be an escape patch in some cases. I do not have the answer, but sometimes it might mean the disqualification of directors for example from doing the same thing in that business or in another business that is subsequently incorporated. Do we think that perhaps that is something we should consider or is that already been considered?

Miss SHAWN BELLE: Madam Chair, just to intervene. there is the mechanism of the imposition of the administrative penalties under Clause 94, so that the Commissioner can after a hearing where they have contravened certain provisions in the legislation and the Commissioner considers it to be in the public's interest they can make an order for the person to pay to the Crown a penalty of an amount not exceeding \$50 000.00. We put that threshold because it is an admin penalty meaning that the Commissioner or functionary is actually imposing it and not the Court, so there needs to be a threshold on that. In imposing that, the factors that the Commissioner will also take in apart from the public interest, is the nature and gravity of the offence, the intentional or negligent character of contravention, previous contraventions of the Data Controller or the Data Processor in relation to offences. Those are the kinds of factors that can be taken into account in terms of imposing an administrative penalty. Remember too that there is also the enforcement notice, which compels or ask persons to refrain from certain behaviours so that the Commissioner's resources in relation to dealing with persons who may be frequent offenders.

MADAM CHAIRMAN: Your question asked about financial penalties and then you asked about others.

Senator R. J. H. ADAMS: Thank you Madam Chair, it may do, I just want to be clear. Let us say we have a case, because this is something I have seen in Europe. The cases I have seen in Europe involved fraud. Someone creates a company, runs a deliberate fraud and the company is disqualified but the directors, because there is an absence of sanction stopping them, will reconstitute another company and do the same thing again. This is really what I am getting at. Can you stop a persistent offender restructuring under a different type of corporate entity and just doing the same thing again?

Miss SHAWN BELLE: No, Sir, we do not have anything like that but perhaps you need to take that into account in terms of the regulatory framework. The tradition is usually to impose penalties, fines and so on. That has usually been the case but in terms of going into specific administrative consequences like suspending the licence and so on, those are things we would have to work on and articulate fully. Maybe we need to look into it; the pilot Ministry.

Senator Ms. A. M. WIGGINS: Madam Chair, I was just wondering, in terms of what Senator Adams alluded to, if that would not be coming under the Companies Act in terms of the treatment of directors. When companies go bankrupt, as you know, the directors are individually and severally liable for all the liabilities of the company so I am just wondering if you could not cross-reference the Companies Act there.

Miss SHAWN BELLE: Madam Chair, it is true that you can have legislation on similar areas interpreted together. The problem here is that you are looking at a different functionary who is imposing a penalty for different reasons. What you would have to do is create the capacity for there to be regulation in that vein, because it is not regulated under CAIPO. It is regulated under a different regime in this Bill.

MADAM CHAIRMAN: Are you saying therefore that it can be addressed in the regulations as well?

Miss SHAWN BELLE: Madam Chair, this is not a matter that you should deal with in regulations. It is a matter that would have to be incorporated into the Bill. The question is whether the pilot Ministry would be in favour of employing those kinds of methods in order to deal with something like that. Remember too that even if you are talking about suspension and cancellation, you still have to have a right to appeal and a right to be heard and all of that. Those kinds of mechanisms would still be put in place in order to protect the rights of persons, because once they get the registration aspect dealt with then there is a question of going to livelihood and their operations.

MADAM CHAIRMAN: That said, may I suggest to the Committee that we take this one away for further consideration and get back to the Committee at our next meeting before we conclude the Report? How does the Committee feel about this?

Miss SHAWN BELLE: Madam Chair, it is still a question of who would get back to the Committee. Certainly the Chief Parliamentary Counsel is not going to put forward anything.

MADAM CHAIRMAN: No, it would not. This would have to be a consideration among the Ministries that would be involved and we would speak to it in the proper context to get back to you on that.

Asides.

MADAM CHAIRMAN: Okay, then it seems as if we have concluded this one Paper. There are three questions in the back but I think we can answer them quite simply. They are speaking to what is the registration fee for the Data Processor and the Data Controller. Those will be dealt with in regulations. The final question is why does the Data Protection Commissioner have to be an attorney-at-law? Simply because of the functions of the Data Protection Commissioner, he or she really needs to know the law. They need to be versed in the law. These are simple questions to be answered. We have now concluded the third of these. There are two others to go.

I now want to move onto the submission which was the third in line, from Mr. Shannon Clarke with regard to the recommendations. We want to make sure that we give the fullest consideration to all of the persons and entities that have taken the time to submit their submissions. Let us move to the penultimate page, the one before the last, under 'Suggestions for improving the Bill'. Let us go through these considerations very quickly and determine whether or not they would have an impact on the Bill. It reads as follows:

"The requirements for the compliance for the business should match the level of access that the company has to customers' private information, such that the company deals with sensitive information."

I believe that is part of what Senator Drakes was saying earlier. Are there any further comments on this? Should this necessarily impact the Bill as it is now?

Senator R. J. H. ADAMS: Madam Chair, just a couple of comments. I think the answer is "no" because to lay out a different set of requirements for different levels of access really requires a lot of consideration business by business by business, and it is sure to open a can of worms when something goes wrong. I think this is one instance where a blunt instrument is better than trying to wield a scalpel across the ten thousand businesses that are in this country.

MADAM CHAIRMAN: Are we all in agreement with Senator Adams and the fact that this suggestion should not impact the Bill at this time?

Asides.

MADAM CHAIRMAN: Okay, good. We move on to No. 2. I believe we have covered No. 2 with regard to using a percentage for the fines versus the flat range or fee so we will move onto No. 3.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I am glad that this has come up again.

MADAM CHAIRMAN: Which one? Are we referring to No. 2? Okay.

Hon. Ms. C. S. V. HUSBANDS: I think it links back to No. 1. I agree that if you start trying to change up the compliance requirements it gets really hairy. The thing would be that when it comes to penalties, this is where the differences between the operators now would become important. I still think that large service providers are not going to be deterred because they will factor that in. The access to people's data for marketing purposes is so major for everybody, and if half of the people are like me when they ask me if I want to receive things, I say no. To have this database of people is going to be a temptation and many companies that need access to that market will say, I will pay the \$500 000. I am not sure that we would get the deterrent that we are looking for. My other concern is, I heard the issue that the Commissioner – Is it the Commissioner that has the power to impose the fine?

Miss SHAWN BELLE: Administrative penalties.

Hon. Ms. C. S. V. HUSBANDS: Sorry, let me get it technically and legally correct, the administrative penalties, the Commissioner can decide between \$0 to ...

Miss SHAWN BELLE: No.

Hon. Ms. C. S. V. HUSBANDS: No. Okay. I have it wrong. Help me there.

Miss SHAWN BELLE: Okay. They are different regimes. In terms of criminal offences, when the penalty provision is constructed the penalty is expressed at the maximum threshold. The judge, in that case, can impose no penalties or the highest penalty based on the case and what the circumstances are but what I am drawing to the attention of the Committee is that the Commissioner has within his toolbox of enforcement the facility to impose administrative penalties and those administrative penalties have a cap necessarily because he is the one imposing them and they also can only apply to certain sections. That is really what I was talking about.

Hon. Ms. C. S. V. HUSBANDS: Okay. The point I was going to raise is that my concern would be if the person imposing the penalty or determining what level to apply, should we assume that they have a good understanding of businesses and business' sensitive and so on. That is my main concern. The same way how we are going to spend time educating the businesses, educating the public about this so that people can transition on to it, should we not make sure that whoever, whether it is the judges, then we should not assume that they have enough knowledge. What sometimes happens because we are all human is that somebody may be brought before the Court, they committed an average offence, it is nothing huge but because sometimes some people do not know how to handle being wrong, they might have a little attitude in front of the judge and the judge decides, "um-hum, see you, \$20 000 in your bosom" and the small business

closed down. That is my concern. I do not know how we can address it but I feel that some education and guidance for the persons who have to impose penalties should have a clear understanding of some of the things to consider when imposing the penalties as a kind of a guideline or something because you are asking somebody to make a judgment call who is not necessarily an expert in business or small business matters. That is my main concern with the penalty as it stands. I feel some attention could be given to looking at it.

Miss SHAWN BELLE: Madam Chairman, just in relation to the administrative penalties, 94(2) sets out the factors. Apart from the public interest, sets out the factors that would guide the judge in terms of what penalty they would impose. That is the Commissioner who would be an expert in the field of data protection.

In relation to the judges, the thing is that in imposing penalties you are not also only taking into account the construction of the penalty itself but you are also taking in the account the jurisprudence that has developed around imposing the sentence so that there would be circumstances which the Courts have already litigated and have found that in this particular circumstance, this particular penalty is appropriate. I take the point that the jurisprudence in data protection may not have the depth of that yet, but there are a number of working studies and so on that the judges can have a look at to inform how they approached things. I think too that you have to give credit to our judges. They are not incompetent and they understand what is serious and what is not. I think you need to differentiate them.

MADAM CHAIRMAN: Senator Wiggins.

Senator Ms. A. M. WIGGINS: Thank you, Madam Chairman. I just wanted to make three points and one may fit into penalties. Speaking with respect to the whole question of the harvesting of the personal data because sometimes when you log into a hotspot your information is automatically captured by the particular company and then you start receiving emails, you see it on your Facebook page and you did not subscribe *per se* to the company or you did not say yes, you did not tick any box, you just logged into the person's Wi-Fi, be it a hotel, because as you, as soon as you check into a hotel you start getting all the confusion that you do not want, all the information about coming back and a year later I am still getting emails inviting me back to hotels. I am saying that sometimes, because you have to log into other people's Wi-Fi you are going to get the unsolicited emails and everything coming at you. This information can be shared and you are totally unaware that somebody has captured your personal information and it is being shared and you do not know. Of course, when you are going on Amazon and those places and logging in, that information too is shared and then not only is your personal data in terms of whatever, but your financial data is also shared with other companies. Again, as I am speaking to financial data and that is why I wanted the Bankers' Association here because they already capture a lot of personal data.

As I said, they have an integrated system and I want to speak to you off the record about something Senator Adams. They already have an integrated system. If you apply at one bank and say you do not have any loans any other place, they know that you do. That system already exists in Barbados. The question is, did you give Bank A permission to share your personal financial data with Bank B? So then there should be cases where the injured party should be able to get some kind of redress especially from a banking institution for sharing your data without your permission because as far as I know, Senator Adams can correct me here, a lot of the information that we take for granted here in Barbados you cannot easily share in the European Union.

Senator R. J. H. ADAMS: Yes, thanks for putting me on the spot. For the avoidance of doubt I want to make it clear, I have none of Senator Wiggins' personal or financial data anywhere. I am not sure I have the answer to the European Union's part of the question but as you were talking what struck me was not so much the enforcement but the fact that many people will ignore the legislation and it is hard to catch them in the net and I think we have to accept that. Any piece of legislation that has a punitive section to it is going to encounter that I think.

From those examples you gave, what often strikes me from a prior job is that you have no way of knowing who breached your data. You may know somebody is misusing it but you do not know how they got it or who is the original offender in that, so that is not really an answer but a supplementary comment.

Miss SHAWN BELLE: Madam Chairman. I just want to say that in the scenarios that Senator Wiggins would have drawn out, you have the right to have your information restricted, you also have the right to erasure and you have the right to access, so within the sections that they are dealt with, your first recourse would be to make the Data Controller know that this is your desire. If then there is a problem then you resort to enforcement from the Data Protection Commissioner, so those are matters that can be dealt with there. If it is in the situation that Senator Adams outlined where there is not a knowledge of who would have disseminated, the Data Protection Commissioner under the information notice could seek out the information because there would have to be an electronic trail and so in investigating then they would try to find who would be the party that needs to be targeted in terms of providing redress.

MADAM CHAIRMAN: Does that address the matter that was raised? Okay.

Hon. Ms. C. S. V. HUSBANDS: Senator Wiggins raised a very important question and I have a slightly different one. I know that the 'on the surface answer' would be "well just don't go there" but there are so many service providers who make it mandatory for you to tick off yes and that they have cookies that they will trail you and yes we will be giving it out to third party persons but in a responsible manner and it is a service that you have to access so for me as a

consumer I often feel cornered by those companies because it is an issue. If I travel and I go into a hotel I have to have the Wi-Fi to do what I have to do because I am travelling on business, I am not joyriding to say well look I do not mind being without my connection for a week or whatever.

Asides.

Hon. Ms. C. S. V. HUSBANDS: Well, who wants to do that? Madam Chairman, I am just wondering if there is anything that can be done about those attempts to corner the consumer in a way that you are obligated to thing if you want to transact.

Miss Shawn BELLE: The Bill will not address that directly but what is happening is that an environment is being created because of the introduction of the GDPR, General Data Protection Regulations, so that you probably would have received notification from even Google to say to you that they have to perform in certain ways and you provide this information or you do not provide this information, but that is not because a jurisdiction went after Google. What they are recognising is that if they do not comply the sphere for operation, it then starts to close. So it is an environment that is being created because several countries are getting together to say this needs to be handled. It is the same way with like treaties. I mean you can go to international courts and all of that but the main form of enforcement is actually peer pressure so that is what is eventually going to happen in relation to the GDPR because even though it started out as an European Union standard because of the size of the European Union it might as well be an international standard. I do not know if people understand.

MADAM CHAIRMAN: Are there any further comments on that at this time? Okay. Then, is it fair and correct for me to say that we have exhausted the discussion on Number 2 and that we stand by the original decision that had been made with regards to the fines but we do take into account that there are other areas such as those pointed out by Minister Husbands, Senator Adams and Senator Wiggins that we would need to take into account.

Can we move on then to Item Number 3, the enactment of the Data Protection Bill needs to be delayed. I believe that this matter was addressed by Miss Belle earlier when she said that it will be done by proclamation and basically you can proclaim the Bill at whatever time you choose to proclaim the Bill, well if it is an Act then it would become and Act, giving yourself enough room to take care of whatever internal matters would need to be put in place in order to facilitate its implementation, so I believe we have dealt with Number 3 and therefore no further impact on the Bill.

With regards to Numbers 4 and 5, one speaks of public education campaign and business training sessions. I do not think that they necessarily relate to the Terms of Reference of this Committee but we did say that there is some consideration that we would have to give to these matters. With that said, based on our

conversations we will note this submission and it would have no further impact on the Bill as it stands.

The final submission for today we can consider is that from Solutions Barbados and I would just ask for you to follow on from one page to the other, there are four pages of submission. I know that certain parts interrelate and so we may very well be able to deal with several parts at once, so let us start with Number 1, the preamble to the page, grammatical errors. I believe errors happened and they will be corrected, that is why this is in a Bill format and so when it is finalised basic errors will be corrected, and indeed we are grateful for some that are pointed out.

Section 9 deals with the non-consistent processing of sensitive information by political parties, and they are suggesting that this should not be permitted. Is there anyone who has a specific perspective on this? In other words, should this at this point in time impact the Bill in any way. Yes/No.

Miss SHAWN BELLE: Madam Chairman, this actually links back to a discussion that we had earlier and the Attorney-General provided clarification as to why it needed to be included so I would defer to the Attorney-General.

MADAM CHAIRMAN: Correct. So we will move past 9.(1) which would have no further impact. Section 10.(3), that the Data Controller shall provide a copy of the personal data undergoing processing to the data subject. The concern here being that when it gets to the point where the Data Controller has reasonable doubts, Section 21 suggest that they may request the provision of additional information necessary to confirm the identity of the subject. My understanding is that this provision was put here to give the controller flexibility in terms of confirming identity as it.... There may be many different ways other than directly with the subject to confirm identity. So, if this Committee is in agreement that, that flexibility should remain for the Data Controller.

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Therefore this one shall have no impact on the Bill either.

Section 15.(3), page 31, in exercising his or her right to Data portability. The concern here was that there are gender references one part of the Bill deals with "his", some say "hers" *et cetera*. For consistency certainly, we agree that it is proper form and we will seek to have that consistency throughout the Bill. So can we move on now to Section 22, to which this reference is made. It is suggesting that we try to define adequate, and appropriate safeguards as it relates to section 22, which says that Personal Data should not be transferred to a Country or territory outside of Barbados unless that Country or territory provides for an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data and appropriate safeguards. On condition that the rights of the data subject are enforceable and there are

available effective legal remedies for data subjects. It asking that we further define adequate and appropriate safeguards *et cetera*. It further suggest that it should be a list. Well, let us deal with that one first before we go on to the next one. Is there some concern here, any comment from the Committee?

Senator R. J. H. ADAMS: Madam Chairman, I guess I have comment. I understand the desire to make everything schematic and box ticking. Did I do this, and did I do that. I cannot help thinking that context is always going to defeat that approach and you have to leave something for if it goes before a Judge for them to interpret. I have some sympathy for this, but I just cannot see it working... the maintenance of a list. We know all about blacklist, and grey list. I am not sure that is a business that I want us to get into just from the maintenance point of view. I think, I would rather we spoke about the, and I am not sure I am making an appropriate, we spoke about the confidence of judges and so on. I think we have to rely on their confidence in this one to define what is adequate and so on and so forth.

MADAM CHAIRMAN: I would certainly agree that for us to start putting Countries on negative list and positive list as this recommended will really create a level of activity on the part of Government that could certainly not be something that we can handle. Plus it is impractical because the list would have, if we put this in the legislation, the list would have to be changing constantly and we would have to bring some kind of legislation by order or some other form. Each time that it has to be changed. I am not sure that currently this is something we want to impose on our system as it is. Therefore, I would say with regards to section 22, it seems that there is consensus around the table that it does not have an impact on the Bill as drafted. Is that correct? Agreed.

Section 50(4), page 59. A person who operates as a Data Controller without being registered will receive a fine. The question raised here is that Data Controller is anyone who is responsible for processing data, which can include every employer, and this needs clarification. I am going to ask Miss Belle, to speak to this matter with regards to any confusion.

Miss SHAWN BELLE: In terms of clarification, the sure answer is that it will apply to legal and natural persons. So, yes it could apply to every employer. In relation to an educational institution, usually there are run by boards, and that would be the legal entity then that would be liable. So it does not need clarification, when you use a person it applies to the natural or to the legal person.

MADAM CHAIRMAN: Now that there is that simple clarification it is an inclusive Bill, so all are included here. Section 55(1). A person shall not operate as a Data Processor unless he is registered in the register of Data Processors, and the point here I make is if there is no separate Registration Act for the new profession should it then be included in the Profession Trade and Business Registration. I believe Miss Belle, spoke to that a little bit earlier, and the reality is that a

new profession is not being created that is not the intention of this Bill. I would let Miss Belle provide a further perspective on that.

Miss SHAWN BELLE: Madam Chairman, yes, just to explain. This is not a new profession in the lane of, oh this is regulating lawyers, and this is regulating accountants. The nature of your activities will dictate whether you are a processor or whether you are a controller. Your registration requirements that come out from that. So that is why then you would only require to register under this Bill. There would be no need to refer or go under the Profession Trade and Business Registration Act.

Senator Miss C. N. DRAKES: Madam Chairman, just thinking this through a bit more as well. We stated earlier that a Data Controller can also be a Data Processor, and a Data Controller needs to be registered. Given that, that may be onerous on businesses, we also spoke about having the possibility of that being outsourced. If that is outsourced from a business what mechanism do we have in place then and this is just thinking it through, because of the conversations that we have had. How does a company then make itself compliant if it outsourced the services of the Data Controllers and the Data Processor?

Miss SHAWN BELLE: Madam Chairman, what would happen is most entities are most likely going to be Data Controllers. The question is whether they are also Data Processors, and the decision to outsource may be there. They may also have to go through the debate as to whether they would register as Data Processors although what I would argue is that there are core activities would suggest where the meaning lies. So that if you are for the most part doing what would be considered the functions of the data controller, you register as a controller particularly, because the Data Controller has responsibilities over the Data Processor. That is how I would, and that is applying a purposive approach to interpretation to make things function. Sometimes everything cannot be put in legislation in terms of how things work, but you cannot interpret the legislation to render it absurd.

Senator Ms. A. M. WIGGINS: Madam Chairman, my concern here in terms what he has if there is no separate legislation then it should be included in the Professions Act. I think again because we are dealing with a small society like Barbados that we must consider the additional persons who will now have our confidential information, and there must be some way of policing them, and I think he is suggesting here that they should be registered because if they are registered [then] they [would] have a higher obligation to be confidential.

Miss SHAWN BELLE: Madam Chair, through you, just to say that [the] profession, trade and business registration is targeted to regulate professions, basically lawyers, doctors and the like. This is not creating a profession, this is basically identifying what this company does and then if you do that activity, then you should be registered as a data controller or a data processor, whatever is applicable to you, and the

registration regime would already control what is required.... Well, okay, I am rambling, sorry.

Senator Miss C. N. DRAKES: Madam Chair, I understand what Mrs. Belle is saying, in terms of not creating a new profession but I am speaking to the very critical issue of accountability.

Miss SHAWN BELLE: Madam Chair, again, the application for registration goes to the Data Protection Commissioner, so [that] the Data Protection Commissioner is going to be the person who has responsibility for maintaining the register and for dealing with the applications, so [that] he is the regulator.

MADAM CHAIRMAN: The question is, can a person, whether legal or human, register as both processor and controller or would they have to choose one?

Miss SHAWN BELLE: It is possible that they may have to do both if they are doing two functions, but I would say that you would lean to the core activities that you are performing and that that informs how you register.

Senator Miss C. N. DRAKES: Madam Chair, so [that] I can recap and make sure I am clear, if my core, let us say for instance, a doctor – bad example – and I outsourced the information to a data controller who is registered, what would happen is [that] the doctor, by virtue of his job, in collecting the information is a controller, because he then organises and distributes that process. He might outsource, which means that he would be outsourcing the processing issue, [would also mean] that processor needs to be regulated.

Miss SHAWN BELLE: Okay.

Senator Miss C. N. DRAKES: Madam Chair, if I can continue to seek clarity, if that doctor outsources that service and the information is then breached, who is responsible?

Miss SHAWN BELLE: The data processor, if you have me having that arrangement, the data processor is accountable to the data controller under the provisions of the Act, so you cannot process without the data controller, meaning the doctor's authorisation and the doctor then, as the data controller, if there was a breach under the Act, the doctor has the responsibility to report it to the Data Commissioner and the Data Subject, particularly where it is infringing that person's rights and there has to be time limits within which to report.

Senator Miss C. N. DRAKES: Thank you, Chair, this is an extremely insightful exercise.

MADAM CHAIRMAN: [Let us] remember that the data controller is responsible, [he is the person] who has the authority to tell you what is the purpose for which your data will be used later on, but then the data processor is the one [who is] doing the manipulation of it, whether it is distributing, et cetera, so [that] you have to separate the data controller who is focused on the purpose, from the data processor who then has control over actually manipulating and using that data. Does that clarify it now, in that regard?

Senator Miss C. N. DRAKES: Yes, Chair.

MADAM CHAIRMAN: If we are to move along from 55(1) with the conclusions we have come to, it then makes the section 55(4) the concern that is at the bottom of page 2. It just makes that null and void because they are not creating professions, therefore, that one is not relevant. Again, we are at the top of page 3, section 68(3) and (4). Where the concession is that there appears to make the Data Privacy Officer the Commissioner's spy, but paid for and maintained by a company. No, this is not the case, the Data Controller designates their own privacy officers and it is to facilitate core operation in the Data Subject's interest, so that, for example, the Privacy Officer is working for the Data Controller but in the interest of the data subject, so [that] the Privacy Officer is really there to take care of the Data Subject's privacy interest, and also they work with the data controller because they are making sure that the data controller's interests are served by complying, so [that] you have to distinguish between the data controller, the data privacy officer and the data processor, so [that] the data controller deals with purpose; the data processor is dealing with the manipulation of information, and the data privacy officer is there to make sure that the data subject's rights are served and to make sure that there is compliance with the Act. Does that now make sense to everyone?

(The Committee responded in the affirmative)

MADAM CHAIRMAN: That said, therefore, section 68(3) the comment made there does not have an impact on the Bill. Is that the understanding of the entire Committee?

Senator R. J. H. ADAMS: Madam Chair, that is my understanding but I do not know if that is helpful but when we wrote back and explained our reasoning to each submission, it struck me [from] reading this that there is a parallel to a compliance officer running KYC AML in a business and the data privacy officer is fairly strong parallel to that norm. I know when you give people these kinds of analogies that they immediately start to open a can of worms and so on but that is the way I set it up in my mind. I know I do not want to drag this out but that does seem to be fairly fair and it might be something that people can more easily grasp when we give them the explanation.

MADAM CHAIRMAN: Thank you. Now we move to section 73(1), that again is the section just below the middle of page 3. The contention here is that the last sentence appears to be glaring loopholes for mischief. If the Commissioner instructs his employees to release someone's personal information to one of their competitors, then, while it is clearly unethical, this clause appears to make it legal, and it is the clause they are referring to above, which I believe all of you [would] have read. I am going to ask Ms. Belle to speak to this matter.

Miss SHAWN BELLE: Madam Chair, this particular provision is very common when you are

dealing with functionaries, to impose upon them a specific obligation to keep things confidential, but you give them some leeway in relation to circumstances where they may have to, in this case, release information. Now, that is not to say that you interpret it to mean, and a court would see it this way, that he can do anything. He has to have in his mind the Bill itself and also other enactments, as well as any common law jurisprudence that has developed on the matter, as well as any customs and practice that may be relevant. It is not that the discretion is unfettered, he has to take all of those things into account and if he does not he can be challenged and disciplined under the Public Service Act because he is a public officer. I just wanted to make that point.

MADAM CHAIRMAN: With that said can we therefore, agree that this Section 73.1 as presented in this submission would have no impact on the Bill as drafted currently. That is agreed? Okay agreed.

Section 73.3, it speaks to, "A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or imprisonment for a term of 12 months, or to both." What is being suggested here is that there will be a minimum fine of \$500 000.00 submitted for this. I believe that this was discussed earlier and the fact that the law really and truly does not allow us to do a minimum penalty on anything and therefore this recommendation would not have an impact on the Bill if the Committee is an agreement with that. Agreed.

Now we are at Section 74," The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any 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 pursuant to this Act." Now again the suggestion here is that this seems to be an excuse for professional negligence and my perspective is certainly the idea of in good faith that that is the measuring stick and where that officer would act outside of good faith then they would be subject again as Ms. Belle said earlier to the Public Service Act as a public servant. Therefore I would say that this submission regarding Section 74 should not have an impact on the Bill as drafted. What says the Committee?

Senator Ms. A. M. WIGGINS: The only thing I would say there is what Senator Adams spoke of earlier serial offenders. What then would be the penalty if the person can be suspended or something of that matter? He wants to say that these persons should not be penalised because they are doing their job in faith, but sometimes people's information can fall off the back of a truck and as he said earlier a serial offender. I do not think you should give just like that, it should be built in mechanisms to protect people's data.

Senator R. J. H. ADAMS: Madam Chair I was just going to say in contrast to my prior comment about blunt instruments and scalpels, this seems to be a

processed question, and I am just wondering what is the legal test for good faith. I guess I am asking would a judge for example not look back and say did this person follow the process. Is that the test or does it have a special definition in the eyes of the law?

Miss SHAWN BELLE: Madam Chair, just to say that this is a common provision again that is put in place in terms of functionaries, because sometimes it is anticipated that functionaries can make errors, but they are acting in good faith and the good faith meaning they were following the proper procedure, they were following the Act as set out, they were following all of the relevant rules that pertain to the execution of their job, and so the Judge then would look at those factors to determine whether they are acting in good faith should it come before a Court. In terms of the Public Service Act, though, there are several mechanisms for disciplining a civil servant. Now the vernacular, I might be getting wrong, but there is the concept of like a lesser type of infraction versus a more serious type of infraction and the lesser types of infractions may attract a reprimand or whereas a more serious may go to the point of even rendering the person to have to be dismissed. There are a gam..... or toolbox of ways in which the Commissioner can be disciplined.

MADAM CHAIRMAN: Anything further on this item? Does that answer the question? Then again it appears then that Section 74 as we have just explained it should have no further impact on the Bill as drafted. Is that correct Committee?

Section 75.(1). *"The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct."*

MADAM CHAIRMAN: The question raised here is there a penalty for not submitting that report. I believe that was just answered. The Commissioner would be subject to the Public Service Act with regard to not executing their duties, and that then would apply in this situation and therefore this suggestion would have no further impact on the Bill. Is that correct Committee? We are in agreement.

With regards to Section 79.(1) and Section 85.(2). These are typos, and as we said typos happen and they will be fixed in the final Bill. It also speaks to copies of documents, sorry, that is Section 79.(1) in particular. Section 85.(2) however, speaks to copies of documents may be seized but the person should be allowed to make copies of materials seized is unrelated to the charge and as part of this business. Now, this is taken in the context of a warrant having been issued by a Judge, and I will let Ms. Belle speak to that, but if a warrant has been issued by a Judge, this idea that you get to take back things and photocopy them is not something that we would wish to do at this stage or at any stage.

Miss SHAWN BELLE: Madam Chair, the thing is that context matters, so the power to inspect and seize is within the context of a warrant. A warrant is a

special document, you have to go before a Judge and you have to lay out a compelling case for him to sit down and it allows the Commissioner or his staff and Police to come to the premises to search, to seize, and inspect the different part. Those are things that ordinarily would not be allowed to do, and so the copying of documents, I understand that maybe it is that there was a thought that maybe you need to retain something. But the fact of the matter is for it to get to that stage, this would have been a very serious infraction in terms of not cooperating with the investigative functions of the Commissioner. Note also that the Commissioner has within their toolbox the capacity to issue an information notice if it is that they need information. The thing is then at that point the person would not be in cooperation and that is why the Commissioner would then resort to seeking a warrant from the Judge. I just wanted to say that.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, while that is so, for it to reach a stage where a warrant has to be issued, the person would have to be not complying. I think the issue being raised here, is that the documents unnecessary for the continued function of the business or they are holding information belonging to a different...

Miss SHAWN BELLE: ... Madam Chair, again this is a lack of knowledge of how warrants function. When you go before the judge, you cannot be asking for information that is not related. It is going to be very specific as to what you are looking for and why, so this concept that you would be seizing just any material; no, that is not the case. You have to understand how warrants work.

Asides

Miss SHAWN BELLE: They would be looking for specific materials and the parameters would be carefully set out in the warrant.

MADAM CHAIRMAN: Given that education on the way warrants work and the fact that this may not necessarily be a major concern, before I continue let me give Senator Drakes the Floor before I wrap up, because it seems that you have a comment to make.

Senator Miss C. N. DRAKES: No, Madam Chair, I understand the concern which the submission has and I am wondering what the precedence is in terms of warrants period. I do not know if a lawyer in the room such as Senator Sands can explain. What is the precedence as it relates to warrants? What can and cannot be taken, and would that then speak directly to this section of the Bill?

Senator D. R. SANDS: Miss Belle actually spoke to it. All a warrant does is specify what the actual officer or commission is looking for, so in a practical sense let us base it on what this gentleman has put in the submission. If the person had all of their information on one sheet of paper, and I want information at Line 7 but all of my information is on this one sheet of paper, then we have a practical issue here which we have to deal

with. I cannot cut out the middle part and leave the balance; I want the document as a whole, so in a situation like that which is peculiar then we may find ourselves in an area of some confusion. However, in the normal course of things if it is File A or File B or File C, the officer would have a warrant speaking to the specific file which he or she is seeking to seize or inspect.

Senator Miss C. N. DRAKES: Madam Chairman, on that note what we are primarily talking about is soft copy. With soft copy you just need access, a password, where you then more than likely have access to all of the information. We are thinking of it in a very physical sense but given you were talking about data, if you need to seize information from my laptop, I have to give you the password to my laptop which then gives you access to all of my information. How does the warrant then apply?

Miss SHAWN BELLE: That is so extreme. A judge will not sit down and fling them like candy like that. You have to establish a case.

Asides.

Miss SHAWN BELLE: And there is an understanding of the fact that you are dealing with electronic information. Okay? This Clause comes from the United Kingdom, the Cayman Islands and those, so there is an understanding that it is electronic information but I just need to stress again: Extreme. Right? So a judge in order to give that type of an order would have to be persuaded by counsel or the Commissioner that there really is a case and there is really an infraction. Also, part of the warrant is almost like an injunction. You would have to say there is an urgency because the person might spirit away the evidence, so there is an urgency attached to that too. I just need to emphasise those points.

Senator Miss C. N. DRAKES: Madam Chair, thank you. I think Miss Belle is giving me more faith in the justice system.

Asides.

Senator Ms. A. M. WIGGINS: Madam Chair, can I say something possibly off the record?

MADAM CHAIRMAN: On the record for Hansard at this point in time.

Senator Ms. A. M. WIGGINS: I was just saying that she spoke to electronic issues, and everyone knows....

MADAM CHAIRMAN: If you want this to be off the record, then turn off your microphone.

Asides.

MADAM CHAIRMAN: That was Section 85.2. Given the extensive discussion and explanation we have had with regard to how warrants really work, do we see this Section having any impact on the Bill as it is drafted currently?

Asides.

MADAM CHAIRMAN: I believe that answer is "no", therefore we move on to Section 85.3, where it reads:

"A judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism, or for artistic or literary purposes unless the determination by the Commissioner has taken effect."

The question here is: What about educational institutions processing student records? Would they fall under that? I am again going to ask Miss Belle to speak to that.

Miss SHAWN BELLE: Madam Chair, it would not apply to educational purposes but just to say that Section 81 deals with the determination of the Commissioner as for the purposes of journalism or artistic or literary purposes. That exception – remember it is under an exception – is the one that is one that is going to cause the greatest challenge because persons are going to want to use the information for those purposes and you may need to drill down to make sure that they really fall within the exception. In short, it does not deal with the educational institutions and I would have to say that there would have to a directive to say that or a reason why you should also cover processing of student records. I do not recall it being something that other legislation dealt with.

MADAM CHAIRMAN: Any further questions on this? It seems as if it would not in any way substantively change the Bill as it is drafted currently. Is that the concurrence of the Committee?

