Mauritius

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 31.03.2020

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	14/11/2013

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 and Cybercrime Act 2003 (Act No. 22 of 2003)** "access" in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system; "computer service" includes data processing and the storage or retrieval of data; "computer system" means a device or combination of devices, including input and output devices, but excluding calculators which are not programmable, and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions; "data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium; "information and communication service" means any service involving the use of information and communication technologies including telecommunication services; "information and communication technologies" means technologies employed in collecting, storing, using or sending out information and include those involving the use of computers or any telecommunication system;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"intercept" in relation to a function of a computer, includes listening to, or recording a function of a computer, or acquiring the substance, its meaning or purport of such function; "investigatory authority" means the police or any other body lawfully empowered to investigate any offence "modification" means a modification of the contents of any computer system by the operation of any function of that computer system or any other computer system as a result of which - (a) any program or data held in the computer system is altered or erased; (b) any program or data is added to its contents; or (c) any act occurs which impairs the normal operation of the computer system; "password" means any data by which a computer service or a computer system is capable of being obtained or used; "program" means a set of instructions, expressed in words, codes, schemes or any other form, which is capable, when incorporated in a machine readable medium, of causing a computer to perform or achieve a particular task or result; "service provider" means any person who provides an information and communication service, including telecommunication; "subscriber" means a person using the services of a service provider; "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, other than traffic or other data, by which can be established - (a) the type of the communication service used, the technical provisions taken to use the communication service and the period of the service;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) the subscriber's identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of a service agreement or arrangement; or (c) any other information on the site of installation of a communication equipment available on the basis of a service agreement or arrangement; "telecommunication" means a transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electro-magnetic systems whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception; "traffic data" means any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or 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.	**Computer Misuse and Cybercrime Act 2003 (Act No. 22 of 2003)** **3. Unauthorised access to computer data** (1) Subject to subsections (2) and (3), any person who causes a computer system to perform a function, knowing that the access he intends to secure is unauthorised, shall commit an offence and shall on conviction be liable to a fine not exceeding 50,000 rupees and to penal servitude not exceeding 5 years. (2) A person shall not be liable under subsection (1) where – (a) he is a person with a right to control the operation or use of the computer system and exercises such right in good faith;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) he has the express or implied consent of the person, empowered to authorise him, to have such an access; (c) he has reasonable grounds to believe that he had such consent as specified in paragraph (b); (d) he is acting pursuant to measures that can be taken under Part III of this Act; or (e) he is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property. (3) An access by a person to a computer system is unauthorised where the person – (a) is not himself entitled to control access of the kind in question; and (b) does not have consent to access by him of the kind in question from any person who is so entitled. (4) 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. **4. Access with intent to commit offences** (1) Any person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system, with intent to commit an offence under any other enactment, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) For the purposes of this section, it is immaterial that - (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time. **Information and Communication Technologies Act** **46. Offences** Any person who – (j) by means of an apparatus or device connected to an installation maintained or operated by a licensee – …. (iii) fraudulently installs or causes to be installed an access to a telecommunication line; (ka) wilfully tampers or causes to be tampered the International Mobile Station Equipment (IMEI) of any mobile device; **47. Penalties** (1) Any person who commits an offence under this Act, shall, on conviction, be liable to a fine not exceeding 1,000,000 rupees and to penal servitude for a term not exceeding 10 years. (2) The Court before which a person is convicted of an offence under this Act may, in addition to any penalty imposed pursuant to subsection (1), order - (a) the forfeiture of any installation or apparatus used in connection with the offence; (b) the cancellation of the licence held by the person convicted; (c) that the person convicted shall not be issued with a licence for such period as the Court thinks fit; (d) that a service provided to a person convicted of an offence under this Act shall be suspended for such period as the Court thinks fit. (3) An offence under this Act shall - (a) be triable by the Intermediate Court;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) not be triable by a District Court.
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 and Cybercrime Act 2003 (Act No. 22 of 2003)** **5. Unauthorised access to and interception of computer service** (1) Subject to subsection (5), any person who, by any means, knowingly - (a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, shall commit an offence. (2) (a) A person convicted for an offence under subsection (1) shall be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years. (b) Where as a result of the commission of an offence under subsection (1), the operation of the computer system, is impaired, or data contained in the computer system is suppressed or modified, a person convicted of such offence shall be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years. (3) For the purpose 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) a program or data held in any particular computer system. (4) A person shall not be liable under subsection (1) where he – (a) has the express or implied consent of both the person who sent the data and the intended recipient of such data; (b) is acting in reliance of any statutory power. **INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 2001** **46. Offences** Any person who - (k) wilfully damages, interferes with, removes or destroys an information and communication installation or service including telecommunication installation or service maintained or operated by a licensee; (m) without the prior approval of the Authority, imports any equipment capable of intercepting a message; (n) discloses a message or information relating to such a message to any other person otherwise than - (i) in accordance with this Act; (ii) with the consent of each of the sender of the message and each intended recipient of the message; (iii) for the purpose of the administration of justice, or (iv) as authorised by a Judge; (o) except as expressly permitted by this Act or as authorized by a Judge, intercepts, authorises or permits another person to intercept, or does any act or thing that will enable him or another person to intercept, a message passing over a network; Amended by [Act No. 21 of 2016]; [Act No. 14 of 2018] **47. Penalties** (1) Any person who commits an offence under this Act, shall, on conviction, be liable to a fine not exceeding 1,000,000 rupees and to penal servitude for a term not exceeding 10 years. (2) The Court before which a person is convicted of an offence under this Act may, in addition to any penalty imposed pursuant to subsection (1), order - (a) the forfeiture of any installation or apparatus used in connection with the

