Ghana

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [19.03.2020]

[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.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	
Ratification/accession:	03/12/2018

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	**S.144 of Act 772 Electronic Transactions Act 2008** 1. "computer" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function but does not include (a) portable hand-held calculator, (b) an automated typewriter or typesetter, (c) a similar device which is non-programmable or which does not contain any data storage facility, or (d) any other device that the Minister may prescribe in the Gazette; 2. "Service provider" means any person providing information system services. 3. Electronic Record: includes data generated, sent, received or stored by electronic means: (a) Voice, where voice is used in an automated transaction; and (b) A stored record 4. Electronic Agent: means a computer programme or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, in an automated

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	transaction. 5. Information System Services: "information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of electronic records between or among points specified by a user and the processing and storage of data at the individual request of the recipient of the service;
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.	**Electronic Transactions Act, 2008 (Act 772)** **Access to protected computer** S.118. A person who secures unauthorised access or attempts to secure access to a protected system in contravention of a provision of this Act commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both. **Section 144 of the Electronic Transactions Act, 2008 (Act 772) (Interpretation)** "access" includes the actions of a person who, after taking note of data, becomes aware of the fact that there is no authorisa-tion to access that data and still continues to access that data; "unauthorised access" is access of any kind by a person to a programme or data held in a computer without authority if (a) the person is not personally entitled to control access of the kind in question to the programme or data; and (b) the person does not have consent to access the kind of programme or data from the person who is entitled to control access;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Electronic Transactions Act, 2008 (Act 772)** **S 124: Unauthorized access or interception:** A person who intentionally accesses or intercepts an electronic record without authority or permission commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both. **Unlawful access to stored communications** 129. (1) Whoever, without lawful authority, intentionally accesses a facility through which an electronic communication service is provided, commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both (2) Whoever without lawful authority exceeds an authorisation to access a facility or obtains, alters, or prevents authorised access to **a wire or electronic communication** while it is in electronic storage in a system commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both. **Section 144 of the Electronic Transactions Act, 2008 (Act 772) (Interpretation)** "intercept" includes, in relation to a function of a computer or electronic record, listening to or recording a function of a computer or electronic record, or acquiring the substance, meaning or purport of it;
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.	**Electronic Transactions Act, 2008 (Act 772)** **S 125: Unauthorized interference with electronic record** A person who intentionally and without authority interferes with an electronic record in a way which causes the electronic record to be modified, destroyed or otherwise rendered ineffective, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	S 131(1): Unauthorized modification of computer programme or electronic record A Person who does any direct or an indirect act without authority which the person knows or ought to have known will cause an unauthorised modification of any programme or electronic record held in a computer commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both. **Unauthorised access to computer programme or electronic record** 130. (1) A person who knowing and without authority causes a computer to perform any function to secure access to a programme or electronic record held in that computer or in any other computer, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both. (2) For the purposes of sections 107 to 141, it is immaterial that the act in question is not directed at (a) a particular programme or electronic record, (b) a programme or electronic record of any kind, or (c) a programme or electronic record held in any particular computer. (3) A person secures or gains access to a programme or electronic record held in a computer if by causing the computer to perform any function, the person (a) alters or erases the programme or electronic record, (b) copies or moves it to a storage medium other than that in which it is held or to a different location in the storage medium in which it is held, (c) uses it, or (d) causes it to be output from the computer in which it is held, whether by

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	having it displayed or in any other manner, and references to access to a programme or electronic record and to an intent to secure the access, shall be read accordingly. (4) A person uses a programme if the function the person causes the computer to perform (a) causes the programme to be executed, or (b) is itself a function of the programme. (5) For the purposes of this Act, the form of any programme or electronic record is immaterial. **Unauthorised modification of computer programme or electronic record** 131. (1) A person who does any direct or an indirect act without authority which the person knows or ought to have known will cause an **unauthorised modification** of any programme or electronic record held in a computer commits an offence and is liable on summary conviction to a fine of not more that five thousand penalty units or a term of imprisonment of not more than ten years or to both. (2) It is immaterial that the act in question is not directed at (a) any particular programme or electronic record, (b) a programme or electronic record of any kind, (c) a programme or electronic record held in any particular computer, or (d) any unauthorised modification is, or is intended to be, permanent or merely temporary. (3) A modification of a programme or electronic record occurs if, by the operation of a function of the computer concerned or any other computer, (a) a programme or electronic record held in the computer is **altered** or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	erased, (b) a programme or electronic record is **added to or removed** from a programme or electronic record held in the computer, or (c) an act occurs which **impairs the normal operation of any computer**. 4) An act which contributes towards causing a modification is regarded as causing it. (5) A modification is unauthorised if the person who causes it (a) is not entitled to determine whether the modification should be made, (b) is not authorised to make the modification or knowingly acted in excess of the authorised modification, or (c) does not have consent to the modification from the person who is entitled.
