Electronic Crimes Act 2013 & Electronic Crimes (Amendment) Act 2018

Antigua and Barbuda

Data Governance

Definitions of Data:

Data includes representation of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic programme, text, images, sound, video and information within a database or electronic system.'

Main Focus of Document:

To govern electronic data usage, the damage of electronic systems or networks, electronic data and other unrelated electronic crimes.

Target Beneficiaries or Sectors:

persons who intend to misuse data that has been obtained.

Key Elements:

"This Act provides for misuse of data and criminalises certain actions of individuals that are committed electronically. Data is prohibited for uses other than that which it was intended. Key sections include:

3. Access and interference (1) A person shall not intentionally, without lawful excuse or justification– (a) access an electronic system or network; (b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium; (c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network; (d) damage or cause to be damaged an electronic system or network, data, electronic data base or other program residing in such electronic system or network; (e) disrupt or causes disruption of an electronic system or network; (f) deny or cause the denial of access to a person authorised to access an electronic system or network by any means; (g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act; (h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network; (i) willfully destroy, delete or alter information residing in an electronic system or diminish its value or utility, or affect it injuriously by any means; or (j) steal, conceal, destroy or alter or cause a person to steal, conceal, destroy or alter any source code used for an electronic system with an intention to cause damage. (2) A person who contravenes subsection (1) commits an offence and is liable on- (i) summary conviction to a fine not exceeding $200,000 or to imprisonment for a term not exceeding three years, or to both; or (ii) conviction on indictment to a fine not exceeding $500,000 or to imprisonment for a term not exceeding seven years, or to both.

4. Identify theft (1) A person shall not intentionally, without lawful excuse or justification make fraudulent or dishonest use of an electronic signature, password or other unique identification feature of another person. (2) A person who contravenes subsection (1) commits an offence and is liable on- (i) summary conviction to a fine not exceeding $200,000 or to imprisonment for a term not exceeding three years, or to both; or (ii) conviction on indictment to a fine not exceeding $500,000 or to imprisonment for a term not exceeding seven years, or to both.

5. Electronic forgery A person who, with intent to defraud, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, whether or not the data is directly readable and intelligible, commits an offence and is liable on; (i) summary conviction to a fine not exceeding $200,000 or to imprisonment for a term not exceeding three years, or to both; or (ii) conviction on indictment to a fine not exceeding $500,000 or to imprisonment for a term not exceeding seven years, or to both.

6. Electronic fraud (1) A person shall not, intentionally or without lawful excuse or justification, induce another person to enter into a relationship, with the intent to defraud that person or cause that person to act to his own detriment or suffer loss of property, by – (a) any input, alteration, deletion or suppression of data; or (b) any interference with the functioning of an electronic system. (2) A person who contravenes subsection (1) commits an offence and is liable on- (a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding three years, or to both; or (b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both.

7. Misuse of encryption (1) A person shall not intentionally, without lawful excuse or justification for the purpose of commission of an offence or concealment of incriminating evidence, intentionally encrypt any incriminating communication or data contained in an electronic system relating to the offence or incriminating evidence. (2) A person who contravenes subsection (1) commits an offence and is liable on- (a) summary conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both; or (b) on conviction on indictment to a fine not exceeding $250,000 or to imprisonment for a term not exceeding five years, or to both.

8. Sensitive electronic system (1) A person shall not intentionally, without lawful excuse or justification disable or obtain access to a sensitive

electronic system whether or not in the course of commission of another offence under this Act. (2) A person who contravenes subsection (1) commits an indictable offence and is liable onconviction to a fine not exceeding $300,000 or to imprisonment for a term not exceeding twenty years or to both. (3) For the purposes of this section a "sensitive electronic system" is an electronic system used directly in connection with or necessary for– (a) the security, defence or international relations of Antigua and Barbuda; (b) the existence or identity of a confidential source of information relating to the enforcement of criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation or public key infrastructure; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; or (e) the purpose declared as such by the Minister by Order published in the Gazette.

9. Electronic terrorism A person who– (a) with intent to threaten the peace, security or sovereignty of Antigua and Barbuda or to strike terror in the people or any section of the people by– (i) denying or causing the denial of access to any person authorised to access an electronic system; (ii) attempting to penetrate or access an electronic system without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce any contaminant into an electronic system, and by means of such conduct causes or is likely to cause death or injury to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure relating to the security of Antigua and Barbuda, or (b) intentionally penetrates or accesses an electronic system without lawful authorization and by means of such conduct obtains access to information, data or electronic database that is restricted for reasons for the security of Antigua and Barbuda or foreign relations, or any restricted information, data or electronic database, with reasons to believe that such information, data or electronic database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty of Antigua and Barbuda, the security of Antigua and Barbuda, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits an indictable offence of electronic terrorism and is liable on conviction pursuant to the penalties prescribed pursuant to the Prevention of Terrorism Act 2005.

10. False websites and spam (1) A person shall not intentionally, without lawful excuse or justification set up a website or send an electronic message with a counterfeit source – (a) with the intention that the recipient or visitor or an electronic system will believe it to be an authentic source; or (b) to attract or solicit a person or electronic system; for the purpose of gaining unauthorized access to commit a further offence or obtain information which can be used for unlawful purposes. (2) A person shall not intentionally without lawful excuse or justification – (a) initiate the transmission of multiple electronic mail messages from or through an electronic system; (b) use a protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or internet service provider, as to the origin of such messages; or (c) materially falsify header information in multiple electronic mail messages and initiate the transmission of such messages. (3) A person who contravenes subsection (1) or (2) commits an offence and is liable on – (a) summary conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both; or (b) on conviction on indictment to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding five years, or to both.

11. Unauthorised access to code (1) A person shall not intentionally, without lawful excuse or justification disclose or obtain a password, an access code or any other means of gaining access to an electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to a person or for any unlawful purpose. (2) A person who contravenes subsection (1) commits an offence and is liable on- (a) summary conviction to a fine of $200,000 or to three years imprisonment, or to both; or (b) conviction on indictment to a fine not exceeding $500,000 and to imprisonment for a term not exceeding seven years, or to both. "

Data Data transfer or transmission Digital infrastructure Electronic crimes Electronic signature Electronic systems Electronic terrorism Encryption Source code

Policy/regulation mirrored:

Computer Misuse Act; Prevention of Electronic Crimes Act

Countries:

Mauritius

Brunei

Pakistan