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	offence; (b) the cancellation of the licence held by the person convicted; (c) that the person convicted shall not be issued with a licence for such period as the Court thinks fit; (d) that a service provided to a person convicted of an offence under this Act shall be suspended for such period as the Court thinks fit. (3) An offence under this Act shall - (a) be triable by the Intermediate Court; (b) not be triable by a District Court. Amended by [Act No. 14 of 2018]
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 and Cybercrime Act 2003 (Act No. 22 of 2003)** **6. Unauthorised modification of computer material** (1) Subject to subsections (3) and (4), any person who, knowingly does an act which causes an unauthorised modification of data held in any computer system shall, on conviction be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years. (2) Where as a result of the commission of an offence under this section - (a) the operation of the computer system; (b) access to any program or data held in any computer; or (c) the operation of any program or the reliability of any data, is suppressed, modified or otherwise impaired, a person convicted for the offence shall be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years. (3) A person shall not be liable under this section where - (a) he is acting pursuant to measures that can be taken under Part III of this Act; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) he is acting in reliance of any other statutory power. (4) A modification is unauthorised if – (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from any person who is so entitled. (5) For the purposes of this section, it is immaterial whether an unauthorised modification or any intended effect of it, be permanent or merely temporary. **INFORMATION AND COMMUNICATION TECHNOLOGIES ACT 2001** **46. Offences** Any person who – (a) by any form of emission, radiation, induction or other electromagnetic effect, harms the functioning of an information and communication service, including telecommunication service; (b) with intent to defraud or to prevent the sending or delivery of a message, takes an information and communication message, including telecommunication message from the employee or agent of a licensee; (c) with intent to defraud, takes a message from a place or vehicle used by a licensee in the performance of his functions; (d) steals, secretes or destroys a message; (e) wilfully or negligently omits or delays the transmission or delivery of a message; (f) forges a message or transmits or otherwise makes use of a message knowing that it has been forged;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(g) knowingly sends, transmits or causes to be transmitted a false or fraudulent message; **(ga)** uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to any person; (h) uses, in any manner other than that specified in paragraph (ga), an information and communication service, including telecommunication service, - (i) for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character; or (ii) which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to that person; (iii) for the transmission of a message which is of a nature likely to endanger or compromise State defence, public safety or public order. (ha) uses an information and communication service, including telecommunication service, to impersonate, or by any other means impersonates, another person which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to that person;
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 and Cybercrime Act 2003 (Act No. 22 of 2003)** **7. Damaging or denying access to computer system** Any person who without lawful authority or lawful excuse, does an act which causes directly or indirectly – (a) a degradation, failure, interruption or obstruction of the operation of a computer system; or (b) a denial of access to, or impairment of any program or data stored in, the computer system, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 and to penal servitude not exceeding 20 years.
Article 6 – Misuse of devices	**Computer Misuse and Cybercrime Act 2003 (Act No. 22 of 2003)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: 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.	**9. Unlawful possession of devices and data** (1) Any person who knowingly manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system or any other device, designed or adapted primarily for the purpose of committing any offence under sections 3 to 8, shall commit an offence. (2) Any person who knowingly receives, or is in possession of without sufficient excuse or justification, one or more of the devices under subsection (1) shall commit an offence. (3) Any person who is found in possession of any data or program with the intention that the data or program be used, by the person himself or another person, to commit or facilitate the commission of an offence under this Act, shall commit an offence. (4) For the purposes of subsection (3), possession of any data or program includes - (a) having possession of a computer system or data storage device that holds or contains the data or program; (b) having possession of a document in which the data or program is recorded; or (c) having control of data or program that is in the possession of another person. (5) Where a person is convicted under this section, he shall be liable to a fine not exceeding 50,000 and to a term of imprisonment not exceeding 5 years.
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	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 and Cybercrime Act 2003 (Act No. 22 of 2003)** **10. Electronic fraud** Any person who fraudulently causes loss of property to another person by- (a) any input, alteration, deletion or suppression of data; or (b) any interference with the functioning of a computer system, with intent to procure for himself or another person, an advantage, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.
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.	**The Child Protection Act** **Section 2 of the Act provides-** "film" has the meaning assigned to it by the Films Act 2002; "indecent photograph" includes an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film; "photograph" includes - (a) the negative as well as the positive version; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(b) data stored on a computer disc or by other electronic means which is capable of conversion into a photograph; "pseudo-photograph" means an image, whether made by computer graphics or by any other means, which appears to be a photograph; **15. Indecent photographs of children** (1) Any person who - (a) takes or permits to be taken or to make, any indecent photograph or pseudo-photograph of a child; (b) distributes or shows such indecent photograph or pseudo-photograph; (c) has in his possession such indecent photograph or pseudo-photographs, with a view to it being distributed or shown by himself or any other person; or (d) publishes or causes to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photograph or pseudo-photograph, or intends to do so, shall commit an offence. (2) Where a person is charged with an offence under subsection (1)(b) or (c), it shall be a defence for him to prove that - (a) he had reasonable grounds for distributing or showing the photograph or pseudo-photograph or having them in his possession; and (b) that he had not himself seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent. (3) Where -

