Kenya

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 28 May 2020

Table of contents

[reference to the provisions of the Budapest Convention]

Chapter I – Use of terms

Article 1 – "Computer system", "computer data", "service provider", "traffic data"

Chapter II – Measures to be taken at the national level

Article 2 – Illegal access
Article 3 – Illegal interception
Article 4 – Data interference
Article 5 – System interference
Article 6 – Misuse of devices
Article 7 – Computer-related forgery
Article 8 – Computer-related fraud
Article 9 – Offences related to child pornography
Article 10 – Offences related to infringements of copyright and related rights
Article 11 – Attempt and aiding or abetting
Article 12 – Corporate liability
Article 13 – Sanctions and measures

Section 2 – Procedural law
Article 14 – Scope of procedural provisions
Article 15 – Conditions and safeguards
Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data
Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

Section 3 – Jurisdiction
Article 22 – Jurisdiction

Chapter III – International co-operation

Article 24 – Extradition
Article 25 – General principles relating to mutual assistance
Article 26 – Spontaneous information
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
Article 28 – Confidentiality and limitation on use
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 – Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance in the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network

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:	-

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	**THE COMPUTER MISUSE AND CYBERCRIMES ACT No. 5 of 2018 (CMCA)** **PART I** **Article 2. Interpretation** "In this Act, unless the context otherwise requires — (…) 'computer system' means a physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system; (…) '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; (…) 'service provider' means — (a) a public or private entity that provides to users of its services the means to communicate by use of a computer system; and (b) any other entity that processes or stores computer data on behalf of that entity or its users; (…) 'traffic data' means computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or the type of underlying 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.	**CMCA, Part III** **Article 14. Unauthorised access** (1) A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both. (2) Access by a person to a computer system is unauthorised if— (a) that person is not entitled to control access of the kind in question to the program or data; or (b) that person does not have consent from any person who is entitled to access the computer system through any function to the program or data. (3) For the purposes of this section, it is immaterial that the unauthorised access is not directed at— (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer system. **Article 15. Access with intent to commit further offence** (1) A person who commits an offence under section 14 with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person, commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) For the purposes of subsection (1), it is immaterial that the further offence to which this section applies is committed at the same time when the access is secured or at any other time.
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.	**CMCA, PART I** **Article 2. Interpretation** (…) "'interception' means the monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system over a telecommunications system, and includes, in relation to a function of a computer system, listening to or recording a function of a computer system or acquiring the substance, its meaning or purport of such function." **CMCA, PART III** **Article 17. Unauthorized interception** (1) A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both. (2) A person who commits an offence under subsection (1) which — (a) results in a significant financial loss; (b) threatens national security; (c) causes physical or psychological injury or death to any person; or (d) threatens public health or public safety, is liable, on conviction to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both. (3) For the purposes of this section, it is immaterial that the unauthorized interception is not directed at — (a) a telecommunication system; (b) any particular computer system data; (c) a program or data of any kind; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) a program or data held in any particular computer system. (4) For the purposes of this section, it is immaterial whether an unauthorized interception or any intended effect of it is permanent or temporary.
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.	**CMCA, PART I** **Article 2. Interpretation** "interference" means any impairment to the confidentiality, integrity or availability of a computer system, or any program or data on a computer system, or any act in relation to the computer system which impairs the operation of the computer system, program or data; **PART III** **Article 16. Unauthorised interference**
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	(1) A person who intentionally and without authorisation does any act which causes an unauthorised interference, to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both. (2) For the purposes of this section, an interference is unauthorised, if the person whose act causes the interference — (a) is not entitled to cause that interference; (b) does not have consent to interfere from a person who is so entitled. (3) A person who commits an offence under subsection (1) which— (a) results in a significant financial loss to any person; (b) threatens national security; (c) causes physical injury or death to any person; or (d) threatens public health or public safety, is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both. (4) For the purposes of this section, it is immaterial whether or not the unauthorised interference is directed at — (a) any particular computer system, program or data; (b) a program or data of any kind; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) a program or data held in any particular computer system. (5) For the purposes of this section, it is immaterial whether an unauthorized modification or any intended effect of it is permanent or temporary.