Botswana

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 01 April 2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	N/A

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Cybercrime and Computer Related Crimes Act, 2018** **Section 2** – In this Act, unless the context otherwise requires- "computer or computer system" means an electronic, magnetic or optical device or a group of interconnected or related devices, including the Internet, one or more of which, pursuant to a programme, performs the automatic processing of data. "data" means — (a) any representation of facts, information or concepts in a form suitable for processing in a computer or computer system; (b) any information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; or (c) any programme suitable to cause a computer or computer system to perform a function, and includes traffic data and subscriber information; "service provider" means any public or private person who — (a) provides to users of its services the ability to communicate by means of a computer or computer system; (b) processes or stores computer data on its behalf or on behalf of the users of its services; or (c) provides an information and communication service, including telecommunication; "traffic data" means any data that — (a) relates to communication by means of a computer or computer system; (b) is generated by a computer or computer system that is part of the chain of communication; and (c) shows the communication's origin, destination, route, time, data, size, duration or type of underlying service;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 4(1)** Subject to subsection (2), any person who — (a) intentionally accesses or attempts to access the whole or any part of a computer or computer system knowing that the access he or she intends to secure is unauthorised; or (b) causes a computer or computer system to perform any function as a result of unauthorised access to such system, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. **(2)** For the purposes of this section, it is immaterial that the unauthorised access is not directed at a — (a) particular programme or data; (b) programme or data of any kind; or (c) programme or data held in any particular computer or computer system
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 9** A person who intentionally, without lawful excuse or justification, and by technical means, intercepts — (a) any non-public transmission to, from or within a computer or computer system; or (b) any electromagnetic emissions that are carrying data from a computer or computer system,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 7(1)** A person who intentionally and without lawful excuse or justification, does or attempts to do any of the following acts — (a) damages, deteriorates, deletes, alters or modifies computer data; (b) renders computer data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of computer data; or (d) denies access to computer data to any person entitled to it, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both. **(2)** Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified — (a) the operation of a computer or computer system; (b) access to any programme or data held in any computer or computer system; or (c) the operation of any programme or the reliability of any data, the person is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Cybercrime and Computer Related Crimes Act, 2018** **Section 8(1)** A person who intentionally, without lawful excuse or justification— (a) hinders or interferes with the functioning of a computer or computer system; or (b) hinders or interferes with a person who is lawfully using or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	operating a computer or computer system, commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both. **(2)** A person who intentionally, without lawful excuse or justification, commits an act which causes, directly or indirectly — (a) a denial, including a partial denial, of access to a computer or computer system; or (b) an impairment of any programme or data stored in a computer or computer system, commits an offence and is liable to a minimum fine of P40 000 or to imprisonment for a minimum term of two years, or to both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise	**Cybercrime and Computer Related Crimes Act, 2018** **Section 10(1)** A person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both. **(2)** A person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and is liable to a fine of P40000 or to imprisonment for a term of two years, or to both. **(3)** A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both. **(4)** For the purposes of subsection (3), "possession of any data or programme" includes having —

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	(a) possession of a computer or computer system or data storage device that holds or contains the data or programme; (b) possession of a document in which the data or programme is recorded; and (c) control of the data or programme that is in the possession of another person. **Section 11** A person who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system — (a) for wrongful gain; (b) for any unlawful purpose; (c) to overcome security measures for the protection of data; or (d) with the knowledge that it is likely to cause prejudice to any person, commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 12(1)** In this section, "computer contaminant" includes any programme which — (a) modifies, destroys, records or transmits any data or programme residing within a computer or computer system; (b) usurps the normal operation of a computer or computer system; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) destroys, damages, degrades or adversely affects the performance of a computer or computer system or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer or computer system. **(2)** A person who intentionally introduces, or causes to be introduced, a computer contaminant into any computer or computer system which causes, or is capable of causing, any of the effects referred to under subsection (1) to such computer or computer system, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 15(1)** A person who performs any of the acts described under this Part, for purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both. **(2)** A person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by — (a) any input, alteration, deletion, delaying transmission or suppression of data; or (b) any interference with the functioning of a computer or computer system, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography	**Cybercrime and Computer Related Crimes Act, 2018** **Section 19(1)** In this section —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(a) "child" means a person who is under the age of 18 years; (b) "child pornography" includes material that visually or otherwise depicts — (i) a child engaged in sexually explicit conduct, (ii) a person who appears to be a child engaged in sexually explicit conduct, or (iii) realistic images representing a child engaged in sexually explicit conduct; and (c) "sexually explicit conduct" means any conduct, whether real or simulated, which involves — (i) sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex, (ii) bestiality, (iii) masturbation, (iv) sadistic or masochistic sexual abuse, or (v) the exhibition of the genitals or pubic area of a child. **(2)** A person who — (a) publishes child pornography or obscene material relating to children through a computer or computer system; (b) produces child pornography or obscene material relating to children for the purpose of its publication through a computer or computer system;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) possesses child pornography or obscene material relating to children in a computer or computer system or on a computer data storage medium; (d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or (e) accesses child pornography or obscene material relating to children through a computer or computer system, commits an offence and is liable to a fine not exceeding P100 000, or to imprisonment for a term not exceeding five years, or to both. **(3)** A person who, by means of a computer or computer system, communicates with a person who is, or who the accused believes is — (a) under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code; (b) under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or (c) under the age of 16 years, for the purpose of facilitating the commission of the offence of defilement or any sexual offence of that person under the Penal Code, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both. **(4)** Evidence that the person in paragraph (a), (b) or (c) of subsection (3) was represented to the accused as being under the age of 18 years or 16 years, as the case may be, shall be, in absence of evidence to the contrary, proof that the accused believed that the person was under that age.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) It shall not be a defence to a charge under subsection (3) that the accused believed that the person he or she was communicating with was at least 16 or 18 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person. **(6)** For the purposes of subsection (3), it does not matter that the person in paragraph (a), (b) or (c) of subsection (3) is a fictitious person, represented to the accused as a real person. **Section 20** A person who, by means of a computer or computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms	**Copyright and Neighbouring Rights, 2006** **Section 31.(1)** Any person who contravenes the provisions of this Act so as to infringe a right protected under this Act for profit, shall be guilty of an offence and upon conviction shall be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding ten years or to both. **(2)** Any person convicted of a second or subsequent offence shall be fined a minimum of P30, 000 or a maximum of P5, 000,000 or be imprisoned for a term not exceeding ten years, or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 7(1)** A person who intentionally and without lawful excuse or justification, does or attempts to do any of the following acts — (a) damages, deteriorates, deletes, alters or modifies computer data; (b) renders computer data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of computer data; or (d) denies access to computer data to any person entitled to it, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both. **(2)** Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified — (a) the operation of a computer or computer system; (b) access to any programme or data held in any computer or computer system; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) the operation of any programme or the reliability of any data, the person is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. **Section 18** A person who willfully, maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. **Penal Code, 1964** **Section 21 (1)** When an offence is committed, each of the following persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say — (a)…; (b) every person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence; (c) every person who aids or abets another person in committing the offence; (d) any person who counsels or procures any other person to commit the offence, and in the last-mentioned case he may be charged either with committing the offence or with counselling or procuring its commission. **(2)** A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence. **Section 388**. Attempt defined **(1)** When a person, intending to commit an offence, begins to put his intention into execution by means adapted to its fulfilment, and manifests his intention by