Senator Miss C. N. DRAKES: Madam Chairman, if it was not under this Bill and this same scenario applied, would they be guilty of an obstruction?

MADAM CHAIRMAN: Yes.

Senator Miss C. N. DRAKES: Therefore, I think we can readily move on at your discretion, Madam Chairman.

Senator R. J. H. ADAMS: No dissenting voice, but I wonder again and I think about the response that we offer to these submissions and this just seems to be one where we say, we may say, we can revisit these levels of trying. If there are not deterrents then we will go back and look at it again but at this stage, why would \$500 000 be more of a deterrent than \$100 000, that part is not clear to me. It is a comment and I think we should respond carefully, except to that one about the ladder when we do reply.

MADAM CHAIRMAN: There are submissions, as we have been told - my apology, my microphone was not on – that we are expecting from the Bar Association and perhaps Barbados Association of Medical Practitioners (BAMP). I believe BAMP has already come and also the Bankers' Association and they are already here. I believe the Parliamentary team will send that out to us tonight as we would have agreed in procedure on Monday. We will reveal those on Monday and I would propose that we reconvene on Monday at 11:00 a.m. as opposed to 10:00 a.m. and at that time, whatever submissions would have been

received from all of the above, and I believe tomorrow is their deadline, again if I may repeat, then they will send it to us electronically. We can then review those on Monday and then prepare for the final report after that.

MADAM CHAIRMAN: Committee, thank you for your indulgence. I was having a conversation with regards to the submissions that have already been received. I believe the Bankers' Association have already submitted. The Parliamentary team will make a request of the others. Would they wish only to make a written submission or would they wish to make an oral submission on Monday as well. The Parliamentary team will get back to us because we are fine with a written and some may be open to also making an oral submission. If that is satisfactory to the Committee we will leave that option also for oral presentations on Monday.

Miss SHAWN BELLE: Madam Chairman, I am partial to just considering the written submissions. Remember that Chief Parliamentary Counsel if there are things that we have to follow up on, we have to do the work and if I am here, then it will be a problem.

MADAM CHAIRMAN: What is the word of the Committee? Please, everyone, make your voice heard.

Senator Miss C. N. DRAKES: Madam Chairman, I would also like to second that because, I think, even though given the experience this morning with the oral submissions, for instance, Mr. Morgan, he had some very good points, however, a written submission would have been better to sit down and analyse. If any amendments needed to be made there is a document you can refer to and if you are serious about the submission and if you are serious about any amendments that needed to be made to the legislation, I would rather us request written submissions.

MADAM CHAIRMAN: Are there any other voices? I really want to hear the other voices on the Committee.

Senator K. J. BOYCE: Madam Chairman, I would request the written submission.

Senator D. R. SANDS: I agree with both of my colleagues, I would require the written submission as well, Madam Chairman.

Senator Ms. A. M. WIGGINS: Madam Chairman, with great respect. Unless the Ministers have House of Assembly on Tuesday, I was just wondering if we could defer the Monday's session until Tuesday.

MADAM CHAIRMAN: There are other things on our schedules other than that and for me in particular I know that there is a major project that I have to work on that day.

Hon. Ms. C. S. V. HUSBANDS: Madam Chairman, I take the point that you need a written submission because when the person gets up and leaves, you want to have the information set out. My only thing, I did not hear a lot of it. All of you had the experience so you can say but I was wondering if it was not helpful having the person explain more of what they

meant because sometimes you may read something and you think of it in a particular way but when the person explains you get an understanding of what they are trying to get at but still have it in written so you can refer.

MADAM CHAIRMAN: There is one person for oral and written.

Senator R. J. H. ADAMS: Thank you, Madam Chairman, I am glad I got to speak last. I needed time to think about it. I think where if we know a submission is going to be a little contentious, for example, that Solutions Barbados submission, if Mr. Phillips was here and could explain...

Asides.

Senator R. J. H. ADAMS: I do not know Mr. Phillips but, for example, on the fines where a lot of misinterpretation has gone on, and we set out that no, actually that is not the way it works, I think we shut down the wrong expression, we satisfy the inquiry. I am tended to say that if it is contentious it is nice to give the person a chance to hear us out but it is not very good use of time overall. I mean if they do put in a written submission, I will hear you but I think they should express themselves pretty clearly and we can give them a response and if they want to come back again and open that up with a different question I guess we could respond again but that takes a certain amount of effort on their part that should focus their mind on getting it right the first time, so I think on balance I would go for the written.

MADAM CHAIRMAN: Okay. I as Chair certainly am open to written so I believe that the Committee... all except one is...

Senator Miss C. N. DRAKES: Madam Chairman, if we can have a middle ground, is there any way they can provide the written submission and there is an invitation update if they want to come and sit in on the closed session, is that allowed?

Miss SHAWN BELLE: Madam Chairman, I get it, you want to give people as much opportunity to express themselves but it was advertised several times on the radio and if you have a material in chest you would be here, and that is my view. The Chief Parliamentary Counsel wants to be cooperative but I am one person and I have to go back and analyse all of the information that I have received. Yes, you all have worked with me before with Public Finance Management Bill and it was like, *snap, snap, snap*, but I am one person.

Senator Miss C. N. DRAKES: Madam Chairman, if I could.

MADAM CHAIRMAN: I beg the Committee's indulgence for one second please, I am just getting a clarification on process. Okay, in terms of seeing how we might be able to have a middle ground, one consideration is that when we have the written submission for Monday, we go through that submission as a Committee and if in going through the submission we discovered that there are some things that we

definitely need to invite the submitters for, then we would have to consider how we might be able to do that. Would that work better for the team in terms of a middle ground?

The Committee in unison answered yes.

MADAM CHAIRMAN: Well, I think if I am to go the democratic route the majority has said let us take a written submission and only if there is need for us then to invite the persons or organisations making the submission, that we do that only then off record. I think the Committee has made its decision and the collective responsibility of all of us to say we are in. That said, is there anything further before we conclude?

Senator Miss A. M. WIGGINS: I would like to put forward a motion for this session to be adjourned and to compliment you, Madam Chairman, on your excellent chairmanship. I will also say, and it happens within the Senate when you are leading as well, that you always sum up so concise and so perfect. You summarise what people say very well. Can I say I admire you for that, and that is my motion?

Senator Miss C. N. DRAKES: Madam Chairman, I would like to say I second that motion.

THE AUDIO FEED ENDED AT THIS TIME AND THE MEETING WAS SUBSEQUENTLY ADJOURNED TO JULY 01, 2019 AT 11:00 A.M.

ENDS TRANSCRIPT OF THE SECOND MEETING OF THE JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, HELD ON JUNE 26, 2019, IN THE SENATE CHAMBER.

**THIRD MEETING
OF THE
JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, 2018
HELD IN
THE HONOURABLE THE SENATE**

MONDAY, JULY 01, 2019

First SESSION 2018-2023

PRESENT:

SENATOR THE HON. MISS K. S. MCCONNEY
(Minister of Innovation, Science and Smart
Technology) (Chairman)

**Hon. D. G. SUTHERLAND, M.P., B.Sc., M.Sc.,
M.B.A (Dist.)** (Minister of Small Business,
Entrepreneurship and Commerce)

**Hon. Ms. C. S. V. HUSBANDS, M.P., B.A. (Hons.),
M.Sc.** (Minister In the Ministry of Foreign Trade)

Mr. N. G. H. ROWE, M.P., (Parliamentary Secretary
in the Ministry of People Empowerment and Elder
Affairs)

Senator R. J. H. ADAMS, B.Sc. (Econ.), M.Sc.
(Political Sociology)

**Senator Miss C. N. DRAKES, B.Sc., (Econ. & Mgmt.)
M.Phil Econ.**

Senator Ms. A. M. WIGGINS, J.P., B.Sc.

In attendance:

Miss S. BELLE, Senior Parliamentary Counsel, Chief
Parliamentary Counsel Office

Mr. C. Coppin, E-Commerce Development Officer,
Ministry of Commerce and Small Business
Development

Mr. N. R. Jones, Deputy Clerk of Parliament

Ms. B. S. Gibbons, Deputy Clerk of Parliament

Miss S. Hamblin, (Library Assistant) Procedural
Officer to the Committee (Ag.)

Call to Order/Welcome

*Madam Chairman, called the meeting to Order at 11:35
a.m.*

MADAM CHAIRMAN: Good morning
everyone, I would like to call this meeting to order now
that we have a quorum. I would also like to welcome
today a student who will be visiting with us when you
see this person around the table. What is your name?

Miss C. Skeete: My name is Charlin Skeete. I
am a first year student at the University of Kent
studying international relations and politics and it is a
pleasure being here with everyone sitting in today.

MADAM CHAIRMAN: With the permission
of the Committee, I would like to ask that the student be
allowed to stay if there are no objections.

The question was put and resolved in the affirmative.

Minutes

MADAM CHAIRMAN: The Minutes of the
Meeting is the next item on the Agenda. I trust
everyone has had the chance to look at the Minutes for
our first meeting which was held on Monday, June 24,
2019. Are there any amendments to those Minutes?

There being no proposed amendments the Minutes I
would like to invite a motion for the Minutes to be
confirmed.

*On the motion of Senator R. J. H. ADAMS, seconded by
Senator Miss A. M. WIGGINS, the Minutes for the
Meeting of June 24, 2109 were confirmed.*

Matters Arising

MADAM CHAIRMAN: On the matters
arising, I would like to raise one matter. On page 4, the
third paragraph down, it is not numbered, speaks to the
fact that the proceedings will be streamed and I simply
want to enter for the record that at our meeting which
followed we agreed that we would stream the oral
presentations but the written considerations will not be
streamed but be done in our private meetings and kept
only for Hansard and internal purposes. That is just the
one adjustment matter that is arising. Are there any
other matters arising?

There were none.

MADAM CHAIRMAN: For today's
proceedings, then just to be clear, it will not be
streamed live to the public, we will simply be
considering as we did the written presentation last
Wednesday the 26th in the afternoon. Without further
ado, I would like to move into the next item on the
Agenda which is the Consideration of Written
Submissions. I would ask that we start first with the
submission from the Barbados Bankers' Association. I
trust that everyone has received the documents and just
as we did in the others we will go through
recommendation by recommendation looking at each
Clause and determining whether or not there would be
any impact on the Bill. I want to take this opportunity
because I know it has been a long time to just remind us
what are the terms of Reference of the Committee. We

are considering these submissions with a view of improving the protection of personal data to contribute to an ethos of compliance with data protection and to make any recommended changes if deemed necessary. Please recall that in our procedures. We had established dates for the Bill to go back to the Honourable the Senate and to go to the House of Assembly, the other place, and therefore we wish to stick to these deadlines and timelines to the extent possible and I would ask that we would see many recommendations that are aspirational, many recommendations that are very nice, and I would ask that we consider those recommendations that are absolutely necessary to ensure that we do no harm to improving the protection of personal data so let us look at what is absolutely necessary at this time moving forward.

In the consideration of the Bankers' Association let us start at the beginning. The very first recommendation speaks to Section 2 where what is being recommended is that the "financial record or position" not be included in the list of personal data deemed to be "sensitive personal data". As you consider this, I simply want to inform that the banks are already under the legal regime that is regulated by the Central Bank and that is for the management of data and consistent with the (GDPR), General Data Protection Regulations, on which this Bill is based, that GDPR does not actually include this as part of the "sensitive personal data" and given that there is significant protection already under the Central Bank of Barbados regulated regime I will be interested in your thoughts on this.

Senator R. J. H. ADAMS: Madam Chairman, when I read this I had trouble understanding what the definition of "financial record or position" and what would actually be contained in there because I find it hard to understand how what could not be "sensitive personal data". Are we merely saying that we are treating it twice under three sets of legislation?

MADAM CHAIRMAN: I will ask the Senior Parliamentary Counsel to speak from a legal perspective then.

Miss Shawn BELLE: Good morning everyone. Madam Chairman, just to say that there was no definition of "financial record or position" included and so it would be left to the ordinary dictionary meaning. It seems as if that this was a relic of a previous draft being the UK 1998 Data Protection Act which did include "financial record or position" but we do acknowledge that is not covered by the GDPR.

MADAM CHAIRMAN: Does any other Member of the Committee want to speak?

Hon. D. G. SUTHERLAND: Madam Chairman, I was checking my files and I do not have a copy of that document. I would like a soft copy. Can you send me a soft copy so that I can mark up my thing and make my notes, I do not like walking around with so much paper these days.

MADAM CHAIRMAN: A copy will be provided to you Minister.

Hon. D. G. SUTHERLAND: Okay, you can proceed. I will share with my colleague for the time being.

MADAM CHAIRMAN: The recommendation is that a "financial record or position" not be included in the list of personal data. Are there any strong thoughts about it?

Miss Shawn BELLE: Madam Chairman, just to say that the problem probably that the Bankers' Association would be having is that really and truly you are not supposed to be processing "sensitive personal data", at all, or except in very limited circumstances. So from the perspective of the Bank it would restrict them quite a lot in relation to their day to day transactions. It may be better for them to be under the normal personal data regime and that would still require them to submit to consent requirements, still require them to do their necessary checks to make sure that the data is not given for any purpose outside of what was agreed. All the different obligations that are set out in the Bill, so I do not think that there should be too much of a problem in terms of letting them be under the personal data protection regime, rather than the sensitive personal data regime.

MADAM CHAIRMAN: So, what I am hearing is that we do no harm? There is no significant harm that is caused to the Data Subject or to their rights by removing this in this way, but it simply does facilitate what would be the normal course of business in this particular sector.

MADAM CHAIRMAN: Is that what my colleagues understand?

Senator R. J. H. ADAMS: I am not sure I understand that. I just want a clarification on something. I am imagining a situation where, we get this already from Banks, we get tailored commercial offers based on our financial spending patterns. I think that is a good argument for, and I do not know if what Senior Counsel covers this, if it is covered well we can scratch everything I am about to say. It is a good argument for putting a wall between that kind of commercial offer and the bank maintaining records that it does not even profit from, so may be that could just be clarified for me.

Miss Shawn BELLE: The only answer I can give is that it is more rooted in the types of operations that the Financial Institutions would be in, and where it may be necessary to share within a framework. That framework can be adequately provided for under the protection for just normal personal data. It is just that "sensitive personal data" now is an extra layer of protection and really and truly it is that you are not really supposed to be processing it at all, and that is because of the extreme personal nature of it. So as you would have seen in the definition they would have had racial and ethnic origin, political opinions, and The *General Data Protection Regulations* (GDPR) would have included membership of political bodies, the genetic and biometric data. So these are things that are very specific, and very personal to the individual. The financial records even though that it has that

characteristic it may not need to be put to the same regime, but the personal data rules that exist including the data protection principles, all of that will still apply.

Senator Ms. A. M. WIGGINS: Madam Chairman, through you to CPC, what we want to find out is that currently the bankers hold personal data anyhow. How with the introduction of this Bill is this data going to be treated any different? Number one. Number two, as I said before currently if you go to one banking association to apply for a loan, and you lie essentially on the application form they already have your information from the credit union, from another existing bank, if you have a loan and all your data. How in fact, does this Bill now protect your personal data given that it is currently shared certainly within the Financial Services Sector?

Miss Shawn BELLE: Madam Chairman, Senator Wiggins, would have outlined one of the reasons why you would not want it then to be under "sensitive personal data", because "sensitive personal data" would prohibit you from doing that, that very thing that you just described. It would then render the operations of the bank in practical, so therefore what you do is then take it out of that definition and let it remain as "personal data". So that then there would still be under obligations to inform the data subject of any rights that may be infringed, but they would not be under the astringent regulation that being classified as "sensitive personal data" would do. Do you understand?

Senator Ms. A. M. WIGGINS: No, I do not. In fact, you know like you said they already do have access to this information, so are you going to say they are going to park this information, because again you have making an application for a loan or whatever service, you are inquiring from the bank. So you going to say that they are going to park the information that, because I think they also had access to some credit bureau information as well. So, I want to know how the different sensitive data from the different agencies that the bank has access to how in fact this Bill more or less gives the data subject some kind of protection.

Miss Shawn BELLE: As it currently stands, the "financial data record or position" is considered to be "sensitive personal data", which means that it ought not to be processed at all, except for certain circumstances as outlined in the Bill, and I think that that is Clause 9. Okay..... so the situations that you would have articulated like the sharing of information and so on that would not be allowed under the current regime. What I am acknowledging from the Bank is that, that would be impractical for their operational purposes, fine. What can be conceded is perhaps they need to be under less a stringent regime, which would be the personal data regime. So that it would not be "sensitive personal data" anymore, it would be just "personal data" in which case you would be subject to the ordinary rules that are stipulated in the Bill already, so the data protection principles would apply. You have to process the information lawfully, you would have to have transparency, you would have to have it fair, you

would have to include consent where required, and all the rights of the data subject would have to be observed. So there is no less protection to the data subject, if you reclassify the financial records as just personal data.

MADAM CHAIRMAN: Senator Drakes.