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the impression conveyed by the pseudo-photograph is that the person shown is a child; or (b) the predominant impression conveyed is that the person shown is a child, notwithstanding that some of the physical characteristics shown are those of an adult, the pseudo-photograph shall be treated for all purposes of this Act as showing a child. **18. Offences and penalties** Section 18(7) provides (7) The Court before which a person is convicted of an offence under section 15 may, in addition to any penalty imposed, order – (a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; (b) that the material subject matter of the offence be no longer stored on and made available through the computer system, or that the material be deleted.
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	**Section 56 of the Copyright Act provides -** **56. Offences** (1) Unless otherwise provided under this Act, any person who – (a) without the express authorisation of the author or owner of the copyright – (i) publishes, distributes or reproduces a work for commercial purposes; (ii) performs a work for the public for gain or against remuneration;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that 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.	(iii) communicates a work to the public for gain or against remuneration ; (iv) broadcasts a work for gain or remuneration; (v) makes a derivative work for gain or against remuneration; (vi) imports, otherwise than exclusively for his own private and personal use, sells, exposes or offers for sale or hire, or has in his possession in the course of trade, any copy of a work which constitutes an infringement of the copyright of its owner, or would constitute such an infringement if the copy of the work were made in Mauritius; (b) without the express authorisation of the owner of the related rights, infringes the exclusive rights of performers, producers of phonograms and broadcasting organisations for gain or against remuneration; (c) manufactures, imports for sale or rental, or provides such services as offering for sale, rental or distribution any device or means which is – (i) specifically designed or adapted to circumvent any device or means intended to prevent or restrict reproduction of a work or to impair the quality of any copy made thereof; or (ii) susceptible to enable or assist in the reception or further distribution of an encrypted program, which is broadcast or otherwise communicated to the public, by a person who is not entitled to receive the program; (d) has in his possession in the course of trade any apparatus, article or thing, knowing that it is to be used for making infringing copies of a work or for a purpose referred to in subsection (b); (e) intentionally or recklessly deprives the copyright owner or author of his rights, for gain or against remuneration, shall commit an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) For the purposes of subsection (1)(a), where a work is communicated to the public on the premises of an occupier by the operation of any apparatus which is provided by or with the consent of the occupier of those premises, the occupier shall be deemed to be the person communicating the work to the public, whether he operates the apparatus or not. (3) (a) Any person who commits an offence shall – (i) on a first conviction, be liable to a fine not exceeding 300,000 rupees and to imprisonment for a term not exceeding 2 years; (ii) on a second or subsequent offence, be liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 8 years. (b) Notwithstanding any other enactment, the Magistrate of the Intermediate Court shall have exclusive jurisdiction to try any person at first instance charged with an offence under this Act. (4) The Court before which a person is convicted of an offence may, in addition to any other penalty imposed – (a) order the forfeiture of any apparatus, article or thing which is the subject-matter of the offence or is used in connection with the commission of the offence; (b) order that such apparatus, article or thing shall be delivered up to any person lawfully entitled to it.
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.	**The Interpretation and General Clauses Act defines attempt as follows -** "attempt", in relation to an offence, means a commencement of execution which has been suspended or has failed in its effect through circumstances independent of the will of the person making the attempt;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Section 45 of the Interpretation and General Clauses Act provides – **45. Accomplices and attempts** Every accomplice and any person who attempts to commit an offence shall commit an offence and shall, on conviction, be liable to the penalty provided for the principal or completed offence, as the case may be. The Criminal Code contains general provisions which apply in cases where a person acts as an accomplice or aids and abets in the commission of a criminal offence **The Criminal Code (Cap 195 – 29 December 1838 Amended 25/01; 30/01; 5/02; 12/03; 22/03; 30/03; 34/05; 24/06)** **37. Accomplices** Except where otherwise provided in any enactment, the accomplices in a crime or misdemeanour shall be punished with the same kind of punishment, or one of the punishments applicable to the crime or misdemeanour, for the time that shall be fixed by the sentence. **38. Giving instructions and aiding and abetting** (1) Any person who, by gift, promise, menace, abuse of authority or power, machination or culpable artifice instigates, or gives any instruction for, the commission of a crime or misdemeanour shall be punished as an accomplice in the crime or misdemeanour. (2) Any person who procures arms, instruments, or any other means used in the commission of a crime or misdemeanour, knowing that they were to be so used, (3) Any person who knowingly aids and abets the author of any crime or misdemeanour in the means of preparing, facilitating or perpetrating the crime or misdemeanour, shall be deemed an accomplice, without prejudice to the punishments specially provided by law against the authors of plots or of instigations to offences affecting the internal or external safety of the State, even