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise 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.	**CMCA, PART III** **Article 18. Illegal devices and access codes** (1) A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both. (2) A person who knowingly receives, or is in possession of, a program or a computer password, device, access code, or similar data from any action specified under subsection (1) and intends that it be used to commit or assist in commission of an offence under this Part commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both. (3) Despite subsections (1) and (2), the activities described under the subsections do not constitute an offence if — (a) any act intended for the authorised training, testing or protection of a computer system; or (b) the use of a program or a computer password, access code, or similar data is undertaken in compliance of and in accordance with the terms of a judicial order issued or in exercise of any power under this Act or any law. (4) For the purposes of subsections (1) and (2), possession of any program or a computer password, access code, or similar data includes having — (a) possession of a computer system which contains the program or a computer password, access code, or similar data; (b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or (c) control of a program or a computer password, access code, or similar data that is in the possession of another person.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**CMCA, PART III** **Article 25. Computer forgery** (1) A person who intentionally inputs, alters, deletes, or suppresses 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 of whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both. (2) A person who commits an offence under subsection (1), dishonestly or with similar intent — (a) for wrongful gain; (b) for wrongful loss to another person; or (c) for any economic benefit for oneself or for another person, is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CMCA, PART III** **Article 26. Computer fraud** (1) A person who, with fraudulent or dishonest intent— (a) unlawfully gains; (b) occasions unlawful loss to another person; or (c) obtains an economic benefit for oneself or for another person, through any of the means described in subsection (2), commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both. (2) For purposes of subsection (1) the word "means" refers to — (a) an unauthorised access to a computer system, program or data; (b) any input, alteration, modification, deletion, suppression or generation of any program or data;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) any interference, hindrance, impairment or obstruction with the functioning of a computer system; (d) copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; or (e) uses any data or program, or has any data or program output from the computer system in which it is held, by having it displayed in any manner.
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 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.	**CMCA, PART III** **Article 24. Child pornography** (1) A person who, intentionally — (a) publishes child pornography through a computer system; (b) produces child pornography for the purpose of its publication through a computer system; (c) downloads, distributes, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, offers in another way, or make available in any way from a telecommunications apparatus pornography; or (d) possesses child pornography in a computer system or on a computer data storage medium, commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty five years, or both. (2) It is a defence to a charge of an offence under subsection (1) that a publication which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, art, representation or figure is in the interest of science, literature, learning or other objects of general concerns. (3) For purposes of this section — "child" means a person under the age of eighteen years;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	"child pornography" includes data which, whether visual or audio, depicts — (a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c) realistic images representing a child engaged in sexually explicit conduct; "publish" includes to — (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) having in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or (c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature for the purpose of doing 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	*Copyright Act, 2001 applies.*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**CMCA, PART III** **Article 42. Aiding or abetting in the commission of an offence** (1) A person who knowingly and willfully aids or abets the commission of any offence under this Act commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both. (2) A person who knowingly and willfully attempts to commit an offence or does any act preparatory to or in furtherance of the commission of any offence under this Act, commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.
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, each Party shall take the measures necessary to ensure that a legal person	**CMCA, PART III** **Article 43. Offences by a body corporate and limitation of liability** (1) Where any offence under this Act has been committed by a body corporate— (a) the body corporate is liable, on conviction, to a fine not exceeding fifty million shillings; and (b) every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity, is also deemed to have committed the offence, unless they prove the offence was committed without their consent or knowledge and