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	some overt act, but does not fulfil his intention to such an extent as to commit the offence, he is deemed to attempt to commit the offence. **(2)** It is immaterial, except so far as regards punishment, whether the offender does all that is necessary on his part for completing the commission of the offence, or whether the complete fulfilment of his intention is prevented by circumstances independent of his will, or whether he desists of his own motion from the further prosecution of his intention. **(3)** It is immaterial that by reason of circumstances not known to the offender it is impossible in fact to commit the offence. **Section 389** Attempts to commit offences Any person who attempts to commit an offence is guilty of an offence. **Section 390.** Punishment of attempts to commit certain offences Any person who attempts to commit an offence of such a kind that a person convicted of it is liable to the punishment of imprisonment for a term of 14 years or more, with or without other punishment, is liable, if no other punishment is provided, to imprisonment for a term not exceeding seven years. **Section 391**. Soliciting or inciting others to commit offence Any person who solicits or incites or attempts to procure another to do any act or make any omission of such a nature that, if the act were done or the omission were made, whether by himself or that other person, an offence would thereby be committed, is guilty of an offence and liable to the same punishment as if he had himself attempted to commit that offence.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person;	**Criminal Procedure and Evidence Act 08:02** **Section 332** Liability to punishment in case of offences by corporate bodies, partnerships, etc. **(1)** In any criminal proceedings under any enactment against a company, the secretary and every director or manager or chairman thereof in Botswana may, unless it is otherwise directed or provided, be charged with the offence and shall

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	be liable to be punished therefor, unless it is proved that he did not take part in the commission of the offence, and that he could not have prevented it. **(2)** In any such proceedings against a local authority, the mayor, chairman, city or town clerk, secretary or other similar officer shall, unless it is otherwise directed or provided, be liable to be so charged, and in like circumstances punished for the offence. **(3)** In any such proceedings against a partnership, every member of such partnership who is in Botswana shall, unless it is otherwise directed or provided, be liable to be so charged, and in like circumstances punished for the offence. **(4)** In any such proceedings against any association of persons not specifically mentioned in this section, the president, chairman, secretary, and every other officer thereof in Botswana shall, unless it is otherwise directed or provided, be liable to be so charged, and in like circumstances punished for the offence. **(5)** Nothing in this section shall be deemed to exempt from liability any other person guilty of the offence. **(6)** In any criminal proceedings against a corporate body, any record which was made or kept by a director, servant or agent of the corporate body within the scope of his activities as such director, servant or agent, or any document which was at any time in the custody or under the control of any such director, servant or agent within the scope of his activities as such director, servant or agent, shall be admissible in evidence against the accused. **(7)** For the purposes of subsection (6) any record made or kept by a director, servant or agent of a corporate body or any document which was at any time in his custody or control shall be presumed to have been made or kept by him or to have been in his custody or control within the scope of his activities as such director, servant or agent, unless the contrary is proved. **(8)** In any proceedings against a director or servant of a corporate body in respect of an offence, any evidence which would be or was admissible against that corporate body in a prosecution for that offence, shall be admissible against that director or servant. **(9)** In this section the word "director" in relation to a corporate body means any person who controls or governs that corporate body or who is a member of a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	body or group of persons which controls or governs that corporate body or where there is no such body or group, who is a member of that corporate body.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**ARTICLE 2** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 4(1)** Subject to subsection (2), any person who — (a) intentionally accesses or attempts to access the whole or any part of a computer or computer system knowing that the access he or she intends to secure is unauthorised; or (b) causes a computer or computer system to perform any function as a result of unauthorised access to such system, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. **ARTICLE 3** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 9** A person who intentionally, without lawful excuse or justification, and by technical means, intercepts — (a) any non-public transmission to, from or within a computer or computer system; or (b) any electromagnetic emissions that are carrying data from a computer or computer system, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both **ARTICLE 4** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 7(1)** A person who intentionally and without lawful excuse or justification, does or attempts to do any of the following acts —

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) damages, deteriorates, deletes, alters or modifies computer data; (b) renders computer data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of computer data; or (d) denies access to computer data to any person entitled to it, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both. **(2)** Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified — (a) the operation of a computer or computer system; (b) access to any programme or data held in any computer or computer system; or (c) the operation of any programme or the reliability of any data, the person is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both. **ARTICLE 5** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 8(1)** A person who intentionally, without lawful excuse or justification— (a) hinders or interferes with the functioning of a computer or computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer or computer system, commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both. **(2)** A person who intentionally, without lawful excuse or justification, commits

