Maldives

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 20th March 2025

[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:	

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	**Act Number 9/2014 (Penal Code of the Maldives)** **Section 250 (c)** "Computer system" means any digital or electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data **Section 250 (e)** "Data" or "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system; **Act Number 23/2010 (The Copyright and Related Rights Act)** **Section 41** 'computer' means an electronic or similar device having information processing capabilities; 'computer program' means a set of instructions expressed in words, codes, schemes or in any other form, which enables a computer to perform or achieve a particular task or result. **Act Number 43/2015 (Telecommunications Act)** **Section 125** "service provider" means a holder of a service provider licence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"service provider licence" means a licence issued under Section 5(a)(2) of the Act allowing for the provision of a telecommunications service specified in the licence "telecommunications service" means a service to the public for the carrying of communications by means of a telecommunications network. "communications" includes any communications:- (a) whether between persons and persons, things and things or persons and things; and (b) whether in the form of speech, music or other sounds; and (c) whether in the form of text; and (d) whether in the form of visual images (animated or otherwise); and (e) whether in the form of signals; and (f) whether in any other form; and (g) whether in any combination of forms.
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.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 240 - Unauthorized access to a computer system** **(a)** A person commits an offence if he does any of the following acts under the following circumstances. **(1)** causes a computer system to perform any function with intent to secure access to the whole or any part of any computer, program or data or to enable any such access to be secured; and **(2)** the access he intends to secure or to enable to be secured is unauthorized and is done so intentionally, and at the time when he causes the computer to perform the function, he knows that the access he intends to secure or to enable to be secured is unauthorized. **(b)** A person commits an offence if he acts recklessly as to whether he has authorization for the conduct under subsection (a)(2) of this Section. **(c)** It shall not be an offence if access to a computer system or program or data or any part thereof is undertaken in compliance with and in accordance with the terms of a warrant under any law or a court order. **(d)** For the purposes of this Section, access of any kind by any person to any computer system, program or data is unauthorized if––

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) he is not himself entitled or permitted to control access of the particular kind or type in question with respect to the computer, computer system, program or data in question; or **(2)** he does not have consent of the person entitled to grant such consent, for the particular kind or type of access in question with respect to the computer, computer system, program or data in question. **(e)** The intention or recklessness referred to in subsections (a) and (b) of this Section need not relate to or be directed at–– **(1)** any particular program or data; **(2)** a program or data of any particular kind; **(3)** a program or data held in a particular computer system. **(f)** The offence in subsection (a) of this Section is a Class 4 felony, if the person secured unauthorized access to a computer system or program or data or any part thereof connected to a critical infrastructure. **(g)** Otherwise, the offence is a Class 5 felony. **(h)** The offence in subsection (b) of this Section is a Class 5 felony, if the person secured unauthorized access to a computer system or program or data or any part thereof connected to a critical infrastructure. **(i)** Otherwise, the offence is a Class 1 misdemeanor. **Act Number 43/2015 (Telecommunications Act of Maldives)** **Section 77- Unauthorised access to computer by telecommunications** (a) Any person who, by a telecommunications service or telecommunications network, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer commits an offence punishable by a fine not exceeding Rf 500,000 (Rufiyaa Five Hundred Thousand) (b) For the purposes of subsection (a), the intent of the person need not be directed at:- (i) any particular program or data; (ii) a program or data of a particular kind; or (iii) a program or data held in a particular computer.
Article 3 – Illegal interception	**Act Number 9/2014 (The Penal Code of Maldives)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Section 242 - Unauthorized interception of computer data** **(a)** A person commits an offence if he does any of the following acts under the following circumstances. **(1)** intercepts or causes interception of the following transmissions, whether temporarily or not, directly or indirectly, by technical means–– **(i)** any non-public transmission of computer data to, from or within a computer system; or **(ii)** any non-public electromagnetic emissions from a computer system carrying computer data. **(2)** and the interception he intends to secure or to enable to be secured is unauthorized and is done so intentionally, and he knows that the interception he intends to secure or to enable to be secured is unauthorized. (b) A person commits an offence if he acts recklessly as to whether he has authorization for the conduct under subsection (a) of this Section. (c) It shall not be an offence if interception is undertaken in compliance with and in accordance with the terms of a warrant under any law or court order. (d) For the purposes of this Section, interception is unauthorized if in relation to a computer system, program or data, any interception where the person intercepting or causing interception to take place–– (1) is not the person with the responsibility for the computer or computer system; (2) is not the person who is entitled to determine whether such interception may take place; or (3) does not have consent for such interception from the person with the responsibility for the computer system. (e) The intention or recklessness referred to in subsections (a) and (b) of this Section need not relate to or be directed at–– (1) any particular computer system, program or data (2) a program or data of any particular kind; or (3) a program or data held in a particular computer system. (f) For the purposes of this Section, it is immaterial whether an unauthorized interception or any intended effect of it, be permanent or temporary. (g) The offence in subsection (a) of this Section is a Class 5 felony (h) The offence in subsection (b) of this Section is a Class 1 misdemeanor. **Act Number 43/2015 (Telecommunications Act of Maldives)** **Section 78- Unlawful interception of communications**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) A person who, without lawful authority under this Act or any other law: (1) intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any communication; (2) uses an apparatus or device to obtain information regarding the contents, sender or addressee of any communication; (3) discloses, or attempts to disclose, to any other person the contents of any communication, knowing or having reason to believe that the information was obtained through the interception of any communication in contravention of this Section; or (4) uses, or attempts to use, the contents of any communication, knowing or having reason to believe that the information was obtained through the interception of any communication in contravention of this Section, commits an offence. (b) A person who intentionally discloses, or attempts to disclose, to any other person the contents of any communication, intercepted by means authorised by this Act, where that disclosure or attempted disclosure was not authorised by this Act or any other law, commits an offence (c) An offence under sub-sections (a) or (b) is punishable by a fine not exceeding Rf 500,000 (Rufiyaa Five Hundred Thousand). (d) A telecommunications officer will not be liable for an activity referred to in section (a) or (b) where the relevant activity is carried out in performance of the person's lawful duties as such an officer
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.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 243 - Unauthorized interference of computer data** **(a)** A person commits an offence if he does any of the following acts under the following circumstances. (1) interferes or causes interference with program or data, whether temporarily or not; **(2)** and such interference with program or data is unauthorized and done so intentionally, and he knows that the interference he intends to secure or to enable to be secured is unauthorized.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) A person commits an offence if he acts recklessly as to whether he has authorization for the conduct under subsection (a) of this Section. (c) It shall not be an offence if interference is undertaken in compliance with and in accordance with the terms of a warrant or judicial order issued under any law. (d) For the purposes of this Section, interference with program or data means–– (1) damaging, deletion, deterioration, alteration, erasure or suppression of computer program or data; (2) addition of any program or data is added to contents of a computer system; (3) preventing or hindering access or availability to any computer program or data; (4) impairing the operation of any program or the reliability of any data; (5) altering the integrity or the content of any program or data; (6) impairing the availability or security of any program or data; (7) enabling, aiding, or abetting any of the actions mentioned in subsections (d)(1) to (d)(6) of this Section to be done. (e) For the purposes of this Section, interference with program or data is unauthorized in the following circumstances. (1) the person doing or causing such interference is not himself a person who has responsibility for the computer or computer system, and is not entitled to determine whether the interference may be done; or (2) the person doing or causing such interference does not have consent for the interference from a person who is entitled to determine whether the interference may be done. (f) The intention or recklessness referred to in subsections (a) and (b) of this Section need not relate to or be directed at–– (1) any particular computer system, program or data; (2) a program or data of any particular kind; or (3) a program or data held in a particular computer system. (g) For the purposes of this Section, it is immaterial whether an unauthorized interference with data, or any intended effect of it, be permanent or temporary. (h) The offence in subsection (a) of this Section is a Class 4 felony, if the person secured unauthorized interference with a program or data or any part thereof connected to a critical infrastructure. (i) Otherwise, the offence is a Class 5 felony.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(j) The offence in subsection (b) of this Section is a Class 5 felony, if the person secured unauthorized interference with a program or data or any part thereof connected to a critical infrastructure. (k) Otherwise, the offence is a Class 1 misdemeanor.
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	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 244 - Unauthorized interference of computer systems** (a) A person commits an offence if he does any of the following acts under the following circumstances. (1) interferes or causes interference with a computer system, whether temporarily or not; and (2) such interference with a computer system is unauthorized and done so intentionally, and he knows that the interference he intends to secure or to enable to be secured is unauthorized. (b) A person commits an offence if he acts recklessly as to whether he has authorization for the conduct under subsection (a) of this Section. (c) It shall not be an offence if interference is undertaken in compliance with and in accordance with the terms of a warrant under any law or court order. (d) For the purposes of this Section, interference with a computer system means by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing a program or data, the serious–– (1) hindering the functioning of a computer system; (2) impairment of the operation of any computer or computer system; (3) damage, prevention, suppression, deterioration, impairment, or obstruction of the functioning of a computer system; (4) hindering, damage, prevention, suppression, deterioration, impairment, or obstruction of communication within or with a computer system; (5) hindering or obstructing access to any computer system; (6) impairing the operation, reliability, or security of any computer system; (7) facilitating, aiding or encouraging any of the actions mentioned in subsections (d)(1) to (d)(6) of this Section to be done.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) For the purposes of this Section, interference with a computer system is unauthorized in the following circumstances. (1) the person doing or causing such interference is not himself a person who has responsibility for the computer system and is not entitled to determine whether the interference may be done; or (2) the person doing or causing such interference does not have consent for the interference from a person who is entitled to determine whether the interference may be done. (f) The intention or recklessness referred to in subsections (a) and (b) of this Section need not relate to or be directed at–– (1) any particular computer system, program or data; (2) a program or data of any particular kind; or (3) a program or data held in a particular computer system. (g) For the purposes of this Section, it is immaterial whether an unauthorized system interference, or any intended effect of it, be permanent or temporary. (h) For the purposes of subsection (d) of this Section, "serious" means the consequence of the offence committed under this Section results in serious harm of one or more of the following kind–– (1) causes significant financial loss; (2) threatens national security; (3) causes physical injury or death to any person; or (4) threatens public health or public safety. (i) The offence in subsection (a) of this Section is a Class 3 felony, if the person secured unauthorized interference with a computer system or any part thereof connected to a critical infrastructure. (j) Otherwise, the offence is a Class 4 felony. (k) The offence in subsection (b) of this Section is a Class 4 felony, if the person secured unauthorized interference with a computer system or any part thereof connected to a critical infrastructure. (l) Otherwise, the offence is a Class 5 felony. .

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Act Number 43/2015 (Telecommunications Act of Maldives) **Section 72 – Interference** (a) A person must not knowingly, and without lawful excuse, use an apparatus, whether or not it is telecommunications equipment, in a manner that causes direct or indirect harmful interference with any telecommunications service lawfully provided, or any telecommunications equipment lawfully operated, in or outside the Maldives. (b) The Authority may, by notice in writing, direct a person possessing an apparatus, whether or not it is telecommunications equipment, to take such measures as the Authority specifies and within the time directed to prevent the interference specified in the notice. (c) A person who contravenes sub-section (a) or fails to comply with a direction under sub-section (b) commits an offence punishable by a fine not exceeding Rf 1,000,000 (Rufiyaa One Million) and is also punishable by a further fine not exceeding Rf 20,000 (Rufiyaa Twenty Thousand) for every day or part of a day during which the contravention continues. (d) The Authority may by written instrument specify the limits of conducted or radiated interference from any apparatus which is not subject to the licensing requirement under Section 4, to prevent harmful interference with telecommunications network, other network facilities or telecommunications services. (e) The powers of the Authority under Chapter 1 of Part 10 extend to the apparatus mentioned in sub-section (d). (f) The Authority may require an apparatus mentioned in sub-section (d) to be submitted to the Authority for testing to verify whether the apparatus complies with the limits specified by the Authority under that Section.
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:	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 245 – Misuse of devices** (a) A person commits an offence if he, intentionally, does any of the following acts under the following circumstances.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) Doing any of the following acts, with the intention that such device primarily be used or with the belief that it is primarily to be used to commit or to aid in the commission of an offence under Section 240, Section 242, Section 243, Section 244, Section 247 or Section 248 of this Act; (i) manufacture, produce, make, generate, adapt, transfer, import, export, distribute, share, supply, offer to supply, sell or otherwise make available primarily for use of any device, or (ii) acquire, obtain or procure primarily for use any device. (b) Although stated in subsection (a) of this Section, it shall not be an offence under this Section in the following circumstances. (1) any act stated in subsection (a) of this Section is done not primarily for the purpose of committing an offence under Section 240, Section 242, Section 243, Section 244, Section 247 or Section 248 of this Act; (2) any act stated in subsection (a)of this Section is done for the authorized training, testing, network analysis, protection of a computer system or similar legitimate use; (3) any act stated in subsection (a) of this Section is done in compliance of and in accordance with the terms of a warrant issued, court order, or in the exercise of any power granted by law. (c) The offence in subsection (a) of this Section is a Class 4 felony.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 247 - Computer-related forgery** **(a)** A person commits an offence if he, intentionally, does any of the following acts. (1) inputs, alters, deletes, or suppresses computer data resulting in inauthentic data, regardless of whether or not the data is directly readable and intelligible; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) it is done with the intent that the inauthentic data be considered or acted upon for legal purposes as if it were authentic. (b) The offence in subsection (a) of this Section is a Class 5 felony. .