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their functions and to prevailing circumstances, and is liable, on conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both. (2) If the affairs of the body corporate are managed by its members, subsection (1)(b) applies in relation to the acts or defaults of a member in connection with their management functions, as if the member was a principal officer of the body corporate or was acting in a similar capacity.
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.	*Sanctions and measures provided for in the body of the Act.*
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such	**CMCA, PART IV** **Article 47. Scope of procedural provisions** (1) All powers and procedures under this Act are applicable to and may be exercised with respect to any — (a) criminal offences provided under this Act; (b) other criminal offences committed by means of a computer system established under any other law; and (c) the collection of evidence in electronic form of a criminal offence under this Act or any other law. (2) In any proceedings related to any offence, under any law of Kenya, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	(3) The powers and procedures provided under this Part are without prejudice to the powers granted under — (a) the National Intelligence Service Act, 2012 (No. 28 of 2012); (b) the National Police Service Act, 2011 (No. 30 of 2011); (c) the Kenya Defence Forces Act, 2012 (No. 25 of 2012); and (d) any other relevant law.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	*The existence of adequate conditions and safeguards is analyzed in each procedural provision under respective domestic laws below.*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	*N/A*
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.	**CMCA, PART IV** **Article 51. Expedited preservation and partial disclosure of traffic data** (1) Where a police officer or an authorised person has reasonable grounds to believe that — (a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible, the police officer or an authorized person shall serve a notice on the person who is in possession or control of the computer system, requiring the person to —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or (ii) disclose sufficient traffic data concerning any communication in order to identify the service providers and the path through which communication was transmitted. (2) The data specified in the notice shall be preserved and its integrity shall be maintained for a period not exceeding thirty days. (3) The period of preservation and maintenance of integrity may be extended for a period exceeding thirty days if, on an application by the police officer or authorized person, the court is satisfied that — (a) an extension of preservation is reasonably required for the purposes of an investigation or prosecution; (b) there is a risk or vulnerability that the traffic data may be modified, lost, destroyed or rendered inaccessible; and (c) the cost of the preservation is not overly burdensome on the person in control of the computer system. (4) The person in possession or control of the computer system shall be responsible to preserve the data specified — (a) for the period of notice for preservation and maintenance of integrity or for any extension thereof permitted by the court; and (b) for the period of the preservation to keep confidential any preservation ordered under this section. (5) Where the person in possession or control of the computer system is a service provider, the service provider shall be required to — (a) respond expeditiously to a request for assistance, whether to facilitate requests for police assistance, or mutual assistance requests; and (b) disclose as soon as practicable, a sufficient amount of the non-content data to enable a police officer or an authorised person to identify any other telecommunications providers involved in the transmission of the communication. (6) The powers of the police officer or an authorised person under subsection (1) shall apply whether there is one or more service providers involved in the transmission of communication which is subject to exercise of powers under this section.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**CMCA, PART IV** **Article 50. Production order** (1) Where a police officer or an authorised person has reasonable grounds to believe that — (a) specified data stored in a computer system or a computer data storage medium is in the possession or control of a person in its territory; and (b) specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation, the police officer or the authorised person may apply to court for an order. (2) The Court shall issue an order directing — (a) a specified person to submit specified computer data that is in that person's possession or control, and is stored in a computer system or a computer data storage medium; or (b) a specified service provider offering its services in Kenya to submit subscriber information relating to such services in that service provider's possession or control.
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	**CMCA, PART IV** **Art. 48 – Search and seizure of stored computer data** (1) Where a police officer or an authorised person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data, that— (a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or (b) has been acquired by a person as a result of the commission of an offence, the police officer or the authorised person may apply to the court for issue