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	an act which causes, directly or indirectly — (a) a denial, including a partial denial, of access to a computer or computer system; or (b) an impairment of any programme or data stored in a computer or computer system, commits an offence and is liable to a minimum fine of P40 000 or to imprisonment for a minimum term of two years, or to both. **ARTICLE 6** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 10(1)** A person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both. **(2)** A person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and is liable to a fine of P40000 or to imprisonment for a term of two years, or to both. **(3)** A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both. **Section 11** A person who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system — (a) for wrongful gain;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) for any unlawful purpose; (c) to overcome security measures for the protection of data; or (d) with the knowledge that it is likely to cause prejudice to any person, commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both. **ARTICLE 7** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 12(2)** A person who intentionally introduces, or causes to be introduced, a computer contaminant into any computer or computer system which causes, or is capable of causing, any of the effects referred to under subsection (1) to such computer or computer system, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both **ARTICLE 8** **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 15(1)** A person who performs any of the acts described under this Part, for purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both. **(2)** A person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by — (a) any input, alteration, deletion, delaying transmission or suppression of data; or (b) any interference with the functioning of a computer or computer system, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ARTICLE 9 **(Cybercrime and Computer Related Crimes Act, 2018)** **Section 20** A person who, by means of a computer or computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both. **ARTICLE 10** **(Copyright and Neighbouring Rights, 2006)** **Section 31.(1)** Any person who contravenes the provisions of this Act so as to infringe a right protected under this Act for profit, shall be guilty of an offence and upon conviction shall be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding ten years or to both. **(2)** Any person convicted of a second or subsequent offence shall be fined a minimum of P30, 000 or a maximum of P5, 000,000 or be imprisoned for a term not exceeding ten years, or to both. **ARTICLE 11** **(Penal Code, 1964)** **Section 21 (1)** When an offence is committed, each of the following persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say — (a)…; (b) every person who does or omits to do any act for the purpose of enabling or aiding another person to commit the offence; (c) every person who aids or abets another person in committing the offence;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) any person who counsels or procures any other person to commit the offence, and in the last-mentioned case he may be charged either with committing the offence or with counselling or procuring its commission. **(2)** A conviction of counselling or procuring the commission of an offence entails the same consequences in all respects as a conviction of committing the offence.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and	**Criminal procedure and evidence Act Cap 08:02** **Section 123(1)** When a person charged with an offence has been committed for trial or sentence before the High Court, the charge shall be in writing in a document called an indictment. **(2)** When the prosecution is – (a) at the public instance, the indictment shall be in the name of, and shall be signed by, the Director of Public Prosecutions; (b) a private one, the indictment shall be in the name of the party at whose instance it is preferred (who must be described therein with certainty and precision) and must be signed by such private party or by counsel on his behalf. **(3)** It shall not be competent for two or more persons to prosecute in the same indictment, except in a case where two or more persons have been injured by the same offence. **(4**) The service upon an accused person of any indictment, together with any notice of trial thereof, shall be made by the person and in the manner provided by rules of court. **Electronic Records (Evidence) act Cap. 11:06**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	**Section 5(1)** Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record. **(2)** A court may have regard to evidence adduced under this Act in applying any common law rule relating to the admissibility of electronic records. **(3)** Notwithstanding section 244 of the Criminal Procedure and Evidence Act, in so far as it relates to the signing and certification of a copy of, or extract from a book or record as true copy or extract, and subject to subsection (4), a person may seek the admission of such copies or extracts from a book or record and of entries in bankers' books in electronic form as evidence in any legal proceedings **Electronic Communications and Transactions Cap. 43:12** **Section (1)** Subject to the Electronic Records (Evidence) Act, in any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of an electronic communication in communications evidence — (a) solely on the ground that it is an electronic communication; or (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. **(2)** Information in the form of an electronic communication shall be given due evidential weight. **(3)** In assessing the evidential weight of an electronic communication, regard shall be had to — (a) the reliability of the manner in which the data message was generated, stored or communicated; (b) the reliability of the manner in which the integrity of the electronic communication was maintained;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) the manner in which the originator of the data message was identified; and (d) any other relevant circumstances. **Cybercrime and Computer Related Crimes Act, 2018** **Section 24**. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Constitution of Botswana** **CHAPTER II** **Protection of Fundamental Rights and Freedoms of the Individual** **Section 3** Fundamental rights and freedoms of the individual **Section 5.** Protection of right to personal liberty **Section 6**. Protection from slavery and forced labour **Section 7.** Protection from inhuman treatment **Section 8** Protection from deprivation of property **Section 9**. Protection for privacy of home and other property **Section 10.** Provisions to secure protection of law **Section 11**. Protection of freedom of conscience **Section 12**. Protection of freedom of expression **Section 13**. Protection of freedom of assembly and association **Section 14.** Protection of freedom of movement **Section 15.** Protection from discrimination on the grounds of race, etc. **Section 16**. Derogation from fundamental rights and freedoms
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the	**Cybercrime and Computer Related Crimes Act, 2018**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 24**. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 25** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to — (a ensure that the data specified in the notice is preserved for the period specified in the notice; or (b) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Cybercrime and Computer Related Crimes Act, 2018 **Section 26 (1)** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer for an order compelling — (a) a person to submit specified data in that person's possession or control, which is stored in a computer or computer system; and (b) a service provider to submit subscriber information in relation to its services in that service provider's possession or control. **(2)** Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible. **ELECTRONIC RECORDS (EVIDENCE) ACT, 2014** **Section 12(1)** Where a court is not satisfied that the electronic record sought to be admitted in evidence under section 4 accurately reproduces the relevant contents of the original record, the court may, in its discretion, call for further evidence. **(2)** Where further evidence is called for under subsection (1), such evidence may be established by an affidavit made by — (a) a person holding a responsible position in relation to the operation or management of the certifying authority appointed under section 6 (2); (b) any other person holding a responsible position in relation to the operation of the electronic records system at the relevant time; (c) the person who had control or access over any relevant records and facts in relation to the production of the electronic record;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) the person who had obtained or been given control or access over any relevant records and facts in relation to the production of the electronic record; or (e) an expert appointed or accepted by the court. **(3)** Notwithstanding subsections (1) and (2), the court may, if it thinks fit, require that oral evidence be given of any matters concerning the authenticity of the electronic record, and may call a deponent of an affidavit under subsection (2) or any person responsible for a certificate issued under section 6 for this purpose.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 27(1)** Where a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information. **(2)** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, in the execution of an order issued under subsection (1), shall — (a) seize or secure a computer or computer system or any information and communication technology medium; (b) make and retain a copy of such data or information; (c) maintain the integrity of the relevant stored data or information; (d) print, photograph, copy or make in any other manner for the purpose of doing an act referred to in paragraph (a); or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(e) render inaccessible or remove the stored data or information from the computer or computer system, or any information and communication technology medium. **(3)** A police officer or any person authorised by the Commissioner or Director-General, in writing, in the execution of an order issued under subsection (1), may order any person who has knowledge about the functioning of the computer system or the measures provided under subsection (2) to protect the data contained therein in order to provide, as is reasonable, the necessary information to enable the undertaking of the measures provided under subsection (2).
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime and Computer Related Crimes Act, 2018** Section 28. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer, ex-parte, for an order — (a) for the collection or recording of content or traffic data, in real time, associated with specified communications transmitted by means of a computer or computer system; or (b) compelling a service provider, within its technical capabilities, to — (i) effect such collection and recording referred to in paragraph (a), or (ii) assist the person making the application to effect such collection and recording.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 9** A person who intentionally, without lawful excuse or justification, and by technical means, intercepts — (a) any non-public transmission to, from or within a computer or computer system; or (b) any electromagnetic emissions that are carrying data from a computer or computer system, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 3** The courts of Botswana shall have jurisdiction where an act or an omission constituting an offence under this Act has been committed — (a) in the territory of Botswana; (b) by a national of Botswana outside the territory of Botswana, if the person's conduct would also constitute an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	(c) on a ship or aircraft registered in Botswana; (d) in part in Botswana; or (e) outside the territory of Botswana and where any result of the offence has an effect in Botswana.