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	**Electronic Transactions Act, 2008 (Act 772)** **S 128: Denial of Service** A person who commits any act described in this Act with intent to interfere with access to an information system to effect a denial, including a partial denial of service to legitimate users commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or a term of imprisonment of not more than two years or to both. **S 134: Causing a Computer to cease to function** A person who intentionally engages in conduct, including virus writing, virus and worm dissemination which causes a computer to cease to function permanently or temporarily commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to imprisonment for a term of not more than ten years or to both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be	**Electronic Transactions Act, 2008 (Act 772)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**S 135 Illegal Devices** A person who intentionally, recklessly, without lawful excuse or justification, possesses, produces, procures for use, imports, exports distribute or otherwise makes available (a) A device, including a computer programme, that is designed or adapted for the purpose of committing an offence or (b) A computer password, access code or similar electronic record which the whole or any part of a computer system is capable of being accessed With the intent that it be used by a person for an offence commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both. **S 126 Unauthorised access to devices** A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapt for use, distributes or possesses any device, including a computer programme or a component, which is designed primarily to overcome security measures for the protection of an electronic record, or performs any of those functions with regard to a password access code or any other similar kind of electronic record, commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years or to both. **S134 Causing a computer to cease to function** A person who intentionally engages in conduct, including virus writing, virus and worm dissemination which causes a computer to cease to function permanently or temporarily commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to imprisonment for a term of not more than ten years or to both. **S127 Unauthorised Circumvention** A person who without lawful authority utilises a device or computer programme in order to overcome security measures designed to protect the electronic

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	record or access to it commits an offence and is liable on summary conviction to a fine of more than two thousand five hundred penalty units or to a term of imprisonment of not more than five years 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.	**Electronic Transactions Act, 2008 (Act 772)** **Section 115 Forgery** Sections 158, 159, 161, 162, 164, 166, 167, 168, 169 and 170 of the Criminal Offences Act, 1960 (Act 29) on forgery apply with the necessary modification to any person who forges anything whether or not the forgery is in whole or in part effected by use of any electronic processor in electronic form. **Section 109 Representation** Section 133 of the Criminal Offences Act, 1960 (Act 29) on false pretences applies with the necessary modification to a representation whether or not the medium used in communicating the representation in part or in whole was an electronic processing system and whether or not the representation consists of an electronic record in part or in whole. **Criminal Offences Act, 1960 (Act 29)** (references made in the ETA on forgery and representation are indicated below) **Section 133—Definition of and Provisions Relating to a False Pretence** (1) A false pretence is a representation of the existence of a state of facts made by a person, either with the knowledge that such representation is false or without the belief that it is true, and made with an intent to defraud. (2) For the purpose of this section — (a) a representation may be made either by written or spoken words, or by personation, or by any other conduct, sign, or means of whatsoever kind; (b) the expression "a representation of the existence of a state of facts" includes a representation as to the non-existence of any thing or condition of things, and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a representation of any right, liability, authority, ability, dignity or ground of credit or confidence as resulting from any alleged past facts or state of facts, but does not include a mere representation of any intention or state of mind in the persons making the representation, nor any mere representation or promise that anything will happen or be done, or is likely to happen or be done; (c) a consent shall not be deemed to have been obtained by a false representation as to the quality or value of a thing, unless, the thing is substantially worthless for the purpose for which it is represented to be fit, or to have been substantially a different thing from that which it is represented to be; and (d) subject to the foregoing rules, if the consent of a person is in fact obtained by a false pretence, it is immaterial that the pretence is such as would have had no effect on the mind of a person using ordinary care and judgment. **Section 158—Forgery of Judicial or Official Document** Whoever, with intent to deceive any person, forges any judicial or official document, shall be guilty of second degree felony. **Section 159—Forgery of Other Documents** Whoever forges any document whatsoever, with intent to defraud or injure any person, or with intent to evade the requirements of the law, or with intent to commit, or to facilitate the commission of, any crime, shall be guilty of a misdemeanour. **Section 160—Forging Hall-mark on Gold or Silver Plate or Bullion** Whoever with intent to defraud, forges or counterfeits any hall-mark or make appointed, under authority of law, by any corporation or public officer to denote the weight, fineness, or age, or place of manufacture of any gold or silver plate or bullion, shall be guilty of a misdemeanour. **Section 161—Forging Trade Mark, etc.** Whoever forges or counterfeits any trade-mark, or marks with a forged or counterfeited trade-mark any goods or anything used in, or about, or in connection with the sale of any goods, or sells or offers for sale any goods or such thing so marked, or has in his possession, custody, or control any goods of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	such thing so marked, or any materials or means prepared or contrived for the forging or counterfeiting of any trade-mark, or for the marking of any goods or thing therewith, intending in any such case fraudulently to pass off, or to enable any other person fraudulently to pass off, any goods as having been lawfully marked with the trade-mark or as being of a character signified by the trade-mark, shall be guilty of a misdemeanour. **Section 162—Forgery of and Other Offences Relating to Stamps** Whoever — (a) forges any stamp, whether impressed or adhesive, used for the purposes of revenue by the Government, or by any foreign country; or (b) without lawful excuse (the proof whereof shall lie on him) makes or has knowingly in his possession any die or instrument capable of making the impression of any such stamp; or (c) fraudulently cuts, tears, or in any way removes from any material any stamp used for purposes of revenue by the Government, with intent that any use should be made of such stamp or of any part thereof; or (d) fraudulently mutilates any stamp to which paragraph (c) applies, with intent that use should be made of any part of the stamp; or (e) fraudulently fixes or places upon any material, or upon any stamp to which paragraph (c) applies, any stamp or part of a stamp which, whether fraudulently or not, has been cut, torn, or in any way removed any other material or out of or from any other stamp; or (f) fraudulently erases or otherwise either really or apparently removes from any stamped material any name, sum, date, or other matter or thing whatsoever written thereon, with the intent that any use should be made of the stamp upon such material; or (g) knowingly and without lawful excuse (the proof whereof shall lie upon him) has in his possession any stamp or part of a stamp which has been fraudulently cut, torn, or otherwise removed from any material, or any stamp which has been fraudulently mutilated, or any stamped material out of which any name, sum, date, or other matter or thing has been fraudulently erased, or otherwise