Senator Miss C. N. DRAKES: Thank you, Madam Chairman. Banks are raising this specifically because this is an issue for them. Taking the financial position from "sensitive personal data", if that is the case can we then also have the type of amendment where it is specifically for the banking sector or financial sector? It is not sensitive to them but it then becomes to any other organisation that may use it, let us say, in a malicious way, if you understand what I am trying to say.

Miss Shawn BELLE: Madam Chair, through you, Senator Drakes, are you proposing that there should be some special regime in relation to banks?

Senator Miss C. N. DRAKES: Or financial institutions, Ma'am? My financial position is known to the bank because of my relationship with the bank. My financial position is not open for use, or my data relating to my financial position is not open for us, let us say, for a supermarket or any other organisation outside of a financial institution. For me, I believe I would then classify that type of data as sensitive, for all other persons outside of the finance industry.

Miss Shawn BELLE: So, the problem with that then is... The current personal data regime will protect against that because yes, the banks would only share that information within a regime. so [that] if it is that they are trying to confirm your status in relation to a loan, that is their ordinary business and that would be protected under the personal data regime because you have to be processing for lawful purposes, transparency would have to be involved, fairness would have to be involved. But if you then put it as "sensitive personal data" they would not be able to do any processing at all, except for the circumstances set out and the circumstances set out may be too stringent. I am acknowledging that it may, in fact, be too stringent and so the personal data regime is probably better in that respect for regulating them and so what you would do is that you would take it from the definition of the personal sensitive data, you do not need to create a separate regime for them.

MADAM CHAIRMAN: I think we have to acknowledge and respect some of the concerns being raised. If I can draw your attention to Clause 9 which speaks to the processing of "sensitive personal data":

9.(1) "Processing of sensitive personal data shall be prohibited unless

(a) the data subject gives his written consent to the processing;

(b) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;

(c) the processing is necessary in order to protect the vital interests of the data subject or another person, in a case where:

- (i) consent cannot be given by or on behalf of the data subject; or
- (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject;
- (d) the processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- (e) the processing
 - (i) is carried out in the course of its legitimate activities by anybody or association which
 - (a) is not established or conducted for profit; and
 - (b) exists for political, philosophical, religious or trade union purposes;
 - (ii) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
 - (iii) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
 - (iv) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (f) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- (g) the processing is necessary
 - (i) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (ii) for the purpose of obtaining legal advice; or
 - (iii) otherwise for the purposes of establishing, exercising or defending legal rights;
- (h) the processing is necessary for the administration of justice;
 - (i) the processing is necessary for the exercise of any functions of either House of Parliament;
 - (j) the processing is necessary for the exercise of any functions conferred on any person by or under an enactment;
 - (k) the processing is necessary for the exercise of any functions of a public authority;
 - (l) the processing is necessary for medical purposes and is undertaken by
 - (i) a health care professional; or
 - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
 - (m) the processing
 - (i) is of sensitive personal data consisting of information as to racial or ethnic origin; and
 - (ii) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
 - (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- (2) The Minister may by Order specify circumstances other than those identified in subsection (1) where sensitive personal data may be processed.

(3) An Order made pursuant to subsection (2) is subject to negative resolution.

(4) For the purposes of subsection (1)(l) "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services."

MADAM CHAIRMAN: If you read that all the way through to page 26 it would give you the opportunity to see where you believe there is some further concern. If I may, we can simply pause for a few minutes to give Committee members an opportunity to just read through that, as you consider your response.

At this time the Committee is reading through the document.

MADAM CHAIRMAN: Senator Drakes.

Senator Miss C. N. DRAKES: Madam Chair, after we read through Clause 9, there is actually in 9.(1). (l) where the processing of "sensitive data" can be prohibited unless the processing necessary for medical purposes. I am just wondering if we can have some amendment then for financial institutions. Leave it under "sensitive personal data" but then just insert similar to what we have for the medical purposes. Ma'am, it is just a suggestion, if not we can move on.

Miss Shawn BELLE: "By or under an enactment". so that there are certain functions that they have under the various enactments and so that would give them the space [in which] to operate.

MADAM CHAIRMAN: In this case the enactment being the "Central Bank regulated and/or all other financial institution Act."

Miss Shawn BELLE: The thing is, this is generic so that you do not have to revisit it all the time but "the medical purposes" is very specific because of the sensitive nature of biometric and genetic material.

MADAM CHAIRMAN: Is there further clarification required? Okay.

Miss Shawn BELLE: Madam Chair, it is therefore my understanding that the Committee is satisfied that "financial records" remained defined as "personal sensitive personal data?"

MADAM CHAIRMAN: Is that the understanding of the Committee or that it can be removed and be treated under "regular personal data?"

Senator Miss C. N. DRAKES: Madam Chair, if the understanding is that the financial institutions can be accommodated under Clause 9.(1)(j), then "yes", we can keep it under "personal sensitive data"

MADAM CHAIRMAN: Are you saying that you keep it or [that] you remove it from under, because the proposal that is being made is that it be removed from being "personal sensitive data" and be treated as "personal data".

Senator Miss C. N. DRAKES: Madam Chair, if my understanding of CPC is that they can use the Clause under 9.(1)(j) then it can be kept under "sensitive personal data".

MADAM CHAIRMAN: Were you seeking to speak Senator Adams?

Senator R. J. H. ADAMS: Thank you Madam Chair. My concern here was that a bank could not take financial and pedal them to a third party and I saw in Section 9.(1)(e)(iv) that that is already covered, so my concern is a

Asides

Senator R. J. H. ADAMS: Thank you for this opportunity to repeat myself. My concern mainly was that a bank could not take financial and monetize them by selling to a third party. That is an important distinction, a wall should be between a bank and the records of its clients and that kind of commerce. Under Section 9.(1)(e)(iv), I can see that I do not have to worry about that because it is covered. If it were not on the sensitive..... I am happy to go along with the Banks' recommendation on the understanding that they would still not be able to do what I fear they might be able to do, because of Section 9.(1)(e)(iv).

MADAM CHAIRMAN: Any further comments? Yes.

Miss Shawn BELLE: I would just say Madam Chair that the capturing of the main functions of the financial institutions would be under Section 9.(1)(j) and it would also infer if you are complying with the enactment that you do not do things that are outside of the enactments contemplation including selling to third parties and so on. I acknowledge Senator Adams point but at the same time I think their operations would be more captured under Section 9.(1)(j). Just to reiterate the Bankers Association is asserting that the GDPR does not in fact classify financial information as "sensitive personal data" and they are asking for it to be removed. We are saying that I should stay as classified and their operations should not be inhibited since Section 9.(1)(j) allows the sphere in which to operate.

MADAM CHAIRMAN: Yes, agreed that it should stay under "sensitive data" and is that the opinion of the entire Committee?

Hon. D. G. SUTHERLAND: (*Indistinct Audio*).....and how people will respond to changes that we are making as a Government. I do not think that the global fit necessarily fits our culture as it relates to using banking information. I would want us to air on the side of caution with this one. We can hear from the bankers but at the end of the day then we have to cater to the consumer who utilise that banks and the businesses. Someone may interpret this as, "hi look, the bank can use my information for whatever purposes they care to", and indeed this will open a can of worms. Those who would have studied the Bill would think differently but not the average man in the street. Then you will have to go through a whole host of stakeholder consultations to explain and indeed I would say air on the side of caution here and leave it classified as "sensitive personal data".

MADAM CHAIRMAN: Well it seems that that is the consensus of the Committee, let us therefore

go by general agreement as oppose to a motion. I am instructed by the Clerk that this is an appropriate protocol, so we are then generally agreeing that it stays as "sensitive personal data". Yes that is for the record, it remains "sensitive personal data".

Next one, the credit reference to an agency. You will notice in Section 2, there is a definition for "Credit Reference Agency". However no place in the Bill does it appear. We would say that it can be removed therefore as it does no harm to the Bill. Is that the general agreement? Generally agreed also for the record.

Moving onto number 3, ensuring the reliability of employees that can access data, this is Section 4.(7), the Bill requires, "The data controller shall take reasonable steps to ensure the reliability of any employees of his who have access to the personal data." The recommendation is that to say that to ensure reliability is a bit vague and therefore that it should be some clarification. Having consulted with CPC, a clarification can easily be made without in anyway impinging on the procedural agreements we made at the very first meeting. If the Committee is in agreement, we can agree to make that clarification. Do we have general agreement? There you go. For the record, state there is general agreement to move forward.

Section 4.(9), that data can only be processed by a data processor under a written contract with the data controller. The recommendations is that a transition period for the implementation of the Bill would facilitate the need to implement new contracts and renegotiate existing contracts *et cetera*. We believe this can be done privately and it need not necessarily become an issue to include in this legislation at this point and that we can leave the matter as is. Are there further thoughts on this? It is on page 2, it is Section 4.(9). Are you able to see it? The matter is that this is not a matter for this Committee to consider at this point as it can be taken care privately. Is that the general agreement of the Committee or are there different thoughts? I believe that when the Bill is proclaimed there are these transition periods that can simply be built in at that point in time and therefore we can treat that in that regard.

MADAM CHAIRMAN: There being a general agreement we move onto number 5, the lawfulness of processing, that is Section 6. It says the processing of data is deemed to be lawful only in certain circumstances, one of which is where it is necessary for compliance with a legal obligation. Now Section 6.(1).(3) exempts obligations imposed by contracts, it is recommended that the exemption be deleted as unnecessary as it is a basic principle in law that persons cannot contract outside of the law. Basically the recommendation is to delete Section 6.(1).(3). That is the effect of the recommendation. Do you have any comment on this at this time?

Miss Shawn BELLE: Madam Chair, I think that this was included as a matter of caution. Let me just re-orient. I do not see the harm in deleting it, but I do

not see the harm in keeping it either, so it can stand because it is just a reiteration of the law.

MADAM CHAIRMAN: If there is anyone who believes there is no harm in keeping or deleting, I ask for your agreement that we simply keep it.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, just a question for clarification from the Chief Parliamentary Counsel. Is it not that a Data Subject can give consent? The Data Controllers and Data Processors cannot do it without consent, so I am not quite getting why they are saying to delete it. A person can give consent to their data being processed in a particular way, once they are consulted and they give the agreement, so I am not quite sure where they are going with this.

Asides.

MADAM CHAIRMAN: Minister Husbands, did you get the clarification you needed?

Hon. Ms. C. S. V. HUSBANDS: Yes, from Minister Sutherland.

Asides.

MADAM CHAIRMAN: That having been said, I believe it is the agreement then of the Committee that we simply keep it as it is doing no harm as it is now. Okay. With regards to No. 6 which deals with children, let us look at Sections 2 and 8. They are asking that the age be lowered to children under 16. Barbados is signatory to the United Nations Convention on the Rights of the Child, and it defines a child as 18 and under. I see no reason therefore why Barbados, which is signatory to this, should in any way change that. What is the thought of the Committee?

Asides.

MADAM CHAIRMAN: It seems as if the Committee is in general agreement.

Miss Shawn BELLE: Madam Chair, just to give clarification. The GDPR speaks to age 16, and then the Bankers' Association said that member states went as low as 13, I think. I believe that you still need to be aware of the international obligations to which we are party. Therefore I think it still needs to be 18 and under.

MADAM CHAIRMAN: So are we in agreement that we keep it to under the age of 18? Let it be for the Record. Moving on to No. 7, Section 9, under the heading "Processing of Sensitive Personal Data". It is suggesting that under section 9.(1)(a), the term "written consent" is used. However, this does not take into consideration – meaning that it be written – the various ways by which one can indicate one's approval or consent in this technological age. Some of us know that we can click "agree" and we can do many things that are not necessarily written but which still do confer consent. The recommendation is that we use "explicit consent" instead of "written consent". That is the

bottom-line of that recommendation. What says the Committee?

Senator R. J. H. ADAMS: Madam Chair, I just have one comment there. Is there any way that "explicit consent" can be defined as explicit by inference, for example? Does it absolutely have to be that I tick the box on the Internet or that it was written, or is it happening where the person directly answers the question?

MADAM CHAIRMAN: I will ask Miss Belle to respond to that.

Miss Shawn BELLE: Madam Chair, I saw their recommendation in terms of explicit consent, so they would be including anything where it would be inferred but it would be a strong inference that consent would be given. The problem with the reasoning, though, is the fact that you are talking about "sensitive personal data". You are talking about genetic material. You are talking about the same financial records, so you have to refer back to the definition of "sensitive personal data". The question therefore is: Would you not want to put it beyond a reasonable doubt that this consent had been given, and would you not want that the way in which you give consent beyond such doubt be in writing?

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I was not clear about the example given earlier. If it is a document on my laptop and I tick or indicate in the box "yes", is that not seen as "written consent", or does "written" mean only handwriting?

Miss Shawn BELLE: Madam Chair, it would mean that. Again, I reiterate the warning in terms of the particular data that you are talking about, which is "sensitive personal data". I acknowledge that there would be mechanisms of consent that could be given, in which case it would mean that if we are talking about "explicit consent" then I would have to try to put in a definition of "explicit consent". It could contemplate that where you are filling out a form and you use a tick or some other form that would indicate beyond a doubt that there has been consent given, I am just saying that I think the "written consent" aspect is generally because of the fact that it is "sensitive personal data".

MADAM CHAIRMAN: How does the GDPR treat to "explicit consent"?

Miss Shawn BELLE: Madam Chair, I would have to look into it a bit more but what the Bankers' Association is saying is that the "explicit consent" would be wider than the "written consent" so that it would contemplate what I just outlined: That if you have on a form a part of the field where you can indicate by a tick or something like that, then that would be explicit consent.

MADAM CHAIRMAN: Let me also say that we will be going in the direction of digital signatures, *et cetera*, and therefore, if we are talking about digital signatures and so on, we cannot constrain ourselves with regards to the means by which we do that. I would want to put this out there for the consideration of the Committee: That in determining whether or not we go forward with "written" or "simply explicit consent" and

then ask that a definition of "explicit consent" be made, that we bear in mind that we are moving into a digitally empowered future where other forms of plain writing will be a part of it. Any further comments from the Committee?

Senator D. R. SANDS: I personally believe that the "explicit consent" may be the way to go. However, I like the recommendation by Miss Belle, which is that you would have to put something in the definition so that we get a clear idea as to what we intend by "explicit". Without the definition it could be misconstrued and, as you correctly stated, Madam Chair, if we are going into the digital age ticking on the computer does not necessarily mean "written", based on the Bill we have now. We therefore could potentially have ourselves in a bundle of mess. So personally I believe that we need to flesh out the "explicit consent". I think that should be the way we go.

MADAM CHAIRMAN: Do I understand then that the Committee is agreeing that we should use "explicit" instead of "written" and have a definition for "explicit"?

Asides.

MADAM CHAIRMAN: Let the Record show that there is general agreement on that.

Asides.

MADAM CHAIRMAN: Moving to Recommendation No. 8 on Page 4, which deals with "The Right to Erasure". The point that is being made here is that when data is stored, erasure of all physical and electronic databases is done by the Controller and such processors could be difficult given that the data, for example, of a large, multinational bank would be in varying formats in databases in different countries on multiple system platforms. It can therefore be administratively challenging and may not be possible for some countries systems which are not designed to handle such data.

It says the banking system is generally not set up to erase customers and an individual's right to request the erasure of this data is therefore not a practical or viable request. In the event that this is kept that a transition period of at least two years would be required to facilitate. I am interested in the thoughts of the Committee on this one.

Senator Miss A. M. WIGGINS: Madam Chairman, I think, I could be wrong, one time you kept information for seven years and then, at that time we were doing the physical thing and then they were shredded. In a sense, that was a form of erasing. How does that now compare seven to two given that they say digital information is not necessarily erased at all because sometimes even if I send you a WhatsApp and close the conversation, it can be retrieved. How do we compare that according to what is being said here?

MADAM CHAIRMAN: Miss Belle?

Miss Shawn BELLE: Madam Chairman, in examining this submission, it seems to me that their main objection is based on the fact that it would be hard

to implement and you would need time to implement it but the fact of the matter is a core part of the GDPR protection is the right to erasure, therefore, I do not think they can use their operational status to delay or to deny a specific right that ought to be respected, therefore, they should not be allowed to use that as an excuse; their operational expense to be an excuse not to adhere to a data subjects wishes to erase.

Just to Senator Wiggins' point. While it is acknowledged that if you render into being an electronic document and that it is extremely hard to make it disappear, the fact of the matter is, for all intents and purposes there would be a standard. It would not be stated here but there would be a standard for what would be considered to be erased. If it is then that a person pursues to the extent that they make it re-emerge then the question is: what is their intent in doing so? Then the law will click in to decide whether you need to prosecute that person for trying to unlawfully obtain information that does not belong to them. That is how I would respond.

MADAM CHAIRMAN: Any further comments.

Mr. Chesterfield COPPIN: Madam Chairman, I would let this provision stay. I just see this as a way where the banks really do not want to go into any cost issues in terms of changing their systems but as is, I would let this provision remain and I do not see how. It would take some time to modify their systems but I do not see this as something we need to go into. Let the provision remain and let the banks get their systems in place.

MADAM CHAIRMAN: Senator Drakes.

Senator Miss C. N. DRAKES: Madam Chairman, I agree with the sentiments that have been shared in the way how we have expressed, we are in a digital era. I do not see how hard it could be, as Miss Belle from CPC stated. If there is a minimum standard where erasure exists for digital information it can be implemented.