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis	**Mutual Assistance in Criminal Matters Act of 1990** **Section 38** Nothing in this Act shall be construed as authorising the extradition, or arrest or detention with a view to extradition, of any person.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	**Mutual Assistance in Criminal Matters Act Cap. 08:04, Mutual Assistance in Criminal Matters (Amendment) Act of 2018** **SECTION 3(1)** Where an arrangement has been made with a foreign country for mutual assistance in criminal matters, the Minister may by statutory instrument make regulations that this Act shall apply to that country. **(2)** Regulations made under subsection (1) may provide that the application of this Act to a foreign country shall be subject to such limitations, conditions,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	exceptions or qualifications as are necessary to give effect to an arrangement made between Botswana and that country. **Section 4.** The object of this Act is to facilitate the provision and obtaining by Botswana of international assistance in criminal matters, including — (a) the obtaining of evidence, exhibits, documents and other articles; (b) the provision of documents and other records; (c) the location and identification of witnesses or suspects and recording of statements; (d) the execution of requests for search and seizure; (e) the making of arrangements for persons to give evidence in person or through video conferencing or assist investigations; (f) the confiscation of property in respect of offences; (g) the recovery of pecuniary penalties in respect of offences; (h) the restraining of dealings in property, or the freezing of assets, that may be confiscated, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences; (i) the location of property that may be confiscated, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences; (j) the service of documents; and (k) joint criminal investigations into an offence **Section 5(1)** A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the request relates to the prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character; (b) subject to subsection (3), there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for an offence of a political character; (c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of his race, sex, religion, nationality or political opinions; (d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Botswana, would have constituted an offence under the military law of Botswana but not also under the ordinary criminal law of Botswana; (e) the granting of the request would prejudice the sovereignty, security or national interest of Botswana; (f) the request relates to the prosecution of a person for an offence in a case where he has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence; or (g) except in the case of a request under section 10, the foreign country is not a country to which this Act applies. (2) A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Attorney-General —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Botswana, would not have constituted an offence against the laws of Botswana; (b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Botswana in similar circumstances would not have constituted an offence against the laws of Botswana; (c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Botswana at the same time and had constituted an offence against the laws of Botswana, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; (d the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Botswana; (e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Botswana); (f) the provision of the assistance would impose an excessive burden on the resources of the State; or (g) the provision of assistance would involve infliction of pain, injury or psychological harm in order to enhance the credibility of an existing threat of any kind to a person in or outside Botswana. **(3)** An offence is not an offence of a political character— (a) if it is an offence in accordance with the provisions of any international convention to which Botswana and the foreign country to which this Act applies are parties and there is an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	obligation on each party to afford mutual assistance in investigation and prosecution of such offence; (b) if it is an offence against the life or person of a Head of State or a member of his immediate family, a Head of Government, or a Minister or any related offence; (c) if it is murder or any related offence. **(4)** For the purposes of subsection (3) (b) and (c), "related offence" means aiding and abetting, counselling or procuring the commission of, being an accessory before or after the fact to, or attempting or conspiring to commit that offence. **Section 6.** Assistance under this Act may be provided to a foreign country subject to such conditions as the Attorney-General may determine. **Section 7** Requests by Botswana for international assistance in criminal matters may be made by the Attorney-General. **Section 8(1)** A request by a foreign country for international assistance in a criminal matter may be made to the Attorney-General or a person authorised by the Attorney-General, in writing, to receive requests by foreign countries under this Act **(2)** A request made under subsection (1) shall be accompanied by- (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) details of the procedure that the foreign country wishes to be followed by Botswana in giving effect to the request, including details of the manner and form in which any information, document or thing is to be supplied to the foreign country pursuant to the request; (e) a statement setting out the wishes of the foreign country concerning the confidentiality of the request and the reasons for those wishes; (f) details of the period within which the foreign country wishes the request be complied with; (g) if the request involves a person travelling from Botswana to the foreign country, details of allowances to which the person will be entitled, and of the arrangements for accommodation for the person, while the person is in the foreign country pursuant to the request; (h) any other information required to be included with the request under an arrangement between Botswana and the foreign country; and (i) any other information that may assist in giving effect to the request; but failure to comply with this subsection is not a ground for refusing the request. **(3)** Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Attorney-General.