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	in cases where the crime which was the object of the conspirators or instigators has not been committed. shall be deemed an accomplice.
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.	**The Interpretation and General Clauses Act defines "person" as follows –** "person" and words applied to a person or individual shall apply to and include a group of persons, whether corporate or unincorporate; **Sections 44, 44A and 44B of the Interpretation and General Clauses Act provides –** **44. Offence by agent or body corporate** (1) Where an offence is committed by— (a) an agent, the person for whom the agent is acting; (b) a body corporate, every person who, at the time of the commission of the offence, was concerned in the management of the body corporate or was purporting to act in that capacity, shall also commit the like offence, unless he proves that the offence was committed without his knowledge or consent and that he took all reasonable steps to prevent the commission of the offence. (2) (a) Where a company, société or other corporate body is charged with an offence, a representative may appear before the appropriate Court and enter a plea of guilty or not guilty on behalf of the company, société or other corporate body. (b) For the purposes of paragraph (a), "representative" means a director, or the secretary, of the corporate body or a person duly authorised by the corporate body to represent it. **44A. Offence by limited partnership**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Where an offence is committed by a limited partnership which does not have legal personality, every general partner shall commit the offence. (2) Where an offence is committed by a limited partnership which has legal personality, every person who, at the time of the commission of the offence, was concerned in the management of the limited partnership or was purporting to act in that capacity, shall also commit the like offence, unless he proves that the offence was committed without his knowledge or consent and that he took all reasonable steps to prevent the commission of the offence. (3) (a) Where a limited partnership is charged with an offence, a representative may appear before the appropriate Court and enter a plea of guilty or not guilty on behalf of the limited partnership. (b) In this subsection, "representative" means a partner, the secretary or any other person duly authorised by the limited partnership to represent it. (4) In this section, "limited partnership" has the same meaning as in the Limited Partnerships Act 2011. [S. 44A inserted by s. 82 of Act 28 of 2011 w.e.f. 15 December 2011.] **44B. Offence by Foundation** (1) Where an offence is committed by a Foundation, every person who, at the time of the commission of the offence, was concerned in the management of the Foundation or was purporting to act in that capacity, shall also commit the like offence, unless he proves that the offence was committed without his knowledge or consent and that he took all reasonable steps to prevent the commission of the offence. (2) (a) Where a Foundation is charged with an offence, a representative may appear before the appropriate Court and enter a plea of guilty or not guilty on behalf of the Foundation. (b) In this subsection, "representative" means the secretary or any other person duly authorised by the Foundation to represent it.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) In this section, "Foundation" has the same meaning as in the Foundations Act 2012. [S. 44B inserted by s. 51 (2) of Act 8 of 2012 w.e.f. 1 July 2012.]
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.	The different sanctions are provided for under the relevant provisions referred to above and they include imprisonment .
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the 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 Constitution is the supreme law of Mauritius and any law which is inconsistent therewith is void to the extent of the inconsistency. The Constitution, although not specifically providing for safeguards relating to cybercrime, contains general provisions which afford protection to fundamental rights and freedoms of persons, such as Article 9 The protection for privacy of the home or other property. Thus section 9(1) provides that except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises. However subsection (2) provides that nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision— … (d) to authorise, for the purpose of enforcing the judgment or order of a Court in any civil proceedings, the search of any person or property by order of a Court or the entry upon any premises by such order, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society. Further section 12 provides for the protection of freedom of expression as follows-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence. (2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision— (a) in the interests of defence, public safety, public order, public morality or public health; (b) for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the Courts, or regulating the technical administration or the technical operation of telephony, telegraphy, posts, wireless broadcasting, television, public exhibitions or public entertainments; or (c) for the imposition of restrictions upon public officers, except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society.
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	**THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 (Act No. 22 of 2003)** **11. Preservation order** (1) Any investigatory authority may apply to the Judge in Chambers 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 purposes of subsection (1), data includes traffic data and subscriber information.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(3) An order made under subsection (1) shall remain in force - (a) until such time as may reasonably be required for the investigation of an offence; (b) where prosecution is instituted, until the final determination of the case; or (c) until such time as the Judge in Chambers 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.	**THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 (Act No. 22 of 2003)** **12. Disclosure of preserved data** The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers 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; (b) sufficient data to identify the service providers and the path through which the data was transmitted; or (c) 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.	**THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 (Act No. 22 of 2003)** **13. Production order** (1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling –