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	either really or apparently removed, shall be liable to a fine not exceeding ¢1 million. **Section 163—Definition of Trade-Mark, and Official Document** (1) In this Chapter, "trade-mark" means any mark, label, ticket, or other sign or device lawfully appropriated by any person as a means of denoting that any article of trade, manufacture, or merchandise is an article of the manufacture, workmanship, production, or merchandise of any person, or is an article or any peculiar or particular description made or sold by any person, and also means any mark, sign, or device which, in pursuance of any enactment relating to registered designs, is to be put or placed upon, or attached to, any article during the existence or continuance of any copyright or other peculiar right in respect thereof. (2) A mark, label, ticket, or other sign or device shall not be deemed to be lawfully appropriated by a person, within the meaning of this section, unless it is of such a kind and so appropriated as that an injunction or other process would be granted by the Court to restrain the use thereof by any person without the consent of the person by whom it is appropriated, or that an action might be maintained by the last mentioned person against any other person making use thereof without his consent. (3) In this Chapter "official document" means any document purporting to be made, used, or issued by any public officer for any purpose relating to his office. **Section 164—Special Provisions Relating to Forgery** The following provisions apply to forgery, namely — (a) a person forges a document if he makes or alters the document, or any material part thereof, with intent to cause it to be believed— (i) that the document or part has been so made or altered by any person who did not in fact so make or alter it; or (ii) that the document or part has been so made or altered with the authority or consent of any person who did not in fact give his authority or consent; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) that the document or part has been so made or altered at a time different from that at which it was in fact so made or altered; (b) a person who issues or uses any document which is exhausted or cancelled, with intent that it may pass or have effect as if it were not exhausted or cancelled, shall be deemed guilty of forging it; (c) the making or alteration of a document or part by a person in his own name may be forgery if the making or alteration is with any of the intents mentioned in this section; (d) the making or alteration of a document or part by a person in a name which is not his real or ordinary name is not forgery unless the making or alteration is with one or other of the intents mentioned in this section; (e) it is immaterial whether the person by whom, or with whose authority or consent, a document or part purports to have been made, or is intended to be believed to have been made, be living or dead, or be a fictitious person; (f) every word, letter, figure, mark, seal, or thing expressed on or in a document, or forming part thereof, or attached thereto; and any coloring, shape, or device used therein, which purports to indicate the person by whom, or with whose authority or consent the document or part has been made, altered executed, delivered, attested, verified, certified, or issued, or which may affect the purport, operation, or validity of the document in any material particular, is a material part of the document; (g) "alteration" includes any cancelling, erase severance, interlineation, or transposition of or in a document or of or in any material part thereof, and the addition of any material part thereto, and any other act or device whereby the purport, operation, or validity of the document may be affected; and (h) all the provisions of this section apply to the forgery of a stamp or trade-mark in the same manner as to the forgery of a document. Illustrations (a) A. endorses his own name on a cheque, meaning it to pass as an endorsement by another person of the same name. Here A. is guilty of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	forgery. (b) A. is living under an assumed name. It is not forgery for him to execute a document in that name, unless he does so with the intent to defraud, etc. (c) A. with intent to defraud, makes a promissory note in the name of an imaginary person. Here A. is guilty of forgery. **Section 165—Being in Possession of means of Forging** Whoever without lawful excuse, the proof whereof shall lie on him, has in his possession any instrument or thing specially contrived or adapted for purposes of forgery shall be guilty of a misdemeanour. **Section 166—Possessing Forged Document etc.** Whoever, with any of the intents mentioned in this Chapter, has in his possession any document or stamp, which is forged, counterfeited, or falsified, or which he knows not to be genuine, shall be liable to the like punishment as if he had, with that intent forged, counterfeited, or falsified the document or stamp. **Section 167—Explanation as to Possession of doing any Act with Respect to Document, or Stamp** (1) A person possesses or does any act with respect to a document knowing it not to be genuine, if he possesses it, or does such act with respect to it, knowing that it was not in fact made or altered at the time, or by the person, or with the authority or consent of the person, at which or by whom or with whose authority or consent, it purports, or is pretended by him to have been made or altered; and in such case it is immaterial whether the act of the person who made or altered it was or was not a crime. (2) In like manner, a person possesses or does any act with respect to a stamp, knowing it not to be genuine, if he possesses in or does such act with respect to it, knowing it is in fact counterfeited or falsified; and in such case it is immaterial whether the act of the person who counterfeited or falsified it was or was not a crime. **Section 168—Definition of Counterfeiting**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	A person counterfeits a stamp or mark if he makes any imitation thereof, or anything which is intended to pass or which may pass as such a stamp, or mark; he shall be guilty of counterfeiting, within the meaning of this Chapter, although he does not intend that any person should be defrauded or injured by, or that any further use should be made of, the specimen or pattern. **Section 169—Uttering Forged Documents etc.** Whoever, with any of the intents mentioned in this Chapter, utters or in any manner deals with or uses, any such document, stamp as in this Chapter mentioned, knowing it to be forged, counterfeited, or falsified, or knowing it not to be genuine, shall be liable to the like punishment as if he had, with that intent, forged, counterfeited, or falsified the document, or stamp. **Section 170—Imitation of Forged Document, etc., need not be perfect** For the purposes of the provisions of this Code relating to the forgery, counterfeiting, falsifying, uttering, dealing with, using, or possessing of any document, stamp, or trade-mark, it is not necessary that the document, stamp, or trade-mark should be so complete, or should be intended to be made so complete, or should be capable of being made so complete, as to be valid or effectual for any of the purposes of a thing of the kind which it purports or is intended to be or to represent, or as to deceive a person of ordinary judgment and observation.
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.	**Electronic Transactions Act, 2008 (Act 772)** **S 123 General Provision for cyber offences** Except as provided for in this Act, any offence under a law which is committed in whole or in part by use of an electronic medium or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification to the person who commits the offence. **S 119 Obtaining Electronic Payment medium falsely** A person who makes or causes to be made either directly or indirectly a false representation to procure the issue of an electronic payment medium personally or to another person commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	of not more than ten years or to both. **S 122 General Offence for fraudulent electronic fund transfer** A person who without authority, in the course of an electronic fund transfer uses the personal or financial record or credit account numbers or electronic payment medium of another with intent to defraud an issuer or a creditor or who obtains money, goods, services or anything fraudulently commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 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	**Electronic Transactions Act, 2008 (Act 772)** **S.136 Child Pornography** (l) A person who intentionally does any of the following acts: (a) publishes child pornography through a computer: (b) produces or procures child pornography for the purpose of its publication through a computer system; or (c) possesses child pornography in a computer system or on a computer or electronic record storage medium commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or to both. (2) In this section: "child pornography" includes material that visually depicts (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; · (c) images representing a child engaged in sexually explicit conduct; and (d) unauthorized images of nude children; "child" means a person below eighteen years;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	"publish" means (a) distribute, transmit; disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; (b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); and (c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature to carry out an act referred to in paragraph (a).