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	of a warrant to enter any premises to access, search and similarly seize such data. (2) A search warrant issued under subsection (1) shall — (a) identify the police officer or authorised person; (b) direct the police officer or authorised person under paragraph (a) to seize the data in question; or (c) direct the police officer or authorised person to– (i) search any person identified in the warrant; (ii) enter and search any premises identified in the warrant; or (iii) search any person found on or at such premises. (3) A search warrant may be issued on any day and shall be of force until it is executed or is cancelled by the issuing court. (4) A police officer or an authorised person shall present a copy of the warrant to a person against whom it is issued. (5) A person who — (a) obstructs the lawful exercise of the powers under this section; (b) compromises the integrity or confidentiality of a computer system, data, or information accessed or retained under this section; or (c) misuses the powers granted under this section, commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both.
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.	**CMCA, PART IV** **Article 52. Real-time collection of traffic data** (1) Where a police officer or an authorised person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a specific criminal investigation, the police officer or authorised person may apply to the court for an order to — (a) permit the police officer or authorised person to collect or record through the application of technical means traffic data, in real-time; (b) compel a service provider, within its existing technical capability —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(i) to collect or record through application of technical means traffic data in real time; or (ii) to cooperate and assist a police officer or an authorized person in the collection or recording of traffic data, in real-time, associated with specified communications in its jurisdiction transmitted by means of a computer system. (2) In making an application under subsection (1), the police officer or an authorised person shall — (a) state the grounds they believe the traffic data sought is available with the person in control of the computer system; (b) identify and explain, the type of traffic data suspected to be found on such computer system; (c) identify and explain the subscribers, users or unique identifier the subject of an investigation or prosecution suspected as may be found on such computer system; (d) identify and explain the offences identified in respect of which the warrant is sought; and (e) explain the measures to be taken to prepare and ensure that the traffic data shall be sought — (i) while maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of data to any party not part of the investigation. (3) Where the court is satisfied with the explanations provided under subsection (2), the court shall issue the order provided for under subsection (1). (4) For purposes of subsection (1), real-time collection or recording of traffic data shall be ordered for a period not exceeding six months. (5) The court may authorize an extension of time under subsection (4), if it is satisfied that— (a) such extension of real-time collection or recording of traffic data is reasonably required for the purposes of an investigation or prosecution; (b) the extent of real-time collection or recording of traffic data is commensurate, proportionate and necessary for the purposes of investigation or prosecution; (c) despite prior authorisation for real-time collection or recording of traffic data, additional real-time collection or recording of traffic data is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	necessary and needed to achieve the purpose for which the warrant is to be issued; (d) measures taken to prepare and ensure that the real time collection or recording of traffic data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; (e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of traffic data is permitted; and (f) the cost of such preservation is not overly burdensome upon the person in control of the computer system. (6) A court may, in addition to the requirement specified under subsection (3) require the service provider to keep confidential the order and execution of any power provided under this section. (7) A service provider who fails to comply with an order under this section commits an offence and is liable on conviction — (a) where the service provider is a corporation, to a fine not exceeding ten million shillings; or (b) in case of a principal officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
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	**CMCA, PART IV** **Article 53. Interception of content data** (1) Where a police officer or an authorised person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for the purposes of a specific investigation in respect of an offence, the police officer or authorised person may apply to the court for an order to— (a) permit the police officer or authorised person to collect or record through the application of technical means; (b) compel a service provider, within its existing technical capability — (i) to collect or record through the application of technical means; or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system. (2) In making an application under subsection (1), the police officer or an authorised person shall — (a) state the reasons he believes the content data being sought is in possession of the person in control of the computer system; (b) identify and state the type of content data suspected to be found on such computer system; (c) identify and state the offence in respect of which the warrant is sought; (d) state if they have authority to seek real-time collection or recording on more than one occasion is needed, and shall specify the additional number of disclosures needed to achieve the purpose for which the warrant is to be issued; (e) explain measures to be taken to prepare and ensure that the real-time collection or recording is carried out— (i) while maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of information and data of any party not part of the investigation; (f) state how the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) state