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.	(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and (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, disc, cassette, or on microfilm, 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;	**THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 (Act No. 22 of 2003)** **14. Powers of access, search and seizure for the purposes of investigation** (1) Where an investigatory authority has reasonable grounds to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to a Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize such data. (2) In the execution of a warrant under subsection (1), the powers of the investigatory authority shall include the power to - (a) seize or secure a computer system or any information and communication technologies medium; (b) make and retain a copy of such data or information; (c) maintain the integrity of the relevant stored data or information; or (d) render inaccessible or remove the stored data or information from the computer system, or any information and communication technologies medium.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 (Act No. 22 of 2003)** **15. Real time collection of traffic data** Where the investigatory authority has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, it may apply to the Judge in Chambers for an order – (1) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or (2) compelling a service provider, within its technical capabilities, to - (a) effect such collection and recording referred to in subsection (1); or (b) assist the investigatory authority, to effect such collection and recording. **16. Deletion order** A Judge in Chambers may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains indecent photograph of children, order that such data be-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) no longer stored on and made available through the computer system or any other medium; or (2) deleted or destroyed. **17. Limited use of disclosed data and information** (1) No data obtained under sections 11 to 15 shall be used for any purpose other than that for which the data was originally sought except – (a) in accordance with any other enactment; (b) in compliance with an order of a court or Judge; (c) where such data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to the Government; (d) for the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or (e) in the public interest.
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.	

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 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.	
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	“ There is in force the Extradition Act 2017 which provides for a list of extraditable and non extraditable offences, and for the manner in which requests for extradition are to be made and processed. The Extradition Act operates in conjunction with the Deportation Act. Under the Extradition Act , offences of a political nature are non – extraditable and extradition requests are not entertained where there is a real risk of the extradited person being likely to be subjected to torture , or not receiving a fair trial (Section 8 of the Extradition Act on “Protection of Human Rights”) Extradition usually takes place when the requirements of the relevant extradition treaty are met and the offence is an extraditable one.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 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	**MUTUAL ASSISTANCE IN CRIMINAL AND RELATED MATTERS ACT** **Act 35 of 2003 – 15 November** 2003 **3. Application of Act** (1) This Act shall apply to— (a) any foreign State, subject to any condition, variation or modification in any existing or future agreement between Mauritius and that State; and (b) any international criminal tribunal. (2) This Act shall apply to requests for assistance in relation to serious offences committed before the coming into operation of this Act. (3) Nothing in this Act shall preclude the making and granting of an application in relation to a criminal matter under the Letters of Request Rules 1985. (4) Nothing in this Act shall prevent informal assistance and continued informal assistance between Mauritius and any other State. [S. 3 amended by s. 29 of Act 14 of 2009 w.e.f. 30 July 2009.]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	''Central Authority" means the Attorney-General, who shall, for the purposes of a request from a foreign State or an international criminal tribunal, or a request from Mauritius to a foreign State or an international criminal tribunal, be the appropriate competent authority; **5. Request to Mauritius** (1) A foreign State may, in relation to a serious offence, and an international criminal tribunal may, in relation to an international criminal tribunal offence, make a request for assistance to the Central Authority in any proceedings commenced in the foreign State or before the international criminal tribunal, as the case may be. (2) The Central Authority may, in respect of a request under subsection (1) from a foreign State— (a) promptly grant the request, in whole or in part, on such terms and conditions as it thinks fit or refer the matter to the appropriate authority for prompt execution of the request, in which case the Central Authority may represent the foreign State in proceedings entered to give effect to the request; (b) refuse the request, in whole or in part, on the ground— (i) that compliance with the request would be contrary to the Constitution; (ii) of prejudice to the sovereignty, international relations, security, public order, or other public interest of Mauritius; (iii) of reasonable belief that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that a person's position may be prejudiced for any of those reasons; (iv) of absence of dual criminality, where granting the request would require a Court in Mauritius to make an order in respect of any person or property in respect of conduct which does not

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	constitute an offence, nor gives rise to a confiscation or restraining order, in Mauritius; (v) that the request relates to an offence under military law, or a law relating to military obligations, which would not be an offence under ordinary criminal law; (vi) that the request relates to a political offence or an offence of a political character; (vii) that the request relates to an offence, the prosecution of which, in the foreign State, would be incompatible with laws of Mauritius on double jeopardy; (viii) that the request requires Mauritius to carry out measures that are inconsistent with its laws and practice, or that cannot be taken in respect of criminal matters arising in Mauritius; or (c) after consulting with the competent authority of the foreign State, postpone granting the request in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of proceedings in Mauritius. (3) The Central Authority may, in respect of a request under subsection (1) from an international criminal tribunal, grant the request, in whole or in part, on such terms and conditions as it thinks fit. (4) A request under subsection (1)— (a) may relate to any matter referred to in section 4 (2); and (b) shall contain such appropriate particulars as are referred to in section 4 (3). (5) A request shall not be invalidated for the purpose of this Act or any legal proceedings by virtue of any failure to comply with section 4 (3), where the Central Authority is satisfied that there is sufficient compliance to enable him to execute the request. (6) Where the Central Authority refuses a request, either in whole or in part, he shall so inform the foreign State or the international criminal tribunal.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(7) For the purpose of a request referred to in subsection (4), any reference in section 4 (2) or (3) to a foreign State or to Mauritius shall be construed as a reference to Mauritius or the foreign State, as the case may be.
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.	The Mutual Assistance in Criminal and Related Matters Act, in its Section 3, leaves open the possibility of informal assistance and continued informal assistance between Mauritius and any other State.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;	The Mutual Assistance in Criminal and Related Matters Act is in force since November 2003. It applies to requests from any foreign State and any international criminal Tribunal. Requests for mutual legal assistance may be refused , in whole or in part, where the request has been made for the purpose of prosecuting a person on account pf race , sex, reliogion, nationality, ethnic origin or political opinions, or the request relates to an offence under military law, or to an offence of a political character. (the full list is at Section 5(2) of the Act)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Section 20 of the Mutual Assistance on Criminal and Related Matters Act provides that documents are to be treated as privileged information. After the request has been dealt with, these documents are also to be returned to source (Section 21 on " Return of Materials")
Article 29 – Expedited preservation of stored computer data	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	
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	The Police Department has designated a number of officers to act as 24/7 points of contact through dedicated phone numbers.

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.	Mauritius acceded to the Convention without any reservations.

Back to the Table of Contents