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 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	**Section 42 of Copyright Act, 2005 (Act 690). Copyright and related rights offences** (1) A person who: (a) reproduces, duplicates, extracts, imitates or imports into the country, except for that person's private use, any work, (b) causes to be reproduced, duplicated, extracted, imitated or imported into the country except for the person's private use any work, (c) distributes or permits or causes to be distributed in the country by way of sale or otherwise any work, (d) exhibits or permits or causes to be exhibited in public any work, (e) removes or alters any electronic rights management information, (f) distributes, imports for distribution, broadcasts, communicates or makes available to the public, works, performances, copies of fixed performances or sound recordings knowing that electronic right management information has

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	been removed or altered without authority, or (g) manufactures, imports, distributes, exports, sells, rents, possesses for commercial purposes, offers to the public, advertises, communicates or otherwise provides any device, product or component that is designed or adapted to remove, alter or add electronic rights management information, or (h) circumvents any technological protection measure applied by the right holder to the protected work, or (i) manufactures, imports, distributes, exports, sells, rents, possesses for commercial purposes, offers to the public, advertises, communicates or otherwise provides without authority devices, components, services or other means, designed, adapted, or promoted to circumvent such a measure, or (j) rents or lends to the public any work where the Person performing the act knew or had reasonable grounds to know that the action induces, enables, facilitates or conceals an infringement of any copyright or related right protected under this Act without the licence or authorisation of the person whose rights are protected under this Act or the agent of that person whose rights are protected, infringes the protected rights and commits an offence punishable under section 43 of this Act. **Section 43 of Copyright Act, 2005 (Act 690)Penalty for copyright offence** A person who infringes a right protected under this Act commits an offence and is liable on summary conviction or to a fine of not more than one thousand penalty units and not less than five hundred penalty units or to a term of imprisonment of not more than three years or to both; and in the case of a continuing offence to a further fine of not less than twenty-five penalty units and not more than one hundred penalty units for each day during which the offence continues.
Title 5 – Ancillary liability and sanctions	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Electronic Transactions Act, 2008 (Act 772)** **Section 112 Aiding and abetting** Sections 20 and 21 of the Criminal Offences Act, 1960 (Act 29) on abetment of crime applies with the necessary modification to any person who abets a crime applies with the necessary modification to any person who abets a crime whether the medium used in whole or in part was an electronic medium or an electronic agent. **Section 111 Attempt to Commit Crimes** Section 18 of the Criminal Offences Act, 1960 (Act 19) on attempts to commit crimes with the necessary modifications to any person who attempts to commit a crime whether the medium used in whole or in part was an electronic medium or an electronic agent. **Criminal Offences Act, 1960 (Act 29)** (references made in the ETA on aiding and abetting and Attempt to Commit crimes) **Section 18—Provisions Relating to Attempts to Commit Crimes** (1) A person who attempts to commit a crime by any means shall not be acquitted on the ground that, by reason of the imperfection or other condition of the means, or by reason of the circumstances under which they are used, or by reason of any circumstances affecting the person against whom, or the thing in respect of which the crime is intended to be committed or by reason of the absence of that person or thing, the crime could not be committed to his intent. (2) Every person who attempts to commit a crime shall, be deemed guilty of an attempt, and shall, except as in this Code otherwise expressly provided, be punishable in the same manner as if the crime had been completed. (3) Where any act amounts to a complete crime, as defined by any provision of this Code, and is also an attempt to commit some other crime, a person who is guilty of it shall be shall be liable to be convicted and punished either under such provision or under this section. (4) Any provision of this Code with respect to intent, exemption, justification, or extenuation, or any other matter in the case of any act, shall apply with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	necessary modifications to the case of an attempt to do that act. **Section 20—Abetment of Crime and Trial and Punishment of Abettor** (1) Every person who, directly or indirectly, instigates, commands, counsels, procures, solicits, or in any manner purposely aids, facilitates, encourages, or promotes, whether by his act or presence or otherwise, and every person who does any act for the purpose of aiding, facilitating, encouraging or promoting the commission of a crime by any other person, whether known or unknown, certain or uncertain, is guilty of abetting that crime, and of abetting the other person in respect of that crime. (2) Every person who abets a crime shall, if the crime is actually committed in pursuance or during the continuance of the abetment, be deemed guilty of that crime. (3) Every person who abets a crime shall, if the crime is not actually committed, be punishable as follows, that is to say— (a) where the crime abetted was punishable by death the abettor shall be liable to imprisonment for life; and (b) in any other case the abettor shall be punishable in the same manner as if the crime had been actually committed in pursuance of the abetment. (4) An abettor may be tried before, with, or after a person abetted, and although the person abetted is dead or is otherwise not amenable to justice. (5) An abettor may be tried before, with, or after any other abettor, whether he and such other abettor abetted each other in respect of the crime or not, and whether they abetted the same or different parts of the crime. (6) An abettor shall have the benefit of any matter of exemption, justification, or extenuation to which he is entitled under this Code, notwithstanding that the person abetted or any other abettor is not entitled to the like benefit. (7) Every person who, within the jurisdiction of the Courts, abets the doing beyond the jurisdiction of an act which, if done within the jurisdiction, would be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a crime, shall be punishable as if he had abetted that crime. **Section 21—Cases where One Crime is Abetted and a Different Crime is Committed** (1) Where a person abets a particular crime, or abets a crime against or in respect of a particular person or thing and the person abetted actually commits a different crime, or commits the crime against or in respect of a different person or thing, or in a manner different from that which was intended by the abettor, the following provisions shall have effect— (a) if it appears that the crime actually committed was not a probable consequence of the endeavour to commit, nor was substantially the same as the crime which the abettor intended to abet, nor was within the scope of the abetment, the abettor shall be punishable for his abetment of the crime which he intended to abet in the manner provided by this Chapter with respect to the abetment of crimes which are not actually committed; and (b) in any other case, the abettor shall be deemed to have abetted the crime which was actually committed, and shall be liable to punishment accordingly. (2) If a person abets a riot or unlawful assembly with the knowledge that unlawful violence is intended or is likely to be used, he is guilty of abetting violence of any kind or degree which is committed by any other person in executing the purposes of the riot or assembly, although he did not expressly intend to abet violence of that kind or degree.
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; 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,	**Section 46 of the Interpretation Act, 2009, Act 792** "person" includes a body corporate, whether corporation aggregate or corporation sole and an unincorporated body of persons as well as an individual; **Companies Act 1963 (Act 179)** **Section 139 Acts of the Company** Any act of the members in general meeting, the board of directors, or a managing director while carrying on in the usual way the business of the company shall be treated as the act of the company itself; and accordingly, the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	company shall be criminally and civilly liable therefore to the same extent as if it were a natural person. Provided that, (a) The company shall not incur civil liability to any person if that person had actual knowledge at the time of the transaction in question that the general meeting, board of directors, or managing director, as the case may be, had no power to act in the matter or had acted in an irregular manner of if, having regard to his position with, or relationship to, the company, he ought to have known of the absence of power of of the irregularity; (b) If in fact a business is being carried on by the company, the company shall not escape liability for acts undertaken in connection therwith merely because the business in question was not among the business authorised by the company's regulations
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	
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	**Chapter 5 of the 1992 Constitution upholds Fundamental Human Rights and Freedoms**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 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 100 of Act 772** **Preservation of evidence** 100. (1) A provider of wire or electronic communication services or a remote computing service on the written request of a law enforcement agency, shall take the necessary steps to preserve records and other evidence in its possession pending the issue of a Court order and shall take steps to ensure that the request by the law enforcement agency is not disclosed to third parties during the period. (2) Where an order from the Court is not obtained and served for fourteen days after the receipt of the written request, the wire or electronic communication services, or remote computing service provider is not under any obligation to preserve the evidence. **Section 104 of Act 772** **Backup preservation** 104. (1) A Court may order that an electronic communication provider shall create a backup copy of the contents of the electronic communications sought to be preserved on application by a law enforcement agency and the electronic communication provider shall, without notifying the subscriber or customer of the order, create the backup copy and shall con-firm to the law enforcement agency that the backup copy has been made. (2) The law enforcement agency shall within three days after receipt of the confirmation of the creation of the backup, notify the sub-scriber or customer of the Court order and compliance by the provider.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) The provider shall not destroy the backup copy until the delivery of a copy of the backup information to the agency or the determination of the trial in respect of which the back-up application was sought. (4) Unless notice to vacate the Court order is obtained by the sub-scriber or customer and served upon the law enforcement agency and the provider, the provider shall release the backup copy to the requesting law enforcement agency fourteen days after receipt of the order for the creation of the backup copy.
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.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 99 of Act 772 Law enforcement officer and third party assistance** 99 (2) A law enforcement officer executing a warrant under this Act is entitled to require (a) the person by whom or on whose behalf, the police officer has reasonable grounds to suspect, to produce a computer which is or has been used, or (b) any person in charge of, or otherwise concerned with the operation of the computer, to provide the officer or any authorised person with the reasonable technical and other assistance required for investigation or prosecution.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	(3) A law enforcement officer executing a warrant under this Act is entitled to require a person in possession of decryption information to grant the law enforcement officer access to the decryption information necessary to decrypt an electronic record required to investigate an offence. **Section 102 of Act 772 Disclosure of electronic information** 102. (1) Except as provided in this Act, a provider of an electronic communication service or remote computing service shall not disclose a record or other information pertaining to a subscriber to a customer of an electronic communication service to any person without the consent of the subscriber or customer. (2) A provider of an electronic communication service or remote computing service shall disclose a record or other information related to a subscriber or customer to a law enforcement agency: (a) on receipt of a Court order for the disclosure, or (b) on receipt of the written consent of the subscriber or customer to the disclosure. **Law enforcement officer and third party assistance** ETA 99 (2) A law enforcement officer executing a warrant under this Act is entitled to require (a) the person by whom or on whose behalf, the police officer has reasonable grounds to suspect, to produce a computer which is or has been used, or (b) any person in charge of, or otherwise concerned with the operation of the computer, to provide the officer or any authorised person with the reasonable technical and other assistance required for investigation or prosecution. (3) A law enforcement officer executing a warrant under this Act is entitled to require a person in possession of decryption information to grant the law enforcement officer access to the decryption information necessary to decrypt an electronic record required to investigate an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ETA 99 appears to enable production of computers, but not production of computer data and thus may not enable ordering production of computer data stored in a storage medium
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. 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.	**Section 98 and 99 of Act 772** **Search and Seizure** **Powers of law enforcement officers** 98. (1) This provision is in addition to the powers of arrest, search and seizure of a law enforcement agency provided by law. (2) A law enforcement agent may seize any computer, electronic record, program, information, document, or thing in executing a warrant under this Act if the law enforcement officer has reasonable grounds to believe that an offence under this Act has been or is about to be committed. **Law enforcement officer and third party assistance** ETA 99 (1) A law enforcement officer executing a warrant may be accom-panied by an authorised person and is entitled, with the assistance of that person, to (a) have access to and inspect and check the operation of any computer to which this section applies; (b) use or cause the computer to be used to search any programme or electronic record held in or available to the computer; (c) have access to information, any code or technology which has the capability of retransforming or unscrambling an en-crypted programme or electronic record held in or available to the computer into readable and comprehensible format or text to investigate an offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under sections 98 to 106; and (d) make and take away a copy of any programme or electronic record held in the computer as specified in the search warrant and any other programme or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	electronic record held in that or any other computer which the law enforcement officer has reasonable grounds to believe is evidence of the commission of another offence. (2) A law enforcement officer executing a warrant under this Act is entitled to requir (a) the person by whom or on whose behalf, the police officer has reasonable grounds to suspect, to produce a computer which is or has been used, or (b) any person in charge of, or otherwise concerned with the operation of the computer, to provide the officer or any authorised person with the reasonable technical and other assistance required for investigation or prosecution. (3) A law enforcement officer executing a warrant under this Act is entitled to require a person in possession of decryption information to grant the law enforcement officer access to the decryption information necessary to decrypt an electronic record required to investigate an offence.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**Economic and Organised Crime Office Act** Power to search for tainted property 25. (5) The Court shall consider an application without notice which claims that communication in any medium including an article sent by post or through a courier service is likely to contain information or a substance that may be relevant to an investigation into an offence under a law in this Country or a corresponding foreign law, and the Court shall, where appropriate, order an authorised officer of the Office to (a) intercept, detain and open the article in the course of transmission by postal or courier service, (b) intercept a message transmitted or received by any means of communication, (c) intercept or listen to any conversation by any means of communication, or (d) enter premises and install on the premises a device for the interception and retention of communications of specified description and remove and retain the device. **Section 101 of Act 772 Interception of Content Data** **Contents of electronic communications in electronic storage** ETA 101 (1) A Court may order the disclosure of the contents of an electronic

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	communication that is in transit, held, maintained or has been in electronic storage in an electronic communications system by an electronic communication service provider. (2) The Court shall not make an order unless it is satisfied that the disclosure is relevant and necessary for investigative purposes or is in the interest of national security. ETA 101 primarily relates to disclosure of content data if so ordered by Court, but does not specifically empower authorities to either record or collect through technical means specified communications in real-time (or to compel service providers to do the same)
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. 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,	**Section 142 of Act 772** **Territorial scope of offences under this Act** 142. (1) This Act has effect in relation to a person of whatever nationality outside as well as within the country and where an offence under this Act is committed by a person in any place outside the country, the person may be dealt with as if the offence had been committed within the country. (2) This Act shall apply if, for the offence in question (a) the accused was in the country at the material time; (b) the electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time; (c) the electronic payment medium was issued by a financial institution in the country; or (d) the offence occurred within the country, on board a Ghana-ian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph (a), (b) or (c) applies. **Section 56 of the Courts Act, 1993 (Act 459)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Criminal Jurisdiction of Courts of Ghana** (1) Subject to this section, the jurisdiction of the courts of Ghana in criminal matters is exercisable only in respect of an offence committed within the territory of Ghana including its territorial waters and air space and in respect of offences committed on any ship or aircraft registered or licensed in Ghana. (2) When an act which if done within the jurisdiction of a court, would be a criminal offence, is done partly within and partly outside the jurisdiction, every person who within or outside the jurisdiction does or abets any part of the act may be tried and punished as if the act had been done wholly within the jurisdiction. (3) A citizen of Ghana who— (a) while employed in the service of the Republic of Ghana or of any statutory corporation does an act outside Ghana which if done in Ghana is punishable as an offence; or (b) does an act outside Ghana which if done in Ghana would constitute the offence of murder or an offence under section 183A of the Criminal Code, 1960 (Act 29); or (c) does outside Ghana any act which if done in Ghana constitutes an offence involving or resulting in the misappropriation, dissipation or loss of— (i) public funds; (ii) government property including damage to government property; (iii) property belonging to a statutory corporation including damage to the property of the statutory corporation; (d) does any act on the premises of a Ghanaian diplomatic mission which if done in Ghana would be punishable as an offence, commits an offence as if the offence was done in Ghana and may, subject to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	section 46 of the Criminal Procedure Code, 1960 (Act 30) be prosecuted and punished in Ghana. (4) Any person (whether a citizen of Ghana or not) is liable to be tried and punished in Ghana for the respective offence if he does an act which if done within the jurisdiction of the courts of Ghana would have constituted any of the following offences— (a) slave trade or traffic in slaves; (b) piracy; (c) traffic in women or children; (d) falsification or counterfeiting or uttering of false copies or counterfeits of any official seal of Ghana or any currency, instrument of credit, stamp, passport or public document issued by the Republic or under its authority; (e) genocide; (f) any offence against the property of the Republic; (g) any offence against the security, territorial integrity or political independence of the Republic; (h) hijacking; (i) unlawful traffic in narcotics; (j) attacks on any international communications system, canal or submarine cable; (k) unauthorised disclosure of an official secret of the Republic; (l) an offence by or against a person in the employment of the Republic or a statutory corporation while acting in the course of the duties of such

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	employment; (m) traffic in obscene publications; and (n) any other offence which is authorised or required by a convention or treaty to which the Republic is a signatory to be prosecuted and punished in Ghana wherever the offence was committed.
Chapter III – International co-operation	
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 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.	**Section 1, Extradition Act, 1960 (Act 22)** **As Amended By Extradition Act, 1960 (Amendment) Decree, 1966 (NLCD 65)1** (1) Where an arrangement has been made with any country with respect to the surrender to that country of any fugitive criminals, the President by legislative instrument may order that this Act shall apply in the case of that country, subject to such conditions, exceptions, and qualifications as may be specified in the order, and this Part shall apply accordingly. (2) An order under subsection (1) shall recite or embody the terms of the arrangement, and shall not remain in force for any longer period than the arrangement. (3) Every order under this section shall be laid before the National Assembly.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**Section 17 of the Mutual Legal Assistance Act, 2010 (Act 807)** **Dual criminality** 17. (1) Despite section 1 (3), where a request by the Central Authority of a foreign State or the competent authority of a foreign entity for mutual legal assistance is in respect of a criminal matter which does not constitute a criminal offence in the Republic, the Minister shall (a) consider details of the relevant conduct underlying the re-quest and the adoption of measures that may be necessary to facilitate the provision of the assistance required, and (b) provide the required assistance (i) in accordance with the laws of the Republic, and (ii) on terms and conditions certified by the Minister.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 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.	**Section 52 of the Mutual Legal Assistance Act, 2010 (Act 807)** **Special co-operation** 52. (1) The Minister may disclose information in the possession of a competent authority in Ghana to the Central Authority of a foreign State or the competent authority of a foreign entity if the disclosure (a) is likely to assist in carrying out any investigation, prosecu-tion or judicial proceedings in the foreign State or by the foreign entity, (b) may lead to a request by the Central Authority of that foreign State or the competent authority of that foreign entity, or (c) may lead to the tracing, freezing and confiscation of the proceeds of crime. (2) Where the information is disclosed, the Minister may impose conditions on the use of the information. (3) The person who receives the information for use shall comply with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	conditions imposed. (4) Without limiting subsection (1), the Central Authority may disclose information on proceeds of crime without prior request.
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 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.	**Section 4 of the Mutual Legal Assistance Act, 2010 (Act 807)** **Section 4 of Act 807** **Administrative arrangements** 4. (1) Where there is no agreement between the Republic and a foreign State or foreign entity, the Minister may enter into an administrative arrangement with the foreign State or foreign entity for mutua1legal assistance in respect of an act specified in the arrangement if that act when committed in Ghana would be a serious offence. (2) Where an agreement expressly states that mutual legal assistance may be provided with respect to an act that does not constitute an offence within the meaning of the agreement, the Minister may enter into an administrative arrangement with the foreign State or foreign entity concerned, for mutual legal assistance with respect to the act specified in the arrangement if that act when committed in Ghana would be a serious offence. (3) An administrative arrangement entered into under subsection (1) or (2) may be implemented by the Minister under this Act, in the same manner as an agreement. (4) An administrative arrangement under subsection (1) or (2) shall have effect as specified in the arrangement or for a period not exceeding six months. (5) Sections 1 and 2 do not apply to an administrative arrangement entered into under subsection (1) or (2) of this section.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Section 11 of Act 807** **Confidentiality of requests** 11. (1) The Central Authority and competent authorities of the Re-public that deal with a request under this Act, shall keep that request, its contents and any information and material supplied in compliance with the request confidential. (2) Despite subsection (1), where the Central Authority of a foreign State or where the competent authority of a foreign entity requires or per-mits the disclosure of the content of a request or information or material supplied in relation to that request, the Minister and Central Authority of that State or competent authority of that foreign entity may after consulta-tion, determine the terms and conditions of the disclosure. **Limitation on use of information or evidence** 12. (1) The Central Authority of a foreign State or competent authority of a foreign entity shall use information or evidence obtained in re-sponse to a request for assistance under this Act, only for the purpose of the criminal matter specified in the request. (2) Despite subsection (1), where the Central Authority of a foreign State or competent authority of a foreign entity requires to use information or evidence for a purpose, other than that specified in the request, that State or entity shall in writing seek the prior written consent of the Minister.
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; 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	**Section 51 of Act 807** **Request for the preservation of communications data** (1) A request by the Central Authority of a foreign State or the competent authority of a foreign entity for assistance for the expeditious preservation of communications data pending the submission of a request for the production of data shall: (a) specify the identity of the agency or authority making the request, (b) contain a brief description of the conduct under investigation,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	(e) contain a description of the data to be preserved and its connection with the investigation or proceedings to which the request relates and which indicates whether the communications data to be preserved includes (i) subscriber information, (ii) traffic data, or (iii) any other information that composes communication data, (d) contain information to identify the custodian of the stored communications data or the location of the computer system, (e) indicate reasons for the necessity of the preservation, and (f) indicate the manner and time within which the foreign State intends to submit a substantive request for assistance for the production of the required communication data. (2) A request for assistance to preserve communications data may be directly transmitted to the competent authority designated by the Minister to do so. (3) A competent authority that receives a request shall notify the Minister. (4) Where the Central Authority receives the request by the Central Authority of a foreign State or the competent authority of a foreign .entity for the preservation of communications data or is notified under subsection (3), the Central Authority shall direct that the communications data be preserved for a period of one hundred and twenty days pending submission of a substantive request by the Central Authority of the foreign State or the competent authority of the foreign entity for assistance to obtain the preserved communications data. (5) The communications data shall be preserved (a) pending the determination of the request, or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) until the data is obtained if the request is granted. (6) Where the Central Authority is of the opinion that the preservation of communications data pursuant to a request (a) does not warrant the future availability of the required communications data; or (b) may threaten the confidentiality of or adversely affect the investigation in the foreign State, or by the foreign entity the Central Authority shall promptly inform the Central Authority of the foreign State or the competent authority of the foreign entity where applicable which shall determine whether to execute the request or not.
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.	