MADAM CHAIRMAN: Senator Adams.

Senator R. J. H. ADAMS: I just wanted to agree with both Miss Belle and Mr. Coppin there. I think that it is not systems that drive the legislation. It is legislation that drives the systems and we are talking about giving people ownership or at least control of their personal data - I am not anti-banks - but rather than accommodating the banks. What strikes me in their submission and more than once is where it is possible to exclude work they are trying to exclude work. Now we want to have children under the age of 18 and adult starts from age 13. Just to be frank, I think the number point is we are trying to put in place privacy protection in a pragmatic way. I think, as far as we can make accommodation we should, but the real point is maybe their systems need to change rather than our legislation.

MADAM CHAIRMAN: Thank you. What I am hearing from the Committee is that we acknowledge it can be hard and it can be expensive however, it is going to be necessary for all of us to do our part in

transitioning, therefore, this recommendation with regards to Section 12 will have no impact on the Bill as drafted therefore there is no change.

Number 9 which relates to Section 15. It says that under this Section, data subjects will be entitled to receive the personal data they have provided to data collector in a "structured, commonly used, and machine readable format." Basically, what is being said here is that currently the data is not systematically organised in such a way as to make it easily retrievable in machine readable format and the recommendation is that in the GDPR on which this Bill is based that the right to data portability which is being able to receive it in that machine readable, structured and commonly used way that data portability only exists where the processing of data is carried out by automated means, meaning that unless it carried out by automated means they should not have the obligation of providing it in any machine readable format. Basically you have to digitise the records in order to be able to share it in a machine readable format. That is the bottom-line here and it is recommended that there will be some special consideration in this regard.

Miss Shawn BELLE: Madam Chairman, just to say that I will concede this point. When you go back to the GDPR, what would have happened is, the first Subsection of 15 would have been put in and then the first part of the article from which it was derived. That is where it was put, but then in the second sentence which starts in Subsection 2 had the, I guess, the conscription or restriction that is set out in A and B. When you look back at the original Article, the A and B should also apply to subsection 1 so I will concede that.

MADAM CHAIRMAN: What would be the effective impact on the Bill as drafted?

Miss Shawn BELLE: It would bring this part of the Bill into an agreement with the GDPR as it was meant to be represented.

MADAM CHAIRMAN: Whereby, therefore, the data subject's right to data portability would exist where the processing of the data is carried out through automated means which means it may be digitised somewhere in an electronic format. Is that correct?

Miss Shawn BELLE: Madam Chairman, what would happen is that you would have up to readable format and then you would say where – this is rough drafting – and then you see the 9.(a) and (b) in (2) that would be placed in (10) as well.

MADAM CHAIRMAN: Are the Committee Members following? So basically there is no harm that is done to data and in fact it improves.

Miss Shawn BELLE: Yes, Madam Chairman, I think that is really what the GDPR meant. So therefore, I will do the amendments to suit.

Senator R. J. H. ADAMS: I am not sure I followed everything. I am reading this and I am just wondering if this is... Okay, I will put this the kind way. If they have a new client, come on, will the bank be obliged to store that new client's personal details in a machine readable format? That is the kind way. The

unkind way is, is this a get out for them not to abide by the idea of portability whatsoever?

Miss Shawn BELLE: Madam Chairman, just to say in this case this is not an escape mechanism from the Bankers' Association, it is actually a recognition of what the GDPR actually says so let me go back to the original GDPR Article 20 and just read how it is supposed to be implemented.

"The data subject shall have the right to receive personal data concerning him or her which he or she has provided to a controller in a structure commonly used and machinery readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data had been provided where (a) the processing is based on consent pursuant to point (A) of Article VI and it goes on – and/or on contract pursuant to Point B of Article VI and the processing is carried out by automated means Now, what I was trying to point out was that the current subsection 1 represents the first part of the Article when in fact both the subsection 1 and subsection 2 are supposed to be subject to (a) and (b).

MADAM CHAIRMAN: They should have been taken together.

Miss Shawn BELLE: yes.

MADAM CHAIRMAN: With that said, it would simply be moving this in compliance with the GDPR which does not further harm in this regard and in fact better explained and makes it easier in terms of implementation. Is that correct?

Miss Shawn BELLE: Madam Chairman, yes. The other thing too is that what I can do, I mean it is going to make an extremely long sentence, but I can combine 1 and 2 in the same way that Article 21 does and then subject it to 'a' and 'b' and that would be in line with the current Article 21.

MADAM CHAIRMAN: Senator Adams.

Senator R. J. H. ADAMS: Thank you, Madam Chairman. I just want one clarification. I understand all of that but the key point was where that data is provided in a machine readable format, what I am imagining is supposed the banks continue to collect all of this data on paper and we want to digitised a lot of this process in the economy and so on, this is the point of clarification, will they be able to do that or is there some – I know we cannot impose a process on them but at the same time if they do not start to digitise some of their processes there is no point having this kind of provision in the legislation.

Miss Shawn BELLE: Madam Chairman, I must confess that in order to break that kind of an issue I would need expert guidance because I am a drafter there is a limit to how much I can understand how it would affect practitioners on the ground so that is the type of question that is being raised by Senator Adams and I cannot without doing research answer it.

MADAM CHAIRMAN: Senator Adams, my understanding is that we are moving towards a more digital world and what is happening is that you are imagining that if this Clause were changed in the way

that it is recommended it gives and out for people to choose not to process their records digitally or electronically be able to keep them in paper and say oh, but this does not apply because I process in paper format. Is that what you are saying?

Senator R. J. H. ADAMS: That is one-half of what I am saying and the other half is: let us suppose it is on paper, it is not digitised, can a data subject still request the same information?

MADAM CHAIRMAN: In a digital format.

Senator R. J. H. ADAMS: Or on paper.

Miss Shawn BELLE: Madam Chairman, It is also recognised in that in the exemption part of the Bill there is reference to manual data which is really a reference to paper-based data and that is acknowledged to be an exemption to the processing requirements under this Bill.

MADAM CHAIRMAN: So that does provide an escape then that we can do it which is precisely what Senator Adams is saying that it can be used as a work-around' in order not to have to comply. That said, Committee, will we recommend that the structured commonly used in machine readable format remain a part of the definition and not change it in any significant way at this point in time to speak to portability that exist where the processing of the data is carried out by automated means? In other words are we going to permit this recommendation to have any impact on the Bill as it is currently drafted?

Senator R. J. H. ADAMS: Madam Chairman, let me make just a small suggestion there. They have suggested transition periods for other areas where it suits them. This might be one where we can elegantly capture... They are going to have to do it and see the light of day.

Hon. Miss C. S. V. HUSBANDS: That was the same point that I was going to make ... a transition period because we should be encouraging everybody in the country to put things in digital form so a transition period should be enough, two years/three years, to get it done.

MADAM CHAIRMAN: My understanding then is that there is general agreement that the Clause should remain as it is and simply seek to make accommodation if we can in a transition period.

Moving on to Number 10, the "transfer of personal" data where we are speaking to Sections 22 to 25, or Clauses 22 to 25 of the Bill. In terms of "transfer of personal data" outside of Barbados: personal data may not be transferred to a country outside of Barbados unless the country provides for an adequate level of protection for the rights of data subjects or (b) they are appropriate safeguards and legal remedies and data controllers and data processors develop very detailed, binding corporate rules. Seeing that under the GDPR data may be transferred to a country that has an adequate level of protection as determined by an authority and that is approach should also be adopted and therefore it is being recommended that the Data Protection Commissioner would have a list of countries for example, deemed to have an adequate level of

protection and this would prevent the individual companies the data controllers and processors from going out there and having to do their own research on the laws and the safeguards *et cetera*. I am interested in hearing the Committee's thoughts on the recommendation that it be the Data Commissioner that would then put together a list of some kind, rather than before it would trigger the Data Controlling, Data Processor to demonstrate that appropriate safeguards are in place, *et cetera*.

Senator Miss. A. M. WIGGINS: Madame Chairman, I just want to make some statements. It may sound like I am rambling on this one, but how does the fact that with the same banking institutions, a lot of their headquarters are actually located in Canada, England or whatever. So technically speaking even though you go into the bank next door your information in fact is residing somewhere else. So in truth and in fact have you the Data Subject, given permission to move the information, because you see we are dealing now with online, and e-transactions. I just want it clarify that in terms of e-banking essentially, how does this Bill impact on e-banking specifically that again is already going on? Similarly, with telecommunications companies your information, people call you from Japan, and say I am calling in connection with your bill, it is not paid. So essentially your information is already outside of Barbados. Did you give permission for that to be done and then of course under the Foreign Accounting Tax Compliance Act (FATCA) Rules, you got to surrender this information. So, I just want CPC, through you Madam Chair, to elucidate on how those international Rules and Regulations would impact this so called permission given for your personal data.

Miss Shawn BELLE: Madam Chairman, what this Bill is designed to do on inspiration from the GDPR is just to basically refine how that is done. So, it is not preventing the bank from sharing the information, but just that they ought to ensure that they follow certain rules in relation to the sharing of that information. Basically, under broad terms that they are adequate protections and there is another limb that they are supposed to adhere to, but those two basic limbs. Then those two limbs are then fleshed out in the following provisions that would be in relation to the adequate safeguards and in relation to the other one. Right. So that is how then their operations would be curtailed. The thing is, what they are asking is whether there should be an authority to say okay, these certain Countries are safe and these other Countries are not. It is in line with a submission that was made by Solutions Barbados in which they were stipulating that they should have a schedule with the Countries set out and they were saying that, that would not be a practical solution.

Having the Commissioner speak to it is not something that is out of the realm of possibility, but my only issue with the bank is the reasoning for why there are saying that they cannot have it. That they want a commission to do that, because they have most of them, the resources to research other jurisdictions on their own.

So, why should you then impose obligation on the part of the Government to step in and do that regulation, so that is my only thing. In the context of the GDPR, I think they were actually trying to point to the fact that the European Commission has some say, but it is not that the Commissioner in this context, Data Protection Commissioner, cannot say what Countries would be doing that, but again you would probably have to do in the form of a guideline or a code. My issue is the reason why they would want to have it, especially where they have the resources to actually do the research themselves. It would mean that the Government would have to take up that expense.

MADAM CHAIRMAN: Thank you. Minister Sutherland.

Hon. D. G. SUTHERLAND: I am seeking a little clarification here to you Miss Belle, the whole GDPR and when I read that paragraph under the European Union (EU) the GDPR data may be transferred to a country that has adequate level of protection, what is that? What is an adequate level of protection? How is it defined, because we may be looking at the adequate as being define as how we define it under section 22 and 23? So, again we still have to understand the reason why the bank is seeking this change for us to make a general adequate level of protection, and how it is define by the European Union (EU) is critical.

MADAM CHAIRMAN: Before Miss Belle, specifies I would like you all to look carefully at the final paragraph it says only in the absence of an assessment by the Data Protection Commissioner, would the banks then be required to demonstrate that there are appropriate safeguards in place. Then the final sentence goes on to say and, "It should not be mandatory requirement for every Data Controller seeking to transfer data out of Barbados." So, I just want you to read very carefully what that final paragraph says. Sorry about that. So be very careful about making this adjustment because it is very explicit what the intention is in this final paragraph. Miss Belle.

Miss Shawn BELLE: Madam Chairman, noting your intervention, I just want to speak to the principles that are governing the transfer of personal data out of Barbados. So the general principle is that the personal data shall not be transferred out of Barbados, unless that Country provides an adequate level of protection for rights and freedoms. They provide an appropriate safe guards on condition about the rights of the Data Subject are enforceable and there are legal remedies for those Data Subjects. Now, in terms of the adequate level of protection that is spelt out in 23 and that Clause 23 is informed by Article 45 of the GDPR. In terms of the apart the appropriate safeguards those are spelt out in Article 46 of the GDPR. When you look at the breakdown in Article 23 in terms of the adequate level of protection this is what they are asking for the Data Commissioner to give guidelines on whether they have the nature of the personal data, the Country of origin of the information contained, the Country of final destination of that

information. Purposes for which and the period during which the data is intended to be process. The law enforced in the country in question, the international obligations of that Country, relevant codes of conduct and the security measures. In terms of the appropriate safeguards, they want to know the legally and binding enforceable instruments, binding corporate rules, standard data protection clauses, contractual clauses and provisions thereto in relation to the transfer of personal data. You would notice in the appropriate safeguards that the standard data protection clauses are prescribed by the Commissioner already, with the approval of the Minister, and the contractual clauses are already stipulated to be authorised by the Commissioner, as well as provisions that would be authorised by the Commissioner in relation to protecting the data subject's right. So [that] there is already intervention in relation to the Commissioner giving approval in relation to certain matters, but as to the general matters of the international standards, those are things that they can do on the ground because they have the resources to check on those things. I am just saying...

MADAM CHAIRMAN: Minister Husbands.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I was looking at it just a little bit differently. I understand the point about the bankers having the capacity but it seems to me that there is a wider application here where, for example, a hotel has acquired a marketing agency overseas to do some promotions in their area to get more business for them and the marketing agency needs to have a sense of the data base of people who [would have] already come to the hotel, where they came from, that type of thing. [for them] to then plan out a strategy to deepen in that particular area where those people came from and therefore has [to be] passed. I think the Commissioner having a list of approved places that anybody can accessed, rather than each entity having to go to the expense of doing the same research, the Commissioner having it in one spot where you can access it, I think [that] would be important.

The other matter that came to my mind in looking at this was going back to the point made by Senator Wiggins which is, when you have branches and headquarters somewhere else, if the data is gathered in Barbados but because it is part of a central system, it is now accessible by somebody outside of the country, does that require this process or is it deemed that once the information is given to the institution, regardless of where the institution is located, that it has been given to one institution, because that is going to be a big issue for a number of entities who have branches. I just wanted to be clear what the legislation is suggesting.

MADAM CHAIRMAN: Miss Belle, I know that the legislation speaks to that in some way, so I will let you address it. If you need a little time to find the specific clause that is fine. I just want to comment, there are some efforts that may not necessarily be best taken on by any local, national or domestic data protection officer but there may be a regional approach to being able to say, okay, these are the jurisdictions, there may

be an international body that helps to establish that this is the case, as opposed to having it on a small island's data commissioner to have do that, so I thought I would put that out for the consideration of the Committee, that this may not be the only way to do this, [that] there are more than one way to skin a cat, and that if we could bring collective resources, international, regional, to bear, [that] that could make it easy for all of us. So I just thought that I would put that out there, knowing that this may not be the only option before us, but [that] we can think outside the box.

Senator Ms. A. M. WIGGINS: Madam Chair, just for clarification from anybody, in terms of the region, [does] any other Caribbean country have the Data Protection Bill? If so, how does that compliment? And those who do not, in terms of sharing information? Let us say within the aspect of CARICOM where there is free movement of people within the region, I just wanted to know how you reconcile all this information. Let us start within CARICOM, if Barbados and other CARICOM nations do not fall under this Act as well.

MADAM CHAIRMAN: I am going to ask Mr. Coppin to respond to that.

Mr. Chesterfield COPPIN: Madam Chair, Trinidad and Tobago in 2011 would have added data protection legislation in place but I suspect that since the introduction of the GDPR that they would have to relook those provisions. Jamaica withdrew theirs from Parliament two years ago because some of the provisions were encroaching on the constitutional rights of the individuals, so that those are the three jurisdictions that looked to do anything as far as the data protection legislation is concerned.

MADAM CHAIR: [Let us] remember this is new, it was only last year that the GDPR came into effect and so we are barely a year into this and they would have had a couple of years before. May I also ask Mr. Coppin to continue?

Mr. Chesterfield COPPIN: Yes, but let us remember that some time before, I think 2010, where we had the HIPCAR Project with the harmonization of legislation within the Caribbean but that did not go as well as we would have expected because certain countries did not want to go that way in terms of harmonized legislation and so on, so that did not come to fruition but I think somewhere along the line we have to seriously consider the harmonization of laws within the Caribbean when dealing with these particular matters, that is the only way that I think we are going to have any meaningful outputs as far as these things are concerned.

MADAM CHAIRMAN: I am glad you say that because I think as part of the single ICT space that has been put out there as some of the considerations that we need to make as a region. Senator Adams.

Senator R. J. H. ADAMS: Thank You Madam Chair, I just want to make a couple of general comments on this one. I am actually surprised [that] we would get this from the banks. We know they have a constant fight with knowing your customer as AML's legislation and I think there is an overlap here. There is

no shortage of cases where banks have been fined, threatened with loss of license because they have not had good processes - in some cases it has been deliberate, in other cases it has been accidental - to understand who is doing what in terms of respecting KYC and AML legislation, so insofar as this overlaps with that, I think it helps them and actually helps the country since we have such a great dependence on financial services generally. I think as a point of principle now on a data commissioner producing a grey list, black list and what-have-you - we mentioned this last time - this is not good practice. There are 198-something countries in the world, you cannot reasonably ask for a blanket escape-from-jail card if you get it wrong and lay it on the Data Commissioner. They know where they operate, they must, through the KYC and AML demands on them, have a pretty good idea of what the legislation looks like. They have compliance teams, legal teams, they got I would say more than any other sector the means by which to make this work for them and not treat it just as bureaucracy but as something that can help them to do their job better and the country also. So I would certainly not be in agreement that a commissioner or someone on the Government side has to produce this list, they know where they operate, we do not, and it is reasonable for them to carry the responsibility and accountability just as they do for KYC, AML and counterterrorism financing.

MADAM CHAIRMAN: Minister Husbands.

Hon. Ms. C. S. V. HUSBANDS: Madam Chair, I just wanted to support what Mr. Coppin was saying. The challenge in CARICOM, however, is that people do not have the in-house resources to do this type of work, they may not have the money and the time, but one of the goals of CARICOM and certainly Prime Minister as lead responsibility for CSME really needs to get harmonization around as many things as possible. The challenge that we have is that if there is no compliance with these things, the region will get a financial lash. Going back to the issue of the data protection commissioner being able to provide the list, I think that idea that you put, CARICOM could share that cost of maybe doing the research, because you could always look to see if there is funding that you could apply for from the EU to do this, a new funding. There are ways in which you can have a common portal where all of the information would be that would allow that compliance because if a hotel slips up, if another entity slips up the cost to us is thing..... I agree the banks may have the resources to do this, but the banks will not be the only persons that need to comply, so it will be safer for the country I think if there is a common list that people can quickly go and look and do the right thing straight up.

MADAM CHAIRMAN: Thank you. Minister Sutherland.

Hon. D. G. SUTHERLAND: Thank you Madam Chair. When I listened to the and I am not being too political here, but when I listen to the Prime Minister with respect to the digital age and with

respect to where we are in the Caribbean region, and I heard Senator Wiggins question while I was outside as to how many countries indeed have the necessary legislation and regulation that we are speaking about with respect to referencing the CARICOM. I would not want us to in no way be afraid to make bold steps, because if we begin to look at the banks questions, yes, and seek to, I would not want to say bend our legislation, I do not want to say amend but bend or legislation to allow the banks to function effectively in their own sphere as oppose to what is right internationally and also regionally and to set certain standards. While we go through this legislation that is where we have to pitch and also when we are debating it, and I actually love Senator Adams questions as it relates to what is in it for the bank and if what is in it for the banks speaks to global and internationally recognise ICT standards whether they are GDPR or whether they are other standards. We therefore when we sit her, thanks to CPC for brining clarity to a lot of the questions posed, do not just allow us to look at it from the bank's perspective only. They are other stakeholders, they are businesses, they are traders engaging in legal commerce in his region and internationally, so that is the question I still would like the answer whether adequate level encompasses what the bank is really asking for us to amend.

MADAM CHAIRMAN: I think you were outside of the room Sir when the reference was made to the several clauses that speak to that and if for the benefit of all.

Hon. D. G. SUTHERLAND: I do not want us to waste time going back, but once it was clarified I can always.....

MADAM CHAIRMAN: It was clarified.

Hon. D. G. SUTHERLAND: Okay no problem, I do not waste time just for..... and I guess the Committee is satisfied that.....

MADAM CHAIRMAN: With that said I think given all of the submissions we are in general agreement that the Bill should not be impacted by this recommendation that things will remain as they are now. Moving onto number 11, the "Binding corporate rules". Basically what it says is that this Section 25.(1)(c), specified that, their legally binding both in and outside of Barbados and that the reference to outside of Barbados should be removed as an entity cannot specify the legal effect of its rules in other countries.

Miss Shawn BELLE:exist in the GDPR under the transfer of data outside of the country, so that you would not be able to remove outside of Barbados in this context. Additionally, the entities should be giving additional..... I guess the structure of the "Binding corporate rules" is to give additional protection to personal data because of the fact that you are transferring it out of Barbados, but it is based on the relationship between the companies. My thing is that perhaps, the constriction or the restriction should be that this should be a clause that applies to legal persons only and that that would be the only specification, but in

terms of them saying you should remove outside of Barbados, that would not be in line with GDPR.

MADAM CHAIRMAN: Okay, with that said, it is not in line with GDPR, it does no harm right now and it creates no significant benefit to change it. Therefore, is the Committee in agreement that it remains the same and will have no impact on the Bill. Okay, there is general agreement for the record.

Moving onto to number 12, there is a legal professional privilege, this is Section 40, for those who want to jump here, it says "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." It is suggesting that this should be widened to include information in respect of which a duty of confidentiality is owed by a professional legal officer to a client or the advisor. Ms. Belle do you want to speak to this?

Miss Shawn BELLE: Madam Chair this is a specific exemption that appears in a number of jurisdictions where the concept of legal professional privilege is understood, and so therefore it is my recommendation that you do not touch it and that there is no need for a widening. The banks especially knows better than that.

MADAM CHAIRMAN: I believe the Committee is in agreement therefore that this should have no further impact on the Bill. Moving onto number 13, registration as a data controller and data processor. It is recommended that persons who process personal data solely for reasons set out in Part 5, which is exemptions, should not be required to register as a data processor or data controller. If it is that you are processing personal data solely of for the reason of all of those exemptions that you then should not have to register as a data processor or data controller. What are the thoughts of the Committee?

Senator Miss C. N. DRAKES: Madam Chair, just for clarification, because I think we mentioned this in another Sitting. But if the person processing the data is part of staff administration then the company would be registered. Is that not the intent of registration? Because what I am thinking that is being asked here is, if they have let us say 40 staff members for processing data, then 40 people have to register. However, I think it should be the company that should be registered and then that gives privilege to those staff members who are processing the data.

MADAM CHAIRMAN: Miss Belle.

Miss Shawn BELLE: Madam Chair, it is really supposed to be the entity that is regulated and it does not apply to the employees. Now it may not be directly specified with the data controller but certainly the data processor, since it says 'other than than the employees'. That is one aspect, and I think that any court which would look at it would interpret it that way. The other aspect of it is the processing for reasons in the exemptions. I think that there is a misunderstanding conceptually here, and I just want to be able to say that in terms of personal data being processed for individual

use, this is already covered by the legislation; it is covered in Clause 41. The kind of recommendation put forward by the bank I am not really understanding, because you already have that special protection for those people who are processing for personal reasons.

MADAM CHAIRMAN: Does any other Committee Member see any reason why this Clause should be changed? It seems as if there is general agreement, therefore, that this particular recommendation should have no impact on the Bill as drafted. Moving along with "Appropriate Technical and Organisational Measures". This relates to Clauses 53, 58 and 62. This recommends that the Data Protection Commissioner be required to issue Codes of Conduct, and that these Sections should provide that adherence to such Codes of Conduct be capable of demonstrating compliance with the abovementioned obligations.

Miss Shawn BELLE: Madam Chair, I just wish to say that Clause 71, Paragraph (r), provides for the Data Protection Commissioner to prepare appropriate codes of practice for the guidance of persons processing personal data. It already provides for the issuance of codes of practice, and additionally in terms of compliance the Commissioner is empowered to impose administrative penalties in relation to the same Clause 62 where they point to adherence to imposition of organisational structures, *et cetera*. The Bill already provides for protection.

MADAM CHAIRMAN: Is the Committee satisfied that the provisions under Clause 71(r) satisfies us and therefore shall have no impact on the Bill as drafted?

Asides.

MADAM CHAIRMAN: Let the Record show there is general agreement that this shall have no further impact. Now we move on to No. 15 under the heading of "Data Privacy Officer". It says that the Data Privacy Officer must have expert knowledge of data protection law and practices, and must report directly to the highest management level. The banks are submitting that they "may need to contract data privacy consultants and hire or identify and train Data Privacy Officers to facilitate implementation of the provisions of the Bill". They are also saying that it should be made clear that the Data Privacy Officer may be assigned other tasks and duties which do not pertain to the Bill, so long as there is no conflict of duty.

Asides.

MADAM CHAIRMAN: Agreed. It goes on to say that a transition period of at least two years is necessary to facilitate implementation.

Asides.

MADAM CHAIRMAN: It seems to me that the Committee is agreeing that this should have no further impact on the Bill as drafted, that this is an

internal matter which can be dealt with and does not need necessarily to be part of the legislation. Let the Record so show. No. 16 is "Functions of the Commissioner". The suggestion here is that the Commissioner should also be empowered to issue advice to Data Processors and Data Controllers upon request, and that their functions should include a mode of Codes of Conduct. I think we dealt with this earlier. The Data Protection Commissioner is already empowered to provide those codes. It is simply a matter of whether or not they can give advice to the Data Processors and other Data Controllers. There is no difficulty. Therefore, this should also not have any further impact as we believe it is already dealt with. Is that correct? Let the Record show that there is general agreement.

No. 17 is "Warrants". It reads: "A warrant can require any person on the premises to provide an explanation of any document found on the premises. This is not feasible or practical." This is the submission that is being made, and it adds that the person asked to explain the document should be duly authorised in writing. I would recommend that this has nothing to do with this particular Data Protection Act. The internal policies of a company we understand, and I think we had that in our previous submissions. We understand how warrants work in Barbados, and that the procedures and protocols that go with warrants we really and truly cannot speak to what the organisations do in response to a warrant. That is entirely theirs. Should I agree that No. 17 shall have no further impact as it relates to Clause 85 of the Bill? Let the Record show such.

Moving along to No. 18. We are almost at the end so hang in there. It is under the heading of "The Administrative Penalty". It reads: "It is recommended that the Bill clarify that if a Data Controller or Data Processor for the same or linked processing breaches several provisions of the Act, the total penalty should not exceed \$50 000." I believe in our last discussions we made agreement that we would keep the penalties the way they are and there was going to be no further adjustment. Consistent with that decision, therefore, this recommendation at No. 18 shall have no further impact on the Bill. At No. 19 is "The Processing of Historical Data". It says that the Bill has no grandfathering provisions for personal data. My understanding is that there is no retroactive piece to a law, so I will ask Miss Belle to speak to that because this, I believe, should have no further impact. However, I will let Miss Belle represent that in the appropriate way.

Miss Shawn BELLE: Madam Chair, what the bank is asserting is that somehow legal obligations would have a retroactive effect, in that they would result in them having to comply with something that was not the law at the time. That is not how laws are construed or interpreted. Usually, laws would not be interpreted in a retrospective way. The only way that can happen is in expressed circumstances, and usually it is in the context of a benefit. For instance, if it were that you got a tax exemption or some kind of other concession that is where it would retrospective. You

would see that in an Act like Duties, Taxes and Other Payments where that has retrospective effect, but in relation to legal obligations, criminal liability is tax liability and fees liability, and imposition of duty is under an Act. That would not be interpreted in a retrospective way.

MADAM CHAIRMAN: So if I understand you correctly, you can have a retroactive benefit but you cannot have a retroactive penalty or liability.

Miss Shawn BELLE: Exactly.

MADAM CHAIRMAN: Okay. Understood. That being the case, this recommendation really will not impact the Bill. Are we in agreement?

Asides

MADAM CHAIRMAN: Let the Record show general agreement. No. 20 is "Employee Data". It states: "*Businesses that do not process large amounts of customer or vendor personal information are still likely to process the sensitive personal information of their employees. Those businesses will have to register as Data Processors and Controllers and meet the requirements of the Bill. It is recommended that given the likelihood of business disruption and increased costs, persons who also process personal data as part of staff administration should also be exempt from registration.*" I believe we dealt with that earlier.

If all employees are required to register and comply with the Bill, clear guidelines, training and education should be provided to all businesses trade unions and members of the public to assist with their understanding of the Bill. A generous transition period is required to facilitate the above. I believe that we spoke in our last meeting about the need for public education and the need for us to use that period when we proclaim before it actually comes into effect. While it does not fit squarely within the Bill as something to be legislated, we did acknowledge that there would be a need for public education and for some trading and upscaling in this regard. That said, if the Committee is in agreement number 20 should have no impact on this Bill as drafted. Is there a general agreement? With that said, let the records show that number 20 shall have no impact.

"Liability of data controller and data processors". It is recommended that the Bill specify whether the data controller or the data processor is liable for the damage caused by processing which infringes the Act. The Act should also explicitly provide that data controllers and data processors are exempted from liability if they are not in any way responsible for the even giving rise to damage. I know that the GDPR has a provision for it and I would like Miss Belle to speak to that please.

Miss Shawn BELLE: Madam Chairman, just to say that you can put in a provision so I do not have any problem providing it.

MADAM CHAIRMAN: Would that provision in anyway impact our procedural timelines?

Miss Shawn BELLE: Madam Chairman, I do not believe so. I think the GDPR has a basic structure and I can design it to suit.

MADAM CHAIRMAN: So yes, we will then seek to include the recommendation as of 21 so that will have an impact on the Bill as drafted.

Number 22, the transition period. It speaks again to the transition period repeated over and over again and as we said, when it is proclaimed this will be addressed at that particular point and time so if the Committee agrees, this 22(2) should have no effect on the Bill as drafted. Let the record show general agreement.

Number 23 speaks to costs. It speaks to the administration costs would have to be borne by data controllers and data processors. That is the administration costs of having to implement this Bill and that data subjects are not required to pay any fees to enforce the rights given to them under the Bill. It is possible, however, and I am reading this directly from the submission, that the costs or parts thereof may be passed on to the customers for business to remain viable. The provisions of the Bill should therefore take into consideration the costs that will be incurred by the Office of the Data Protection Commissioner in the exercise of this function.

I am very curious as to the thoughts of the Committee on this one.

Based on the silence of the Committee on this, it will have no further impact on the Bill. Is that the general agreement? Yes? Any further comments? I am hearing some murmurings. Is it an intervention to the contrary? Minister Husbands?

Hon. Ms. C. S. V. HUSBANDS: The only thing is there is an implied threat here that if we do not find a way to minimise costs, they are going to penalise the consumer and a Government always has to be conscious of, I am not saying that we need to change anything but I think we need to be aware of what is the potential add on cost ...

Asides.

Hon. Ms. C. S. V. HUSBANDS: I do not know that you can really speak to it in the Bill but maybe how it is worded ...

Asides.

Hon. Ms. C. S. V. HUSBANDS: Right, so that is something we might want to be aware.

Asides.

Senator Ms. A. M. WIGGINS: When we are debating? Okay.

MADAM CHAIRMAN: Thank you very much for that. I believe this concludes our thorough examination and respectful consideration of the submission by the Barbados Bankers' Association. There are two other submissions to be considered at this

time. There is the Barbados Bar Association and there is also a submission from Mr. Devaron Bruce and I am told that there is a written submission also from Ms. Wiggins who would have done an oral presentation on June 26.

SUSPENSION

MADAM CHAIRMAN: May I, respectfully, suggest to the Committee that we suspend for lunch at this point in time and return for 2:15 p.m. It is now 1:25 p.m. If the Committee is in agreement because I know there are some other members of the Committee who have to go to an urgent meeting so the sooner we come back the sooner we can conclude our considerations. If the Committee is in agreement may I invite a motion for the suspension for lunch?

Motion inaudible.

MADAM CHAIRMAN: Thank you. We will be back from lunch at 2:15 p.m.

RESUMPTION

MADAM CHAIRMAN: I would like to call this meeting back to order after lunch.

Minister Sutherland exited the meeting after the luncheon period.

MADAM CHAIRMAN: The first consideration will be that of the Barbados Bar Association and we will go through the same process that we did where we look at each recommendation and we made a decision as to whether to not it would have an impact on the Bill so the first aspects are general and the first one is to draft regulations. It says: "*It is important to include the draft regulations otherwise there will be a lacuna between proclamation and implementation. It is always useful to hold consultations and discussions on the regulations in tandem with the discussion on the Bill*".

This regulation does not have any immediate impact on the Bill itself and certainly the Government will consider having consultations on the regulations as well. Are there any further comments on this?

There were none.

MADAM CHAIRMAN: Well, then we agree that as this is not directly relevant to the Bill then it will simply be noted for consideration.

The second aspect is enforcement provisions generally where it says that: Penalties for breach or failure to comply occur throughout the Bill". What this is recommending is that there be some civil liability alone or dual civil or criminal liability applied in situations where we need to enforce the Bill. Why I will say here is that we already have Administrative and criminal penalties and I will ask the Committee whether we think that there is a need now to add civil penalties at this particular stage in the Bill given that there are already Administrative and criminal penalties in the Bill.

There were no comments from the Committee.

MADAM CHAIRMAN: Okay, is it my understanding therefore that it is the agreement of the Committee that the recommendation for civil penalties to be added in fact at this stage will not receive consideration in the Bill. Is that correct?

The question was put and resolved in the affirmative.

MADAM CHAIRMAN: Let the record show that there is general agreement on that as well. Moving right along. The next recommendation relates to Part I – Preliminary, where there are a number of references in the Bill to "Court". Basically what they are asking is that in those several places that there be greater clarification of what is meant by "Court" and it cites several places in the Bill at least six places, I will not go through them now because I know that all of you have already read them so the question is: Is there any concern or objection? What do you say about bringing greater clarification to the term "Court"? Miss Belle.

Miss Shawn BELLE: Just to say that I have no objection with going through and making clarifications on "Court".

MADAM CHAIRMAN: Will such have any impact on the procedural timeline?