the manner in which they shall achieve the objective of the warrant, real time collection or recording by the person in control of the computer system where necessary. (3) Where the court is satisfied with the grounds provided under subsection (2), the court shall issue the order applied for under subsection (1). (4) For purposes of subsection (1), the real-time collection or recording of content data shall not be ordered for a period that exceeds the period that is necessary for the collection thereof and in any event not for more than a period of nine months. (5) The period of real-time collection or recording of content data may be extended for such period as the court may consider necessary where the court is satisfied that — (a) such extension of real-time collection or recording of content data is required for the purposes of an investigation or prosecution;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) the extent of real-time collection or recording of content data is proportionate and necessary for the purposes of investigation or prosecution; (c) despite prior authorisation for real-time collection or recording of content data, further real-time collection or recording of content data is necessary to achieve the purpose for which the warrant is to be issued; (d) measures shall be taken to prepare and ensure that the real-time collection or recording of content data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; (e) the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of content data is permitted; and (f) the cost of such real-time recording and collection is not overly burdensome upon the person in control of the computer system. (6) The court may also require the service provider to keep confidential the order and execution of any power provided for under this section. (7) A service provider who fails to comply with an order under this section commits an offence and is liable, on conviction — (a) where the service provider is a corporation, to a fine not exceeding ten million shillings; (b) in case of an officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	*N/A*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
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	*Cybercrime offences are not currently included among the extradition crimes listed in the Extradition (Contiguous and Foreign Countries) Act, 1968.*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	**CMCA, PART V** **Article 57. General principles relating to international cooperation** (1) This Part shall apply in addition to the Mutual Legal Assistance Act, 2011 and the Extradition (Contiguous and Foreign Countries) Act. (2) The Central Authority may make a request for mutual legal assistance in any criminal matter to a requested State for purposes of—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or data; (b) collecting evidence of an offence in electronic form; or (c) obtaining expeditious preservation and disclosure of traffic data, real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act. (3) A requesting State may make a request for mutual legal assistance to the Central Authority in any criminal matter, for the purposes provided in subsection (2). (4) Where a request has been received under subsection (3), the Central Authority may, subject to the provisions of the Mutual Legal Assistance Act, 2011, the Extradition (Contiguous and Foreign Countries) Act, this Act and any other relevant law — (a) grant the legal assistance requested; or (b) refuse to grant the legal assistance requested. (5) The Central Authority may require a requested State to — (a) keep the contents, any information and material provided in a confidential manner; (b) only use the contents, information and material provided for the purpose of the criminal matter specified in the request; and (c) use it subject to other specified conditions.
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	**CMCA, PART V** **Article 58. Spontaneous information** (1) The Central Authority may, subject to this Act and any other relevant law, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences or might lead to a request for co-operation by the foreign State under this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	(2) Prior to providing the information under subsection (1), the Central Authority may request that such information be kept confidential or only subject to other specified conditions. (3) Where a foreign State cannot comply with the specified conditions specified under subsection (2), the State shall notify the Central Authority as soon as practicable. (4) Upon receipt of a notice under subsection (3), the Central Authority may determine whether to provide such information or not. (5) Where the foreign State accepts the information subject to the conditions specified by the Central Authority, that State shall be bound by them. **MUTUAL LEGAL ASSISTANCE ACT, 2011 (MLAA), PART VIII** **Article 48. Special co-operation** Subject to any written law and without prejudice to its own investigations, prosecutions or judicial proceedings, Kenya shall take measures to permit it to forward information on proceeds of criminal offences to a requesting state without prior request, where it considers that— (a) the disclosure of such information might assist a requesting state in initiating or carrying out investigations, prosecutions or judicial proceedings; or (b) it might lead to a request by a requesting state under this Act.
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;	**MLAA, PART I** **Article 3. Scope of application** This Act shall— (a) apply to requests for legal assistance from any requesting state or international entity to which Kenya is obligated on the basis of a legal assistance agreement or not; (b) regulate the rendering of legal assistance to any requesting state, unless otherwise regulated by agreement.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	**MLAA, PART II** **Article 5. Central Authority** (1) There is established an authority to be known as the Central Authority to perform functions specified in this Act. (2) The office of the Attorney-General shall be designated as the Central Authority established under subsection (1) of this section. **Article 6. Functions of central authority** (1) The functions of the Central Authority shall include— (a) transmitting and receiving requests for legal assistance and executing or arranging for the execution of such requests; (b) ensuring that requests for legal assistance conform to the requirements of law and Kenya's international obligations; (c) where necessary, certifying or authenticating, or arranging for the certification and authentication of, any documents or other material supplied in response to a request for legal assistance; (d) taking practical measures to facilitate the orderly and rapid disposition of requests for legal assistance; (e) negotiating and agreeing on conditions related to requests for legal assistance, as well as to ensuring compliance with those conditions; (f) making any arrangements deemed necessary in order to transmit the evidentiary material gathered in response to a request for legal assistance to a requesting state or to authorize any other authority to do so; (g) carrying out such other tasks as provided for by this Act or which may be necessary for effective legal assistance to be provided or received. (2) For the purposes of this Act, legal assistance means mutual legal assistance in criminal matters and includes, but is not limited to— (a) identifying and locating of persons for evidential purposes; (b) examining witnesses; (c) effecting service of judicial documents; (d) executing searches and seizures; (e) examining objects and sites;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(f) providing, including formal production where necessary, originals or certified copies of relevant documents and records, including but not limited to government, bank, financial, corporate or business records; (g) providing information, evidentiary items and expert evaluations; (h) facilitating the voluntary attendance of witnesses or potential witnesses in a requesting state; (i) facilitating the taking of evidence through video conference; (j) effecting a temporary transfer of persons in custody to appear as a witness; (k) interception of items during the course of carriage by a public postal service; (l) identifying, freezing and tracing proceeds of crime; (m) the recovery and disposal of assets; (n) preserving communications data; (o) interception of telecommunications; (p) conducting covert electronic surveillance; (q) any other type of legal assistance or evidence gathering that is not contrary to Kenyan law.
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.	**CMCA, PART V** **Article 57. General principles relating to international cooperation** (…) (5) The Central Authority may require a requested State to — (d) keep the contents, any information and material provided in a confidential manner; (e) only use the contents, information and material provided for the purpose of the criminal matter specified in the request; and (f) use it subject to other specified conditions. **MLAA, PART VI** **Article 27. Interception of telecommunications** (…)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(5) The information provided under this section shall be confidential and shall be kept in accordance with the provisions of this Act or any other relevant written law. **Article 31. Preservation of communication data** (…) (5) If the Competent Authority considers that the preservation of communications data pursuant to a request made under this section will not ensure the future availability of the communications data, or will threaten the confidentiality of, or otherwise prejudice the investigation in a requesting state, it shall promptly inform a requesting state, which shall then determine whether the request should nevertheless be executed. **MLAA, PART VIII** **Article 42. Confidentiality** The confidentiality of a request and its contents and the information and materials supplied under this Act shall be maintained except for disclosure in the criminal matter specified in the request and where otherwise authorized by the other state.
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 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	**CMCA, PART V** **Article 59. Expedited preservation of stored computer data** (1) Subject to section 57, a requesting State which has the intention to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of data, may request the Central Authority to obtain the expeditious preservation of data stored by means of a computer system, located within the territory of Kenya. (2) When making a request under subsection (1), the requesting State 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;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(c) the stored computer data to be preserved and its connection to the offence; (d) any available information identifying the custodian of the stored computer data or the location of the computer system; (e) the necessity of the preservation; and (f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored computer data. (3) Upon receiving the request under this section, the Central Authority shall take the appropriate measures to preserve the specified data in accordance with the procedures and powers provided under this Act and any other relevant law. (4) A preservation of stored computer data effected under this section, shall be for a period of not less one hundred and twenty days, in order to enable the requesting State to submit a request for the search or access, seizure or securing, or the disclosure of the data. (5) Upon receipt for a request under this section, the data shall continue to be preserved pending the final decision being made with regard to that request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**CMCA, PART V** **Article 60. Expedited disclosure of preserved traffic data** Where during the course of executing a request under section 57 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Central Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