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:	**Mutual Legal Assistance Act, 2010 (Act 807)** **Section 20 of Act 807 Request for search and seizure** 20. (1) Where a request is made by the Central Authority of a foreign State or the competent authority of a foreign entity for assistance to search for and to seize property in Ghana, the Central Authority of that State or competent authority of that entity shall so far as practicable specify (a) the property to be searched for and seized, and

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.	(b) information required to obtain the requisite warrant and facilitate the execution of the request. (2) Where the Minister approves the request, the Minister shall authorise a police officer or any other person in writing to apply ex parte to the court for the relevant warrant. (3) Without limiting the provisions of section 10 (6), the Central Authority shall certify and forward to the Central Authority of the foreign State or the competent authority of the foreign entity a report that contains information on the (a) outcome of the search, (b) place and circumstances of the seizure, and (c) subsequent custody, detailed description and state of the property seized. **Section 21 of Act 807** **Issue of search warrant** 21. (1) Where a court receives an application for a search and seizure and is satisfied by evidence on oath that there are reasonable grounds to believe that (a) a serious offence over which the respective foreign State or foreign entity has jurisdiction has been or may have been committed, and (b) evidence of the commission of the offence, may be found in a building, receptacle, vessel or place in the country the court may issue a search warrant authorising the police officer or the person named in the warrant to execute it. (2) The court that issues the warrant may subject the execution of the warrant to conditions including the time or manner of its execution. (3) For the purpose of subsection (1) (a), a statement contained in the request of the Central Authority of the foreign State or the competent authority of the foreign entity to the effect that a serious offence over which the foreign State or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	foreign entity has jurisdiction has been or may have been committed is prima facie evidence of that fact. (4) The court that issues a warrant shall determine a time and place for a hearing to consider the report of the police officer or an authorised person who executed the warrant and the circumstances of its execution. **Section 22 of Act 807** **Content of search warrant** 22. (1) A search warrant issued under section 21 (1) shall be in the form prescribed under the Criminal and other Offences (Procedure) Act 1960, (Act 30) and may be varied to suit the purpose of each case. (2) A search warrant issued under section 21 (1) shall (a) specify the time and place for the hearing required under section 21 (4), (b) state that, at the hearing to consider its execution, an order shall be sought to send to the Central Authority of the foreign State or the competent authority of the foreign entity, records, computer data or items seized in execution of the warrant, and (c) state that (i) each person from whom a record, item or computer data is seized in execution of the warrant, and (ii) a person who claims to have an interest in a record, item or computer data seized in execution of the warrant has the right to make representations at the hearing before an order is made concerning the record, item or computer data. **Section 25 of Act 807** **Hearing on execution of warrant**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	25. (1) The court that issued the warrant under section 21 (1) or a court designated by the Chief Justice, shall regulate the procedure for the hearing in respect of the execution of the warrant. (2) Where the court is not satisfied (a) that the warrant was executed in accordance with its terms and conditions, or (b) that an order should be made for a record, item or computer data seized in execution of the warrant to be sent to the Cen-tral Authority of the foreign State or the competent authority of the foreign entity which requested the search and seizure, the court may order that the record, item or computer data seized in execution of the warrant be returned. (3) The return of an item seized as a result of the execution of a search warrant shall be made to (a) the person from whom it was seized, if possession of it by that person is lawful; or (b) the lawful owner or the person who is lawfully entitled to its possession, if the owner or that person is known and posses-sion of the item by the person from whom it was seized was unlawful. (4) Where the court orders that an item seized in execution of the warrant be sent to the Central Authority of the foreign State or the competent authority of the foreign entity which requested for the search and seizure, the court may include in the order terms and conditions that the court considers necessary, including terms and conditions (a) necessary to give effect to the request, (b) with respect to the preservation and return to Ghana of the item, and

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.	**Section 45 of Act 807** **Request for interception of telecommunications in Ghana by service provider** 45. (1) Where the request for interception involves the interception of telecommunication services that are operated through a gateway in this country, the Minister shall after consultation with the Ministers responsible for the Interior and Communication ensure that the systems of telecom-munications are made directly accessible for the lawful interception by the foreign State concerned through the intermediary of a communications service provider in this country designated by the Minister responsible for Communications. (2) A foreign State shall be entitled for the purpose of criminal investigation and in accordance with the laws of the Republic to carry out the interception through the designated service provider if the subject of the interception is present in this country without involving any other foreign State on whose territory the gateway is located. (3) The Minister responsible for Communications shall designate a communications service provider by publication in the Gazette.
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	**Mutual Legal Assistance Act, 2010 (Act 807)** **Request for interception of telecommunications in Ghana**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
their applicable treaties and domestic laws.	43. (1) A request by the Central Authority of a foreign State or the competent authority of a foreign entity for assistance to intercept telecom-munications in this country may comprise assistance to (a) intercept and immediately transmit to the Central Authority of the foreign State or the competent authority of the foreign entity the content of the communication, or (b) intercept, record and subsequently transmit to the Central Authority of the foreign State or the competent authority of the foreign entity the content of the communication. (2) Without limiting subsection (1) a request may be made for the interception of telecommunications by the subject if the subject is present in (a) a foreign State and that foreign State needs the technical as-sistance of the Republic to intercept the tele-communications; (b) a foreign State and its telecommunications are capable of being intercepted in that State; or (c) a foreign State other than the foreign State which requested for assistance and has been informed of the required techni-cal assistance of the Republic to intercept communications to assist the foreign State or foreign entity that initially requested for assistance. (3) For the purposes of this section, the interception of telecom-munications may be effected electronically or through any other technology approved by the Minister after consultation with the Ministers responsible for the Interior and Communications. **Order for interception of telecommunications** 46. (1) Where the Minister approves a request by the Central Authority of a foreign State or the competent authority of a foreign entity to intercept telecommunications in Ghana regarding an offence, the Minister shall ex-peditiously authorise a police officer to apply to the relevant court without notice to the person whose telecommunication is to be intercepted for an order

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	to intercept telecommunications. (2) Despite subsection (1), a police officer may, with the prior written consent of the Minister, apply to the relevant court for the order without notice, to the person whose telecommunication is to be intercepted in furtherance of obtaining evidence of the commission of an offence under this Act. (3) The court to which an application is made under subsection (1) or (2) may make an order for the prevention of crime on reasonable grounds to (a) require a telecommunications service provider to intercept and retain a specified communication or communication of a specified description received or transmitted by that telecom-munications service provider, (b) authorise a police officer to intercept or listen to conversation provided by a telecommunications service provider, (c) authorise a police officer to enter premises and to install on the premises a device for the interception and retention of specified telecommunications or telecommunications of a specified description and to remove and retain the device, or (d) authorise a competent authority to facilitate access to the systems of telecommunication services required to be inter- cepted to execute the request where there is suspicion of the commission of an offence or the whereabouts of a person suspected by the police officer to have committed an offence is contained in that telecommunication or telecommunica-tions of that description. **Request for the interception of communications to provide stored communications** 48. (1) Where the request by the Central Authority of a foreign State for the interception of telecommunications is for the purpose of the pro-vision of stored communications, the request shall be accompanied with (a) the name of the authority with access to the relevant com-munication, (b) the location at which the communication is held,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) the intended purpose for the required communication, (d) sufficient information to identify the communications, (e) details of the data of the relevant interception, (f) the recipient of the communication, (g) the intended duration for the use of the communication, and (h) the terms for the use and disclosure of the communication to third parties. (2) Where the Minister approves a request for the interception of telecommunications for the provision to a foreign State or foreign entity of stored communications, the Minister shall apply without notice to the relevant court for an order to intercept the telecommunications in Ghana. (3) Section 46 (3) shall apply with the necessary modification for the purpose of an order to provide stored communications.
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; 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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