Miss Shawn BELLE: No, Madam Chairman.

MADAM CHAIRMAN: Okay. That said, may I propose that we agree that the Chief Parliamentary Counsel will go through and make the necessary corrections to the term "Court". Is the Committee in agreement?

The question was put and resolved in the affirmative.

MADAM CHAIRMAN: Let the record show that we have agreed.

Moving on to Part III, Rights of a Data Subject. I am going to ask Ms. Belle to speak to what it is being asked here.

Miss Shawn BELLE: Madam Chairman, the Bar Association is drawing attention to the fact that there should be protection under the Constitution for the right to privacy. They submit as a part of their, to support their argument citation of the Charter of the Fundamental Rights and Freedoms of the European Union in support of that, but just to say that that is an underlying fundamental freedoms document that European Union citizens can draw from in relation not the protection of their rights in addition to the GDPR. I want just to say that submission was made to the Ministry to indicate to them that they should consider whether the Constitution should be amended to reflect protections under - of privacy specifically. At that time a decision was made not to touch the Constitution at this time and rights can be protected by ordinary legislation, but since then a case called Nervais indicated that there can be litigable rights arising from the Section 11 of our Constitution. Now, section 11 of our Constitution basically is a recital of general rights

and was often thought of as merely pre-amble or introductory in orientation and it is in that particular section that the word privacy appears, so the old perspective legally was that a persons could not claim to rights of privacy under the Constitution by the mention of that one word in the enforceable provision under Section 11, but now with the Caribbean Court of Justice decision in Nervais they are saying that they are willing that court is saying that we find that Section 11 is separately enforceable and so it is possible for persons to claim privacy. Just to step out in relation to amending the Constitution I will just say that it is something to consider in the future in the sense that that particular provision only speaks to privacy once, it does not have the traditional structure where you would have a declaration of the right first and then the derogations from the right in terms of the interest of the State second. That is usually how the fundamental rights provisions are constructed, so that in a future exercise it would be good to expand it beyond section 11 and hopefully you all were not completely bored by that explanation.

MADAM CHAIRMAN: Senator Adams.

Senator R. J. H. ADAMS: Thank you, Madam Chairman. I just want to make sure that I understand what M. Belle just said. Are they saying on the one hand this is unnecessary because the Nervais precedent has been set and the second part is: Would we not in any way have to have these rights to privacy spelt out separately? Would we really want to put this Act inside the Constitution? Could there not be a cross reference or something?

Miss Shawn BELLE: Okay. I am understanding. Let me explain that they are in fact saying that Nervais would negate your need to spell it out because the court is saying that it is willing to interpret Section 11 which has the privacy word, it is saying that legal rights can be derived from that one word in that one section but... and then we can speak to this. That privacy word is saying that legal rights can be derived from that one word, in that one section, alright. To my mind it would be better to spell it out, and other jurisdictions have gone to the trouble of actually spelling it out. It is my understanding that Jamaica did make a move to deal with it in more elaborate terms in the way that I just suggested, which is the declaration of the right. Then the restrictions there under which is the usual way that constitutional provisions are constructed.

MADAM CHAIRMAN: I think this submission is a very useful submission and I think this committee will definitely take it into consideration as to how we move. I think as many people who know about Data Protection Legislation it often is part of a three part. Where you got the freedom of information, you have got data protection, you have got privacy as three parts of a one suite. Barbados is seeking to do each piece of legislation with the intention that we will eventually have the full suite and the recognition in the right places. So, just saying that this is under consideration at this point in time and it speaks of

course to a different legislation than this one, but, we are aware and we are certainly taking that into consideration, so that said we will note and take it into consideration. However, it will have no immediate impact on this Bill as it speaks to making amendment to a different kind of legislation, namely the Constitution. The next item speaks to the right to compensation, it is whereby companies are required to specify the rights of data subjects to obtain any other available form of redress. This is according to section 25(1) (E) of the Bill. The recommendation is that in Part 3 there is no specific right to compensation for the Data Subject, and that in the absence of this right to compensation for damage suffered arising, whether in respect of material or nonmaterial damage then it places a burden to show and prove pecuniary or other loss. In the rom of data and privacy infringements this can be difficult to quantify, and so basically what they are asking is that they be some recognition of a right to compensation. I will ask Miss Belle, to speak to that first before.

Miss Shawn BELLE: Madam Chairman, just to say that this was raised by the bankers as well, and so it was agreed there under that we would put in a clause speaking to the right to compensation.

MADAM CHAIRMAN: Any further thoughts from the Committee on this matter? Mr. Coppin.

Mr. Chesterfield COPPIN: Madam Chairman, it is just that, I think provision, I think Article 82. I think the GDPR does make reference to some compensation for the Data Subject as well.

MADAM CHAIRMAN: So you are saying that in us making that adjustment it would be compliant and certainly in keeping with it. Okay, that said may I ask the agreement of the Committee that, that clause be inserted that would speak to compensation for the Data Subjects.

The question was put to the Committee and resolved in the affirmative without division.

MADAM CHAIRMAN: Let the record show there is general agreement in that. The next matter deals with sections 22-28 part 4, transfers of personal data outside of Barbados, and I will read from the submission. *"It was clear that the intention of the legislature and an important facet of this Bill to hold foreign governments and foreign corporations and businesses liable for processing of or I should say accountable, they say liable also, for the processing of data of Barbadians. Section 22 of the Bill speaks to a general principle for data transfers and this section states that the Country or territory to which data is transferred must provide an adequate level of protection for the rights and freedoms of Data Subjects".* It goes on to speak to base on section 23 of the Bill, which speaks to what will constitute as adequate protection as stated in section 22. *"Enforcement of the protection of the data of Barbadians is dependent on whether the foreign Country has adequate legislation, the laws enforced in the land or in territory in question and international*

obligations of that Country". Basically, what they are asking us to do is to pull out certain clauses with regards to the transfer of data and I am summarizing the other 3-4 paragraphs that follow, and I know that all members of the committee have read. What I am advised and in fact, rather than say what I have been advised let me let the Senior Parliamentary Counsel speak to the matter, and give the Committee the background from which to make an informed decision.

Miss Shawn BELLE: It seems like there is a request to rather than have these provisions dealing with the transfer of data outside of the Country that you would rather rely on reciprocal agreements that can be used then to enforce the rights of persons, Data Subjects. This is not advised in the sense that it is outside of the GDPR's arrangement, and if it is that we are seeking to be within that arrangement it would not be good for us to do so. Even when you use these reciprocal agreements as they put them, it will only be between that Country and ours, it would not include other jurisdictions. The GDPR has a wider scope and since many jurisdictions are headed in that direction in terms of submitting to that framework it is advisable to submit to the wider framework.

MADAM CHAIRMAN: Senator Wiggins.

Senator Miss. A. M. WIGGINS: Thank you, Madam Chairman. In looking at section 4 and scanning through it quickly one of the things that come to mind, CPC spoke of reciprocal agreements, which is a good bridging point that you made. What happens in the case now and if you read down further. As you know we will be collecting Value Added Tax (VAT) on International transactions, so you have the Data Processors such as VISA and Amex, and all of those are now going to become what? They are going to become Data Processors, and or Data Controllers. So how are we going to reconcile that position there and like I said, if you read further down it was issues that at least I have eluded to previously when we spoke. Outside of the reciprocal agreements now, because Amex and Amazon and all of those would have captured our basic information, anyhow. First of all, you have someone who is purchasing goods from Amazon, Ali Baba and then secondly, you are using your financial data now, by use of a VISA, Amex, PayPal, *et cetera*. I just want to know how you reconcile all that information with everything that is contained right now in part 4.

MADAM CHAIRMAN: Miss Belle.

Miss Shawn BELLE: See in Clause 3 the scope of the legislation, and attention is drawn to (1) (B). It says that the Act will apply to the processing of personal data of Data Subjects in Barbados by the Data Controller or the Data Processor not established in Barbados. Where that the processing activities are related to offering of goods or services to Data Subjects in Barbados, so there is a parameter that is set up in relation to the extent to which the Bill would cover. I do not know if that provides you with any clarity or....

Asides.

Miss Shawn BELLE: Well, that really is the scope of application in terms of data subjects that are not established here. I do not know, maybe you can give more examples so that I can try to assuage you.

Senator Ms. A. M. WIGGINS: Well, they have alluded to the same issues about Cambridge Analytical that was spoken about earlier, so it means that given that your personal data is now being collected outside of Barbados, in countries in which we have no legal jurisdiction, what redress does a data subject have if your personal data is harvested by someone similar to Cambridge Analytical?

Miss Shawn BELLE: You would have to pursue an enforcement in that jurisdiction. Now, if that jurisdiction does not have the appropriate legal framework, [then] there would be a problem, which is why you have the stipulation in the general principles that you are not to transfer data to jurisdictions that do not have the necessary framework. Otherwise, the data subjects would therefore not be able to enforce their rights in that jurisdiction.

Senator Ms. A. M. WIGGINS: I want Senator Adams, through you, Chair, to reply to this one. Senator Adams always tells me [that] I am giving him all of this credit. What I am speaking about, I do not recall any penalties that were meted out to Cambridge Analytical except that the company was dissolved. I do not recall, so [that] I am just trying to figure out if you do recall if there were any penalties that they suffered as a result of harvesting people's personal data illegally.

Senator R.J.H. ADAMS: Madam Chair, if I can just add sort of a general comment, specifically on the parameters that were laid out, so [that] when I read this, I could not help but thinking that our legislation is more about prevention than cure, although there is a cure part in there and that these seem slightly off-base the way that they are set out. Although I understand and it is reasonable, clearly there are limits to what we can enforce in someone else's jurisdiction and the best result is that, especially companies that are locally domiciled, they do not transfer the information but the problem comes when you have a foreign company whose services.... and their site, **WhatsApp**, **Facebook** and so on, now there you are on really tricky grounds. I am not sure [that] there is anything we could draft that could deal with that. There is no form of words, I think, that we could easily deal with that, so I understand Miss Belle's answer about pursuing people in their own jurisdiction, but in my mind I just got it separate from that example and the domestic treatment of this data, knowing that there is always going to be a gray area. I hope that [that] answers you a little bit.

MADAM CHAIRMAN: Thank you. I think what we are seeing from this discussion is that this is still an evolving area of law right now and [that] there are many things that we can address and there are things that we will have to be constantly staying vigilant and seeking to find types of redress for them as we go forward. I would say, as the recommendation speaks here in terms of calling for us to look at supporting legislation to hold foreign governments and private

companies accountable for instances, I think that was covered very succinctly and clearly in the interventions of Miss Belle, as well as Senator Adams. At this point in time I cannot see how we could include this within our legislation, there is just not the scope for us to do it within this legislation but we would want to remain engaged with the rest of the world as we all grapple with this, for the same reasons. That said, then this submission with regards to Sections 22 to 28 shall have no further impact on the Bill as drafted.

Senator Ms A. M. WIGGINS: Madam Chair, I understood everything that you have said but I think that "for further consideration..." [should be added].

MADAM CHAIRMAN: Is that where the Committee is comfortable, that it will have no impact on the Bill at this time, [but that] however, we will keep it for further consideration. Are there any objections?

MADAM CHAIRMAN: It seems as if from the nodding of heads there general agreement of the Committee on that. The next....

Senator R.J.H. ADAMS: Madam Chair, I am sorry, as you said that, I am thinking to myself, legislation is dynamic. We can call it "for further consideration." I am happy with that but I take it, to my mind, it might be better for us to realise, we cannot revisit. Does it have a function of available tool, for example? I am not clear what "further consideration" would be but I thoroughly recognise that situations are dynamic and things can change but I am not sure that [that] adds a great deal of value.

MADAM CHAIRMAN: I think it brings a greater precision in language, with an understanding that because it is dynamic and ever-changing that there would be some room for revisiting at that time. I beg your indulgence, we are seeking to see where the next section begins and ends for the next recommendation. One minute, please. The next one is a general comment calling for supporting legislation or amendments to existing electoral laws to protect data subjects from fraudulent and malicious manipulation of data that it will affect political outcomes. I think we are familiar with some cases that would have happened recently, particularly in the case of the United States of America and therefore there is some legitimate reason for this to be raised. At this point this is rather aspirational in terms of what this piece of legislation can do and I think [that] it falls in the same realm where there are certain limitations to individual pieces of legislation, but this is something that as the whole environment remains dynamic that we should continue to be vigilant for solutions to this. Are there any further concerns, comments or perspectives from members of the Committee?

The Committee responded in the negative.

MADAM CHAIRMAN: There being no others, then this request for amendments to existing electoral laws falls outside the scope and will not have an impact immediately on this legislation. Are we in agreement?

The Committee responded in the affirmative.

MADAM CHAIRMAN: Let the record show that there is general agreement. "Part VI: Data Controller and Data Processor." I am going to ask Miss Belle to speak to this particular recommendation, please.

Miss Shawn BELLE: Madam Chair, this is again a call to expand the choice of penalties that should be imposed for breaches in the Bill and in this regard they want a focus on the data controllers and I am presuming the data processors in terms of them being registered pursuant to the legislation. They are also critiquing the fact that the flat fine provided for would not be effective for particularly large, foreign corporations and so that there should be consideration to addressing those types of offenders. You would recall in previous discussions that the fine is not a flat fine but it is a range between zero to \$500 000.00. Well in this case I do not know if this would be a \$500 000.00 one, but just to say as a principle, all of the penalties are expressed at their maximum. In terms of the introduction of civil penalties, we just discussed that that is something that would have to be revisited at a later stage. This is basically where this is going, that the fines and the penalties should be revisited, that there should be more choice and there should be higher set of fines where it comes to larger corporations.

MADAM CHAIRMAN: I believe that in our session on Wednesday perhaps that we did recognise that this may very well be a way to go in the future but at the moment that we would stay with the fines as we have them with the view to reviewing at some stage to determine whether we need to adjust the way we access those fines. With that said is there any need for us to amend that decision which would have been made on June 26? Then it seems there is the agreement of the Committee that that decision remains, no need to adjust it.

The next recommendation relates to territorial scope. I will again ask Ms. Belle to speak to that recommendation.

Miss Shawn BELLE: Madam Chair the Bar Association points to Article 3 of the GDPR saying that this regulation applies to the processing of personal data of data subjects of the union by a controller or a processor not established in the union, emphasis added. Then they go on to speak about basically the application the GDPR generally. They then do a comparison with the Bill and they are trying to indicate that the Bill departs in its language and so therefore there is a different burden that is placed on data subjects or that somehow application of the Bill is different from the application of the GDPR. When you look at the language that the Bill uses, it is very similar, it is just that we use Barbados, so in Clause 3 it would read, "this Act applies to," and then you would go down to be the processing of personal data of data subjects in Barbados by a data controller or a data processor not established in Barbados, which is similar to the wording

that they would have cited in their own submission by a controller or processor not established in the union. I am not really understanding where the differentiation lies, so I would suggest that no amendment is necessary.

MADAM CHAIRMAN: Given that suggestion, is there any other member of the Committee with an opposing view? With that said, we are agreed that the recommendation on territorial scope should have no further impact on the Bill as drafted. We now move to "Part 7, Data Protection Commissioner". I am going to ask Ms. Belle to speak to this at this point and I will give any further clarification that may be necessary.

Miss Shawn BELLE: The GDPR requires that the supervisory authority be independent. Independent basically of any undue influence either by the Government or any other constituency of say a particular industry. Usually the approach that would be taken would be to have a statutory corporation and then like for instance a Commission, similar to the Fair Trading Commission or other such entity, then that Commission would regulate the operations under the said subject on a particular subject area. From that perspective they are recommending that the data commissioner, in being a public officer would not have the separation or the independence that would be required under GDPR. Now the thing is that what people do not quite understand is within the civil service, just because you are a public officer, it does not mean that you cannot act independently and your position would be protected under the Public Service Act and then way that you are funded and staffed would be dealt with by the Government yes, but at the same time you would be secure in your operations, so that nobody would sit down and say for instance that the SG is not an independent party if it is that there is an entity that is out of line or a department of Government that is out of line, the SG would say you need to comply with the law. In the same way the commissioner is empowered by virtue of the Bill to act in a fashion that would keep public entities in line. There are several directives that can be made pursuant to Clause 71 of the current Bill to speak to guiding to public entities where they may be out of line. I am just saying that just because you have put a data protection commissioner as the public officer, it does not necessarily mean that independence has been lost. From that perspective we do not need to pursue separation to the extent that they may be recommending at this time.

MADAM CHAIRMAN: Senator Wiggins.

Senator Ms A. M. WIGGINS: Yes Madam. In terms of the protection to the Data Commissioner, correct me if I am wrong, I think the Auditor General is protected by the Constitution, but this Data Commissioner you said is under the Public Service Act. Explain what protection the Data Commissioner will really have vice versa, let us say the Auditor General who is protected by the Constitution.

Miss Shawn BELLE: The Constitution, yes would be fundamental law and would have a stronger

protection but the Bill will also provide protection in terms of you would have seen that if it is that they operate in good faith then they would not be liable to being sued. In terms of the Public Service Act, the qualifications and your security in your position is established and so therefore the very establishment acts as a protection for that officer. Those things give protection and security for that person. It is only then if they were to depart from their duties in some way, then they would become subject to that same Public Service legislation which would then render them subject to discipline.