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or	**Mutual assistance in criminal matters Act Cap. 08:04** **Section 8(1)** A request by a foreign country for international assistance in a criminal matter may be made to the Director of Public Prosecutions or a person authorised by the Director of Public Prosecutions, in writing, to receive requests by foreign countries under this Act. (2) A request made under subsection (1) shall be accompanied by- (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; (d) details of the procedure that the foreign country wishes to be followed by Botswana in giving effect to the request, including details of the manner and form in which any information, document or thing is to be supplied to the foreign country pursuant to the request; (e) a statement setting out the wishes of the foreign country concerning the confidentiality of the request and the reasons for those wishes;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the	(f) details of the period within which the foreign country wishes the request be complied with; (g) if the request involves a person travelling from Botswana to the foreign country, details of allowances to which the person will be entitled, and of the arrangements for accommodation for the person, while the person is in the foreign country pursuant to the request; (h) any other information required to be included with the request under an arrangement between Botswana and the foreign country; and (i) any other information that may assist in giving effect to the request; but failure to comply with this subsection is not a ground for refusing the request. **(3)** Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Director of Public Prosecutions. Section 10.(1) Where a request is made by a foreign country that- (a) evidence be taken in Botswana; or (b) documents or other articles in Botswana be produced, for the purposes of a proceeding in relation to a criminal matter in the foreign country, the Director of Public Prosecutions may by writing in accordance with the approved form, authorise the taking of the evidence or the production of the documents or other articles, and the transmission of the evidence, documents or other articles to the foreign country. (2) Where the Director of Public Prosecutions authorises the taking of evidence or the production of documents or other articles under subsection (1)-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	(a) in the case of taking evidence, a magistrate may take the evidence on oath of each witness appearing before him to give evidence in relation to the matter, and a magistrate who takes any such evidence shall- (i) cause the evidence to be put in writing and certify that the evidence was taken by him; and (ii) cause the writing so certified to be sent to the Director of Public Prosecutions; or (b) in the case of the production of documents or other articles, a magistrate may require the production of the documents or other articles and, where the documents or other articles are produced, he shall send the documents, or copies of the documents certified by him to be true copies, or the other articles, to the Director of Public Prosecutions. **(3)** The evidence of such a witness may be taken in the presence or absence of the person to whom the proceeding in the foreign country relates or of his legal representative, if any. **(4)** The magistrate conducting a proceeding under subsection (2) may permit- (a) the person to whom the proceeding in the foreign country relates; (b) any other person giving evidence or producing documents or other articles at the proceeding before the magistrate; and (c) the relevant authority of the foreign country, to have legal representation at the proceeding before him. **(5)** The certificate by the magistrate under subsection (2) shall state whether, when the evidence was taken or the documents or other articles were produced, any of the following persons were present-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the person to whom the proceeding in the foreign country relates or his legal representative, if any; (b) any other person giving evidence or producing documents or other articles or his legal representative, if any. **(6)** For the purposes of this section, the person to whom the proceeding in the foreign country relates is competent but not compellable to give evidence
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Mutual assistance in criminal matters Act Cap. 08:04** **Section 6** Assistance may be provided subject to conditions Assistance under this Act may be provided to a foreign country subject to such conditions as the Director of Public Prosecutions may determine.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation;	**Cybercrime and Computer Related Crimes Act, 2018** **Section 24** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure	**Section 25** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to — (a) ensure that the data specified in the notice is preserved for the period specified in the notice; or (b) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted. **Section 26(1)** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer for an order compelling — (a) a person to submit specified data in that person's possession or control, which is stored in a computer or computer system; and (b) a service provider to submit subscriber information in relation to its services in that service provider's possession or control. **(2)** Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible. **Section 27(1)** Where a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information. **(2)** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, in the execution of an order issued under subsection (1), shall —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	(a) seize or secure a computer or computer system or any information and communication technology medium; (b) make and retain a copy of such data or information; (c) maintain the integrity of the relevant stored data or information; (d) print, photograph, copy or make in any other manner for the purpose of doing an act referred to in paragraph (a); or (e) render inaccessible or remove the stored data or information from the computer or computer system, or any information and communication technology medium. **(3)** A police officer or any person authorised by the Commissioner or Director-General, in writing, in the execution of an order issued under subsection (1), may order any person who has knowledge about the functioning of the computer system or the measures provided under subsection (2) to protect the data contained therein in order to provide, as is reasonable, the necessary information to enable the undertaking of the measures provided under subsection (2).