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: 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.	**CMCA, PART V** **Article 61. Mutual assistance regarding accessing of stored computer data** (1) Subject to section 57, a requesting State may request the Central Authority to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of Kenya, including data that has been preserved in accordance with section 60. (2) When making a request under subsection (1), the requesting State shall — (a) give the name of the authority conducting the investigation or proceedings to which the request relates; (b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws; (c) give a description of the purpose of the request and of the nature of the assistance being sought; (d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested State, give details of the offence in question, particulars of the investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) give details of any procedure that the requesting State wishes to be followed by the requested State in giving effect to the request, particularly in the case of a request to take evidence; (f) include a statement setting out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes; (g) give details of the period within which the requesting State wishes the request to be complied with; (h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the requested State; (i) give details of the stored computer data, data or program to be seized and its relationship to the offence; (j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or electronic device; (k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and (l) give any other information that may assist in giving effect to the request. (3) Upon receiving the request under this section, the Central Authority shall take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law. (4) Where the Central Authority obtains the necessary authorisation in accordance with subsection (3), including any warrants to execute the request, the Central Authority may seek the support and cooperation of the requesting State during such search and seizure. (5) Upon conducting the search and seizure request, the Central Authority shall, subject to section 59, provide the results of the search and seizure as well as electronic or physical evidence seized to the requesting State.
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	**CMCA, PART V** **Article 62. Trans-border access to stored computer data with consent or where publicly available**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	A police officer or authorised person may, subject to any applicable provisions of this Act — (a) access publicly available stored computer data, regardless of where the data is located geographically; or (b) access or receive, through a computer system in Kenya, stored computer data located in another territory, if such police officer or authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**CMCA, PART V** **Article 63. Mutual assistance in the real-time collection of traffic data** (1) Subject to section 57, a requesting State may request the Central Authority to provide assistance in realtime collection of traffic data associated with specified communications in Kenya transmitted by means of a computer system. (2) When making a request under subsection (1), the requesting State shall specify — (a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant traffic data; (d) the location at which the traffic data may be held; (e) the intended purpose for the required traffic data; (f) sufficient information to identify the traffic data; (g) any further details relevant to the traffic data; (h) the necessity for use of powers under this section; and (i) the terms for the use and disclosure of the traffic data to third parties. (3) Upon receiving the request under this section, the Central Authority shall take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Where the Central Authority obtains the necessary authorisation including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the search and seizure. (5) Upon conducting the measures under this section the Central Authority shall, subject to section 57, provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the requesting State.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**CMCA, PART V** **Article 64. Mutual assistance regarding the interception of content data** (1) Subject to section 57, a requesting State may request the Central Authority to provide assistance in the real-time collection or recording of content data of specified communications in the territory of Kenya transmitted by means of a computer system. (2) When making a request under subsection (1), a requesting State shall specify — (a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant communication; (d) the location at which or nature of the communication; (e) the intended purpose for the required communication; (f) sufficient information to identify the communications; (g) details of the data of the relevant interception; (h) the recipient of the communication; (i) the intended duration for the use of the communication; (j) the necessity for use of powers under this section; and (k) the terms for the use and disclosure of the communication to third parties. (3) Upon receiving the request under this section, the Central Authority shall, take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Where the Central Authority obtains the necessary authorisation, including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the requesting State during the search and seizure. (5) Upon conducting the measures under this section the Central Authority shall subject to section 57, provide the results of such measures as well as real-time collection or recording of content data of specified communications to the requesting State.
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 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.	**CMCA, PART V** **Article 65. Point of contact** (1) The Central Authority shall ensure that the investigation agency responsible for investigating cybercrime, 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, including carrying out the following measures — (a) the provision of technical advice; (b) the preservation of data pursuant to sections 59 and 60; (c) the collection of evidence, the provision of legal information, and locating of suspects, within expeditious timelines to be defined by regulations under this Act. (2) The point of contact shall be resourced with and possess the requisite capacity to securely and efficiently carry out communications with other points of contact in other territories, on an expedited basis. (3) The point of contact shall have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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