Senator Ms. A.M. WIGGINS: I am wondering then why the Data Protection Commissioner could not then be protected by the Constitution rather than by the Public Service Act.

Miss Shawn BELLE: I have not seen any jurisdiction actually protect the Data Protection Commissioner under the Constitution; most likely because with an officer like the one you would have spoken about that has to do with money and maybe management of the Consolidated Fund. The thing is that it goes back to the constitutional provisions there. This is slightly different, so the insulation which the authority would receive would be this Bill plus the Public Service legislation.

MADAM CHAIRMAN: At this time does any Member of the Joint Committee see it necessary for us to make any adjustments to any protection for the Data Protection Commissioner in order to secure any further independence?

Asides.

MADAM CHAIRMAN: From the response of the Committee, I take it that this recommendation with regard to the Data Protection Commissioner would have no further impact on the Bill as drafted. Let the Record show agreement. Finally, on this particular submission is a general comment with regard to the commencement date. You would see on Page 16 of the submission by the Barbados Bar Association. I know all of you have read it so I will not read the entire matter. What I would recommend as Chair is that the matters which are raised here with regard to the commencement are all dealt with in the Proclamation of the Act when it becomes law. Therefore, there is no need for us to make any further adjustment to the provisions for commencement. Is the Committee in agreement?

Asides.

MADAM CHAIRMAN: Let the record show we are in full agreement and we have now concluded the submission from the Barbados Bar Association. Thank you so much for your attention. I will just ask that we take a break for about five minutes just for people to refresh themselves as we enter the final submission to be reviewed by the Joint Select Committee.

At this point, a suspension was taken. However on resumption, the recording went straight into a submission by Miss Shawn Belle.

Miss SHAWN BELLE: ... it is the bottom part which says, "Main concern" and he basically is stating that the references made to the protection of personal data as it relates to the use of social media. He is questioning the adequacy of protections which are not afforded to data that is classified as sensitive personal data. My problem with the point that he is submitting is that it seems to me that he is interpreting the abundance of provisions speaking to personal data as being more than those dealing with data. I think one of the things that he is not understanding is that sensitive personal data is treated at a very strict level, meaning that sensitive personal data is not really supposed to be processed at all save in very exceptional circumstances. That, almost immediate, dismantles most of his submission because a lot of it is predicated on the fact that he feels that more protections need to be afforded in relation to sensitive personal data against the backdrop of social media and from that perspective. I think he has a misunderstanding. That is how I would treat it.

Just to speak to some of his other points, mitigating threats to data privacy and sensitive data manipulation. Clause 9.(1) states that sensitive personal data should not be processed except in certain circumstances and the circumstances themselves, as stated in Clause 9, imposed obligations on data controller and data processors which dictates how such data should be processed. He also raises under Disclosure Requirements for Companies that Process Social Data Media, that there should be specific obligation to protect sensitive social media data but as set out before, sensitive personal data is not supposed to be processed except in certain circumstances.

The other matter then that attracted attention was the enhancing of user control over data and it just to say that there is already a right to erasure and also a right to restrict. The right to restrict is not only to correct inaccurate data as asserted but it is to correct the data as the data subject sees fit. There is also a submission to amend the Constitution of Barbados to recognise the right of privacy. As we would have discussed earlier, that is a proposal that the Government is taking into account at a future date therefore, from that perspective then it will be addressed at a time to be determined. That is my commentary on, Mr. Brewster's submission.

MADAM CHAIRMAN: Are there any further submissions from the Joint Selection Committee at this stage? With there being no further comments I believe the Committee is in agreement that this submission is helpful, it is beneficial, it draws our attention to the need for us to look at greater regulation in social media, however, it will not have any impact on the Bill as drafted. Is that the general agreement of this Committee?

The Committee unanimously agreed.

MADAM CHAIRMAN: That being said, we now draw this to conclusion. Finally, before we go through the Bill Clause by Clause, I would wish to acknowledge that Miss Cynthia Wiggins, who made an oral presentation to this Joint Select Committee on Wednesday, June 26, did indeed follow up as promise with her written submission. Given that, it pretty much mirrors her oral submission it will receive no further consideration at this time. Is that the consensus of the Joint Select Committee? Let the record show that it is so joined.

SUSPENSION

MADAM CHAIRMAN: Again, we have one of our Joint Select Committee members who has to step out for a minute. Let us simply suspend for five minutes so that we can then go through the Clause with a full quorum at that time.

RESUMPTION

MADAM CHAIRMAN: We will simply now go through the Bill. Is there anything in addition to what has already been agreed as amendments that we would wish.....? We will do it Part by Part. Part I, is the Interpretation Section. Is the Committee in agreement that nothing further than the amendments already made would apply?

The Committee agreed that nothing further than the amendments already made should apply.

MADAM CHAIRMAN: There is general agreement, let the record show.

Parts II was called. Is there anything in addition?

There was none.

The Committee agreed that Part II should not change in anyway other than what was already agreed.

Parts III to X inclusive were called and passed.

The Schedule was called.

The Committee agreed that there should be no further amendments than what have already been agreed to the respective Parts just read. The Schedule was passed.

ANY OTHER BUSINESS

MADAM CHAIRMAN: Is there Any Other Business?

There was none

MADAM CHAIRMAN: There being no further business for this Joint Select Committee, I now invite a motion for us to adjourn until a date to be announced, and that on that next occasion we should see the amended draft Bill and we should sign off on

that before it goes back to the Honourable the Senate for continuation of the Second Reading. I would like to invite a motion for the adjournment until a date to be announced.

ADJOURNMENT

On the motion of Mr. N. G. H. ROWE, seconded by Senator R. J. H. ADAMS, the Committee was adjourned sine die and MADAM CHAIRMAN adjourned the meeting accordingly.

**FOURTH MEETING
OF THE
JOINT SELECT COMMITTEE ON THE DATA PROTECTION BILL, 2018
HELD IN
THE HONOURABLE THE SENATE**

MONDAY, JULY 8, 2019

First SESSION 2018-2023

PRESENT:

Senator the Hon Miss K. S. McCONNAY
(*Madam Chairman*)
Hon. D. D. MARSHALL, Q.C., M.P.
Hon. D. G. SUTHERLAND, M.P.
Mr. N. G. H. ROWE, M.P.
Senator R. J. H. ADAMS
Senator Miss C. N. DRAKES
Senator Miss A. M. WIGGINS

Also Present were:

Miss SHAWN BELLE (*Senior Parliamentary Counsel*)
Mr. CHESTERFIELD COPPIN (*E-Commerce
Development Officer*)
DEPUTY CLERK Nigel Jones
DEPUTY CLERK Miss Beverley Gibbons
Miss Suzanne Hamblin, (LIBRARY ASSISTANT)
PROCEDURAL OFFICER TO THE COMMITTEE
(Ag.)

CALL TO ORDER/WELCOME

Madam Chairman called the meeting to order at 2:25 p.m.

MADAM CHAIRMAN: There being a quorum at this time I would like to call the meeting to order.

MINUTES

MADAM CHAIRMAN: Many of you would have received the Minutes of the last two meetings, which would have been meeting number 2, and meeting number 3. Are there any corrections to the Minutes at this stage?

Senator Miss. A. M. WIGGINS: Madam Chairman, just one correction, just to have my name spelt correctly, a-l-"p" as in Poland, "h" as in Holland, e-a, Wiggins throughout the document, thank you.

MADAM CHAIRMAN: Okay.

Senator Miss. A. M. WIGGINS: "P" as in Poland, "h" as in Holland, throughout the entire document in both minutes.

MADAM CHAIRMAN: Okay.

Senator Miss. A. M. WIGGINS: Thank you.

MADAM CHAIRMAN: Any further corrections? Okay, there being no further corrections, I would like to invite a motion that we confirm the Minutes with the aforementioned amendment throughout the document for the spelling of Senator Wiggin's name. I would like to invite a motion for the confirmation of the Minutes.

On the motion of Senator D. R. SANDS, seconded by Senator Miss A. M. WIGGINS, the Minutes were confirmed.

MATTERS ARISING

MADAM CHAIRMAN: Are there any matters arising from the Minutes?

There were no matters arising from the Minutes.

DRAFT REPORT

MADAM CHAIRMAN: The next item is the draft report. There is currently the Revised Bill, which would have been sent out last week. I trust all Members had the opportunity to take a look at them. Are there any changes that were made that you saw that were missing from the deliberations of the Committee?

What we will do is take a look at the clauses that were amended and ensure that indeed we are all in agreement with the amendments that were made.

The first was to amend the long Title that would say "*To Provide for Matters*", that correction has been made. Anything further on that one?

The second amendment was to Clause 2, to delete the reference to "credit reference agency". That has been completed.

Amendment to Clause 4(7), "to ensure the reliability in respect of employees"; that has been clarified.

With respect to Clause 9(1) (a), we were to delete the word "written consent" and replace that with "explicit consent". That has been completed.

Miss Shawn BELLE: Madam Chairman, just to say that the words "written consent" were to be removed and replaced with "explicit consent", but you would see that the word "consent" remains unqualified and that is because "consent" is then defined in Clause 2, so that there is a clarification as to what "consent"

would mean. I did because from research there was nothing connected to The General Data Protection Regulation (GDPR) connected with the definition of "explicit consent", but there was for "consent", so for clarity sake I defined "consent" then in clause 2.

MADAM CHAIRMAN: Any questions?

There were no questions.

MADAM CHAIRMAN: Okay, then, thank you.

Number 5, Clause 15, to remove reference to "his/her". I think this was a general correction throughout the Bill, because they were different ways in which we use "his", "her", "they", *et cetera*. So for consistency it was suggested that we address this matter and that has now been addressed throughout.

Clause 71, "to empower the Commissioner to issue advice to Data Processors and Data Controllers upon request". If we see Clause 71(M).

Miss Shawn BELLE: Madam Chairman, through you, just to say that "person" was inserted and that then would give the scope for Data Processors and Data Controllers, as well as other persons who may need advice from the Commissioner in relation to the implementation of the legislation.

MADAM CHAIRMAN: Okay, I guess that covers that one. Now, with regard to Clause 79 (1), requiring the Data Controller "to furnishing..." It was a typographical error that has now been corrected.

Reference to the word "court" that was in several different clauses which we see here and if we see Clause 2 reference to the word "court" in the Bill should be clarified so see Clause 2 "definition of sensitive personal data" paragraph (k), Clause 16, *et cetera*. That matter has now been addressed as well.

The next one was to insert a clause on the liability of Data Controllers and Data Processors, if we look at Clause 93, the new Clause 93, that matter has now been addressed and that now deals also with the right of compensation, which was also an area to be addressed.

I believe that concludes all of the major amendments from the last two meetings that were to be made, and we can see that they have all been addressed.

I would like to invite a motion for us to confirm that all revisions as determined by the Joint Select Committee have now been made in the Revised Bill.

Senator Miss. A. M. WIGGINS: I am putting forward the motion that all the revisions made by the Joint Select Committee have now been corrected and [that] this will be the Revised Bill. Thank you.

A motion was moved by Senator Miss A. M. WIGGINS, seconded by Senator Miss C. N. DRAKES, that all the revisions made by the Joint Select Committee have now been corrected and that this will be the Revised Bill.

MADAM CHAIRMAN: Members, I am told by the Clerk of Parliament that the Draft Report has just

been circulated. You should check your emails and find that. I would suggest that we suspend for about 10 minutes to give you the opportunity to go through that, so that we can consider it in a minute. We will resume at 2:45 p.m., giving you time to look at that report.

The Committee was thereby suspended until 2:45 p.m.

RESUMPTION

MADAM CHAIRMAN: I would wish to resume now. I imagine all persons have seen the report. Any suggested amendments? On Page 1 the name "Alphea" again is to be corrected as in all the Minutes mentioned earlier. On Page 2 No. 4: "*The Committee scheduled meetings for the following dates: June 24, June 26, Monday, July 1 and Monday, July 8*".

Therefore, you are adding "and Monday, July 8." Further down in the same No. 4 at the very bottom, the very last paragraph on Page 2:

"The agreed procedure that informed the Committee was for the Committee to receive the oral presentations at the second meeting during the morning session on Wednesday, June 26, 2019. After lunch, consideration was given to the written submissions."

There is therefore a period after "2019" and a new sentence starting with "After lunch". If we move to Page 3, the second paragraph from the top:

"The Committee determined that it would complete its work by Monday, July 1, 2019 and be in a position to report to the Honourable the Senate, and thereafter the Bill be submitted to the Honourable the House of Assembly."

MADAM CHAIRMAN: We are therefore removing everything after "Senate" in the second line all the way to "Bill" in the third line. Do I need to repeat? On that same Page 3, it reads:

"Written submissions were received from the following persons, organisations"

MADAM CHAIRMAN: The first person there is Miss Belle, and that was not a submission by Miss Belle. She would have done a presentation, and she is an advisor to the Committee so that would not apply. Of course, with Miss Belle being removed at that first level, Page 3, last paragraph, it then has a consequential re-numbering that would have to occur. Also in reference to that same paragraph, when we go to the very first paragraph at the top of Page 4, it states, "These submissions", referring to the same submissions we just renumbered and took Miss Belle's submission from being included. They are appended here and marked as (e). The submission from Miss Belle was marked as (e). Given that it is no longer being treated as a submission, we would need to remove (e), and that would have a consequential re-alphabetising of the appendices.

Asides.

MADAM CHAIRMAN: Yes, we will re-letter them accordingly. If you look at the fourth

paragraph down on Page 4, it states:

"The reference in the Report to the amendments are obviously to the old Bill."

Remove the word "obviously". Further and just below that it states:

"Monday, June 24, it was agreed that the Committee would switch the order."

That is already contained in the Minutes of the Meeting which we just confirmed. Therefore, we can remove all the way from "Monday" down to the word "last". Then we can end with the paragraph which states:

"Having given due consideration to the various submissions, the Committee agreed to the following Amendments to the Bill, and as reflected in the revised Bill."

MADAM CHAIRMAN: Did you get it, Hansard Reporter?

Asides.

MADAM CHAIRMAN: Okay, good.

Asides.

MADAM CHAIRMAN: The Clerk has spotted an additional adjustment on Page 2, the very bottom of the page, the last paragraph. It reads:

"Each presenter had ten minutes".

He wants to insert after "minutes" the words "for their presentations". He also wants to remove "up" and "with" with the word "by". The sentence is, in part, "by 15- and 20-minute question-and-answer segments." There being no further edits or amendments. I wish to invite a Motion that we confirm the Report as amended.

Senator Miss. A. M. WIGGINS: Madam Chair, I would like to confirm the Report as amended.

Senator D.R. SANDS: I second that Motion, Madam Chair.

MADAM CHAIRMAN: Is there any other business?

Asides.

MADAM CHAIRMAN: I would simply wish to advise the Committee that there was a further submission from the Barbados Association of Medical Practitioners. It would have been after the date of the submissions. Miss Belle has kindly considered that submission, and there are some responses to it. None of the responses, however, require any consequential adjustment or will have any impact on the Bill as it is revised. I want to thank Miss Belle for taking the time even after that submission period, and for doing her due diligence in that regard to make sure that we did not miss anything that was urgent or that would in some way compromise our ability to protect the rights of the Data Subject. Is there any other business?

*A
sides.*

MADAM CHAIRMAN: There being no further business, I just wish to inform that the Clerk of Parliament will be circulating the Amendments to the Minutes and to the Report, as we would have just agreed, and a round-robin approval would be required so that we can then move to the Honourable the Senate as planned. The date on which that Report will go to the Senate will be determined in collaboration with the Parliament. That being the case, I wish to thank all of you for serving on this Committee. It has been an absolute pleasure, and we look forward to the further advancement of the Bill through the Parliament. Have a good evening, all.

That ended the fourth meeting of the Joint Select Committee focusing on the Data Protection Bill.

Approved by this Joint Select Committee on the **Data Protection Bill, 2019.**

Senator the Hon. Miss Kay S. McConney
Chair



Senator Damien R. Sands



Senator Rawdon J. H. Adams



Senator Miss Crystal N. Drakes



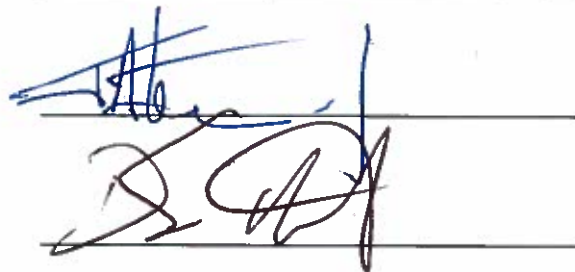
Senator Kevin J. Boyce



Senator Ms. Alpheia M. Wiggins

Hon. Dale D. Marshall, Q.C., M.P.

Bishop Joseph J. S. Atherley, J.P., M.P.



Hon. Dwight G. Sutherland, M.P.

Hon. Ms. C. Sandra V. Husbands, M.P.



Mr. Neil G. H. Rowe, M.P.



Dated this 17th day of **July, 2019**