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Cybercrime and Computer Related Crimes Act, 2018** **Section 25** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to — (a) ensure that the data specified in the notice is preserved for the period specified in the notice; or (b) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted. **Section 26(1)** A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer for an order compelling —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) a person to submit specified data in that person's possession or control, which is stored in a computer or computer system; and (b) a service provider to submit subscriber information in relation to its services in that service provider's possession or control. **(2)** Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible. **Mutual assistance in criminal matters Act Cap. 08:04** **Section 5.(1)** A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Director of Public Prosecutions- (a) the request relates to the prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character; (b) subject to subsection (3), there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for an offence of a political character; (c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of his race, sex, religion, nationality or political opinions; (d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Botswana, would have constituted an offence under the military law of Botswana but not also under the ordinary criminal law of Botswana;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) the granting of the request would prejudice the sovereignty, security or national interest of Botswana; (f) the request relates to the prosecution of a person for an offence in a case where he has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence; or (g) except in the case of a request under section 10, the foreign country is not a country to which this Act applies. **(2)** A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Director of Public Prosecutions- (a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Botswana, would not have constituted an offence against the laws of Botswana; (b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Botswana in similar circumstances would not have constituted an offence against the laws of Botswana; (c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Botswana at the same time and had constituted an offence against the laws of Botswana, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; (d) the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Botswana;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Botswana); or (f) the provision of the assistance would impose an excessive burden on the resources of the State. **(3)** An offence is not an offence of a political character- (a) if it is an offence in accordance with the provisions of any international convention to which Botswana and the foreign country to which this Act applies are parties and there is an obligation on each party to afford mutual assistance in investigation and prosecution of such offence; (b) if it is an offence against the life or person of a Head of State or a member of his immediate family, a Head of Government, or a Minister or any related offence; (c) if it is murder or any related offence. **(4)** For the purposes of subsection (3)(b) and (c), "related offence" means aiding and abetting, counselling or procuring the commission of, being an accessory before or after the fact to, or attempting or conspiring to commit that offence.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where:	**Cybercrime and Computer Related Crimes Act, 2018** Section 27(1) Where a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	(2) A police officer or any person authorised by the Commissioner or by the Director-General, in writing, in the execution of an order issued under subsection (1), shall — (a) seize or secure a computer or computer system or any information and communication technology medium; (b) make and retain a copy of such data or information; (c) maintain the integrity of the relevant stored data or information; (d) print, photograph, copy or make in any other manner for the purpose of doing an act referred to in paragraph (a); or (e) render inaccessible or remove the stored data or information from the computer or computer system, or any information and communication technology medium. **(3)** A police officer or any person authorised by the Commissioner or Director-General, in writing, in the execution of an order issued under subsection (1), may order any person who has knowledge about the functioning of the computer system or the measures provided under subsection (2) to protect the data contained therein in order to provide, as is reasonable, the necessary information to enable the undertaking of the measures provided under subsection (2). **Mutual Assistance in criminal matters (Amendment) Act, 2018** **Section 14 (2)** Where information about a transaction conducted through an account with an institution in Botswana is reasonably believed to be relevant to the proceedings or investigations, the Director of Public Prosecutions may authorise the law enforcement officer to apply to a magistrate or a judge of the High Court for the order requested by the foreign country.”.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30;	**Mutual assistance in criminal matters Act Cap. 08:04** **Section 8(1)** A request by a foreign country for international assistance in a criminal matter may be made to the Director of Public Prosecutions or a person authorised by the Director of Public Prosecutions, in writing, to receive requests by foreign countries under this Act. **(2)** A request made under subsection (1) shall be accompanied by-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	(*a*) the name of the authority concerned with the criminal matter to which the request relates; (*b*) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (*c*) a description of the purpose of the request and of the nature of the assistance being sought; (*d*) details of the procedure that the foreign country wishes to be followed by Botswana in giving effect to the request, including details of the manner and form in which any information, document or thing is to be supplied to the foreign country pursuant to the request; (*e*) a statement setting out the wishes of the foreign country concerning the confidentiality of the request and the reasons for those wishes; (*f*) details of the period within which the foreign country wishes the request be complied with; (*g*) if the request involves a person travelling from Botswana to the foreign country, details of allowances to which the person will be entitled, and of the arrangements for accommodation for the person, while the person is in the foreign country pursuant to the request; (*h*) any other information required to be included with the request under an arrangement between Botswana and the foreign country; and (*i*) any other information that may assist in giving effect to the request; but failure to comply with this subsection is not a ground for refusing the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Director of Public Prosecutions
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents