Uganda

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 02 March 2022

[reference to the provisions of the Budapest Convention]

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	No
Ratification/accession:	No

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	Computer Misuse Act (2011) **Part I – Preliminary** 2. Interpretation "**access**" means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective; "**application**" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system; "**child**" means a person under the age of eighteen years; "**computer**" means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices; "**computer service**" includes computer time, data processing and the storage retrieval of data; "**data**" means electronic representations of information in any form; "**electronic device**", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer; "**electronic record**" means data which is recorded or stored on any medium in or by a computer or other similar device, that can be read or perceived by a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	person or a computer system or other similar device and includes a display, printout or other out put of that data; "**function**" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer; "**information**" includes data, text, images, sounds, codes, computer programs, software and databases; "**information system**" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system; "**intercept**", in relation to a function of a computer, includes listening to or recording a function of a computer or acquiring the substance, meaning or purport of such a function; "program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function; "**traffic data**" means any computer data relating to 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 Copyright and Neighbouring Rights Act, 2006 PART I—PRELIMINARY 2. Interpretation "**computer programme**" means a set of instructions expressed in any language, code or notation, intended to cause the device having an information processing capacity to indicate, perform or achieve a particular function, task or result; Electronic Transactions Act (2011) "**electronic transaction**" means the exchange of information or data, the sale or purchase of goods or services, between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks; "**computer**" means electronic, magnetic, optical, electrochemical, or other data processing device or a group of such interconnected or related devices,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	performing logical, arithmetic or storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or a group of such interconnected or related devices; "**service provider**" means— (i) any public or private entity that provides to the 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;
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.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **12. Unauthorised Access** (1)A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence. (6) The intent of a person to commit an offence under this section need not be directed at— (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer. (7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.
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.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **12. Unauthorised Access** (1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence. (7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	15. Unauthorised use or interception of computer service (1) Subject to subsection (2), a person who knowingly— (a)secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service; (b)intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device whether similar or not; or (c)uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both. (3) For the purposes of this section, it is immaterial that the unauthorised access or interception 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. Uganda Communications Act (2013) PART XIII—OFFENCES AND PENALTIES **79. Interception and disclosure of communication.** (1) Any operator of a communications service or system, or employee of an operator of a communications service or system who— (a) unlawfully intercepts any communication between other persons sent by means of that service or system; (b) unlawfully interferes with or obstructs any radio communication; or (c) unlawfully discloses any information in relation to a communication of which that operator or employee is aware, commits an offence and is liable on conviction to a fine not exceeding one hundred

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and twenty currency points or imprisonment not exceeding five years or both. (2) Any person who without lawful excuse, intercepts, makes use of or divulges any communication except where permitted by the originator of the communication, commits an offence and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **12. Unauthorised Access** (2)A person who intentionally and without authority to do so, interferes with data in a manner that causes the program or data to be modified, damaged, destroyed orrendered ineffective, commits an offence. (7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both. **16. Unauthorised obstruction of use of computer.** A person who, knowingly and without authority or lawful excuse— (a) interferes with or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer, commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both. **8. Unauthorised modification.** Modification is unauthorised if— (a) the person whose act causes it, is not entitled to determine whether the modification should be made; and (b) he or she does not have consent to the modification from a person who is entitled.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	14. Unauthorised modification of computer material. (1) A person who— (a) does any act which causes an unauthorised modification of the contents of any computer; and (b) has the requisite intent and the requisite knowledge at the time when he or she does the act, commits an offence. (2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer and by doing so— (a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; or (c) to impair the operation of any such program or the reliability of any such data. (3) The intent under subsection (1)(b) need not be directed at— (a) any particular computer; (b) any particular program or data or a program or data of any particular kind; or (c) any particular modification or a modification of any particular kind. (4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification that the person intends to cause is unauthorised. (5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind specified in subsection (2) is intended to be permanent or temporary. (6) A person who commits an offence under this section is liable on conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	Computer Misuse Act (2011) **Part III – Computer misuse offences** **16. Unauthorised obstruction of use of computer.** A person who, knowingly and without authority or lawful excuse— (a) interferes with or interrupts or obstructs the lawful use of, a computer; or commits an offence. commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise 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.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **12. Unauthorised Access** (3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence. (4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data, commits an offence. (7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both. **17. Unauthorised disclosure of access code** (1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence. (2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both. **18. Unauthorised disclosure of information.** (1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.
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.	
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.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **19. Electronic fraud** (1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both. (2) For the purposes of this section "electronic fraud" means deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.
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;	Computer Misuse Act (2011) **Part III – Computer misuse offences** **23. Child pornography** (1) A person who— (a) produces child pornography for the purposes of its distribution through a computer; (b) offers or makes available child pornography through a computer;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(c) distributes or transmits child pornography through a computer; (d) procures child pornography through a computer for himself or herself or another person; or (e) unlawfully possesses child pornography on a computer, commits an offence. (2) A person who makes available pornographic materials to a child commits an offence. (3) For the purposes of this section "child pornography" includes pornographic material that depicts— (a) a child engaged in sexually suggestive or explicit conduct; (b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or (c) realistic images representing children engaged in sexually suggestive or explicit conduct. (4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.
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	The Copyright and Neighbouring Rights Act, 2006 **46. Infringements of copyright** (1) Infringement of copyright or neighbouring right occurs where, without a valid transfer, licence, assignment or other authorisation under this Act a person deals with any work or performance contrary to the permitted free use and in articular where that person does or causes or permits another person to— (a) reproduce, fix, duplicate, extract, imitate or import into Uganda otherwise than for his or her own private use; (b) distribute in Uganda by way of sale, hire, rental or like manner; or (c) exhibit to the public for commercial purposes by way of broadcast, public performance or otherwise.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that 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.	(2) The use of a piece of work in a manner prejudicial to the honour or reputation of the author shall be deemed an infringement of the right of the owner of the right. **47. Offences and penalty** (1) A person who, without the authorisation of or licence from the rights owner or his or her agent— (a) publishes, distributes or reproduces the work; (b) performs the work in public; (c) broadcasts the work; (d) communicates the work to the public; or (e) imports any work and uses it in a manner which, were it work made in Uganda, would constitute an infringement of copyright; commits an offence and is liable on conviction, to a fine not exceeding one hundred currency points or imprisonment not exceeding four years or both. (2) A person who contravenes the rights of a producer of sound recording or audio-visual fixation, a broadcasting company or a producer of programme carrying signals commits an offence and is liable on conviction to a fine not exceeding wenty five currency points or imprisonment not exceeding on year or both. (3) Where a work is communicated to the public on the premises of an occupier or by the operation of any apparatus which is provided by or with any consent of the occupier of those premises, the occupier shall be deemed to be the person communicating the work to the public whether or not he or she operates the apparatus. (4) A person who sells or buys in the course of trade or imports any apparatus, article, machine or thing, knowing that it is to be used for making infringing copies of work, commits an offence and is liable on conviction, to a fine not exceeding fifty urrency points or imprisonment not exceeding one year or both. (5) In addition to the punishment prescribed by subsection (4) the Court shall, where an offence is committed under that subsection, order the forfeiture of the apparatus, article or thing which is the subject matter of the offence or which is used n connection with the commission of the offence. (6) Any person who does any act to make other people believe that he or she is the author or performer of a piece of work, whether that act is— (a) by words or writing; (b) through conduct or fraudulent tricks; or (c) the use of electronic or other device; commits an offence. (7) A person commits an offence who, having reasonable grounds to know or suspect that the act will induce, enable, facilitate or conceal an infringement of a copyright or a neighbouring right, does the following—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) remove or alters any electronic moral rights information without lawful authority to do so; (b) distributes, imports for distribution, broadcasts, communicates or makes available to the public any pirated work; (c) without lawful authority, distributes, imports for distribution, broadcasts, communicates or makes available to the public, any performance, copy of a sound recording or audio-visual fixation knowing that the moral rights information has been unlawfully removed or altered. (8) Where a work is communicated to the public on the premises of an occupier by live performance without the authority of the owner of the copyright or neighbouring right or agent, the occupier of the premises shall be deemed to have communicated the work to the public.
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.	Computer Misuse Act (2011) **Part III – Computer misuse offences** **21. Abetment and attempts** (1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence. (2) Any person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence. **22. Attempt defined** (1) When a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence. (2) It is immaterial— (a) except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	Computer Misuse Act (2011) **Part I – Preliminary** 2. Interpretation "person" includes any company or association or body of persons corporate or unincorporate;
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.	Computer Misuse Act (2011) Sanctions are set out under each specific offence.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on	Constitution of the Republic of Uganda (1995, as last amended in 2018) Chapter Four Protection and promotion of fundamental and other human rights and freedoms **27. Right to privacy of person, home and other property** (1) No person shall be subjected to— (a)unlawful search of the person, home or other property of that person; or (b)unlawful entry by others of the premises of that person.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property. International Covenant on Civil and Political Rights (1976), ratified by Uganda in 1995 **Article 17** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks. **Article 19** 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. The African Charter on Human and People's Rights (ACHPR, 1981) ratified by Uganda in 1986 **ARTICLE 9** Every individual shall have the right to receive information. Every individual shall have the right to express and disseminate his opinions within the law.
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	Computer Misuse Act (2011) **Part III – Investigations and procedures** **9. Preservation order** (1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification. (2) For the purpose of subsection (1), data includes traffic data and subscriber information. (3) An order made under subsection (1) shall remain in force—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(a) until such time as may reasonably be required for the investigation of an offence; or (b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Computer Misuse Act (2011) **Part III – Investigations and procedures** **10. Disclosure of preservation order** The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of— (a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or (b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.
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.	Computer Misuse Act (2011) **Part III – Investigations and procedures** **11. Production order** (1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling— (a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

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. 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.	(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control. (2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data;	Computer Misuse Act (2011) **Part V – Miscellaneous** **28. Searches and seizure** (1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing— (a) that an offence under this Act has been or is about to be committed in any premises; and (b) that evidence that such an offence has been or is about to be committed is in those premises, the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary. (2) An authorised officer may seize any computer system or take any samples or copies of applications or data— (a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere; (b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or (c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant. (4) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (3). (5) An authorised officer executing a search warrant referred to in subsection (3), may— (a) at any time search for, have access to and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant; (b) require a person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution ofthat search warrant; and (c) compel a service provider, within its existing technical capability— (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorties in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system. (6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (5), an authorised officer shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities. (7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers under this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both. (8) A computer system seized or samples or copies of applications or data taken by the authorised officer shall be returned within seventy two hours unless the authorised officer has applied for and obtained an order in an inter party application for extension of the time. (9) In this section— "authorised officer" means a police officer who has obtained an authorising warrant under subsection (1); and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hover craft.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Computer Misuse Act (2011) **Part V – Miscellaneous** **28. Searches and seizure** (3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant. 5) An authorised officer executing a search warrant referred to in subsection (3), may— (c) compel a service provider, within its existing technical capability— (i) to collect or record through the application of technical means; or (ii) to co-operate and assist the competent authorities in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system.
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	**Regulation of Interception of Communications Act 2010** 1. **Interpretation** "intercept" in relation to any communication which is sent; a) by means of a telecommunication system or radio communication system, means to listen to, record, read or copy the contents, whether in whole or in part;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	"interception interface" means the physical location within the service provider's telecommunication facilities where access to the intercepted communication or call related information is provided. "interception subject or "interception target" means the person whose communication are to be or are being intercepted. "service provider" means the provider of a postal service or telecommunication service. **Section 2 – Control of Interception** – restricts the right to intercept communications to a party to the communication; where a person has received consent of the person to whom, or the person by whom the communication is sent; or where a person is authorized by warrant **Section 4 – Restricts the right to intercept communications** to only authorized persons who must apply for warrant of interception. The following persons are duly authorized to apply for warrants of interception a. The Chief of Defense Forcers or his or her nominee b. The Director General of the External Security Organization or his or her nominee c. The Director General of the Internal Security Organization or his or her nominee d. The Inspector General of Police or his or her nominee **Section 8 (1), (a), (b), (c), (d) – Assistance by service providers** – Requires service providers to put in place mechanisms to support lawful interception of communications. Further provides that all call related information should be provided in real time or as soon as possible upon call termination **Section 8 (1) (h)** provides, where necessary, the capacity to implement a number of simultaneous interceptions in order – i. to allow monitoring by more than one authorized person;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ii. to safeguard the identities of monitoring agents and ensure the confidentiality of the investigations. **Section 11 – Interception capability of telecommunication service** – requires service providers to provide telecommunication service which has the capability to be intercepted and also to store call-related information in accordance with the Law
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	Computer Misuse Act (2011) **Part V – Miscellaneous** **30. Territorial jurisdiction** (1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda. (2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda. (3) For the purposes of this Act, this section applies if, for the offence in question— (a) the accused was in Uganda at the material time; or (b) the computer, program or data was in Uganda at the material time. **31. Jurisdiction of courts** A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.
Article 24 – Extradition	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 7 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.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents