Data Protection Act 2013

Antigua and Barbuda

Data Governance

Definitions of Data:

Data is not defined specifically. However, provides a definition for data subject and data user. 'Data subject means a natural or legal person who is the subject of personal data'. 'Data user means a person who either alone or jointly in common with other persons processes any personal data or has control over or authorizes the processing of any personal data...'

Main Focus of Document:

To promote the protection of personal data by public and private bodies and for other incidental connected purposes.

Target Beneficiaries or Sectors:

general public, commercial sector, both local and international

Key Elements:

"Provides a legislative framework for any medium in which data is recorded, whether printed or on tape or on film; and including electronic means. The main objective of the Act is to safeguard personal data which is processed by both public and private bodies. Consent should be given for the processing of such data and relevant information should not be disclosed. Key section details are summarised below:

5. General Principle (1) A data user shall not–

(a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or

(b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 18.

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

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

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

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

(e) for the administration of justice; or

(f) for the exercise of any functions conferred on a person by or under any law.

(3) Personal data shall not be processed unless the–

(a) personal data is processed for a lawful purpose directly related to an activity of the data user;

(b) processing of the personal data is necessary for or directly related to that purpose; and

(c) personal data is adequate but not excessive in relation to that purpose.

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

7. Disclosure Principle Subject to section 17, no personal data shall, without the consent of the data subject, be disclosed– (a) for any purpose other than– (i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or (ii) a purpose directly related to the purpose referred to in subparagraph (i); (b) to any party other than a third party of the class of third parties as specified in section 6 (d).

8. Security Principle (1) A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard to– (a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; (b) the place or location where the personal data is stored; (c) any security measures incorporated into any equipment in which the personal data is stored; (d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and (e) the measures taken for ensuring the secure transfer of the personal data. (2) Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor– (a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and (b) takes reasonable steps to ensure compliance with those measures.

9. Retention Principle (1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. (2) It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

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

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

12. Processing of sensitive personal data (1) Subject to subsection (2) and Part II, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions– (a) the data subject has given his or her explicit consent to the processing of the personal data; (b) the processing is necessary– (i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment; (ii) in order to protect the vital interests of the data subject or another person, in a case where– (A) consent cannot be given by or on behalf of the data subject; or (B) the data user cannot reasonably be expected to obtain the consent of the data subject; (iii) 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; (iv) for medical purposes and is undertaken by– (A) a healthcare professional; or (B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare profession for; (v) the purpose of, or in connection with, any legal proceedings; (vi) the purpose of obtaining legal advice; (vii) the purposes of establishing, exercising or defending legal rights; (viii) the administration of justice; (ix) the exercise of any functions conferred on any person by or under any written law; or (x) any other purposes as the Minister thinks fit; or (c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject. (2) The Minister may by Order published in the Gazette exclude the application of subparagraph (1)(b)(i), (viii) or (ix) in such cases as may be specified in the order, or provide that, in such cases as may be specified in the order, the condition in subparagraph (1)(b)(i), (viii) or (ix) is not to be regarded as satisfied unless such further conditions as may be specified in the Order are also satisfied. (3) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding three years or to both."

Consent Data Data integrity Data processing Data protection Data subject Data user Legislative framework Personal data

Policy/regulation mirrored:

Data Protection Acts

Countries:

Botswana

Jamaica

Singapore

Cyprus

Malta