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.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 248 - Computer-related fraud** **(a)** A person commits an offence if he, intentionally, does any of the following acts under the following circumstances. (1) causes a loss of property to another person by any unauthorized input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system; and (2) it is done with fraudulent or dishonest intent of procuring an unauthorized economic benefit or other wrongful gain of any other thing of value for himself or for another person. (b) The offence in subsection (a) of this Section is a Class 4 felony.
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.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 246 – Child Pornography** **(a)** A person commits an offence if he, intentionally, does any of the following acts. (1) publishes child pornography through a computer system; **(2)** produces child pornography for the purpose of its publication through a computer system; (3) possesses child pornography in a computer system or on a computer data storage medium. (b) It is an acceptable legal defence to a charge of an offence under subsection (a)(1) or (a)(3) of this Section if the person establishes that the access and/or possession of child pornography is for a *bona fide* scientific, research, medical, or law enforcement purposes.

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.	(c) (1) For purposes of subsection (a) of this Section, "child pornography" includes all photographs, videos, animations, realistic images and audio that depicts–– (i) a minor engaged in sexually explicit conduct (ii) a person who appears to be a minor engaged in sexually explicit conduct. (2) For purposes of subsection (a) of this Section, "minor" means a person under the age of 18 (eighteen) years. (3) For purposes of this Section, "publish" includes–– (i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or (ii) have in possession or custody, or under control, for the purpose of doing an act referred to in subsection (e)(1) of this Section; or (iii) print, photograph, copy, image, or make in any other manner something similar, for the purpose of doing an act referred to in subsection (e)(1) of this Section. (d) The offence in subsection (a) of this Section is a Class 3 felony. **Section 622 – Producing or Distributing Obscene Material** (a) Offense Defined. A person commits an offense if, with knowledge of its obscene nature or content, he: (1) sells, delivers, or provides one or more obscene writings, pictures, records, or other representations or embodiments of the obscene; or (2) presents or directs an obscene play, dance, or other performance; or (3) publishes, exhibits, or otherwise makes available anything obscene; or (4) performs an obscene act or otherwise presents an obscene exhibition of his body for gain; or (5) advertises or otherwise promotes the sale of material represented or held out by him to be obscene; or (6) creates, buys, procures, or possesses obscene matter or material with the purpose of distributing it in violation of this Section; or (b) Exception. A person does not commit an offense under Subsections (a)(1) through (a)(6) if the distribution is only to an institution or an individual having scientific or other special justification for possession of such material. (c) Rebuttable Presumption. The trier of fact shall presume, subject to rebuttal, a purpose to distribute from the creation, purchase, procurement, or possession of a mold, engraved plate, or other embodiment of obscenity specially adapted for reproducing multiple copies.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) Definition. Material or a performance is "obscene" if the average person, applying the contemporary adult community standards of the Maldives, would find that: (1) taken as a whole, the material or performance appeals to a prurient interest, and (2) depicts or describes sexual acts in a patently offensive way. (e) Grading. (1) Promoting Obscenity. The offenses in Subsections (a)(1) through (a)(6) are Class 1 misdemeanors. (2) Consuming Obscenity. Otherwise the offense is a Class 3 misdemeanor. (3) Aggravation for Child Pornography. The offense is one grade higher than it otherwise would be if the obscene material or performance is of a person who: (A) is a minor, or (B) cannot comprehend the nature of his acts because he is incompetent. **Act Number 12/2009 (Special Provisions Act to Deal with Sexual Abuse Offenders of Children)** **Section 18** (a) A person commits an offence, if he intentionally causes child prostitution, or involves a child in the creation of pornography or creates pornographic material where a child's sexual organ can openly be seen. (b) The offence prescribed in subsection (a) of this section shall be punishable with imprisonment for a period between 20 years and 25 years.
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	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 249 - Infringement of copyright and related rights** **(a)** A person commits an offence if he intentionally infringes any rights protected under Law Number 23/2010 (Copyright and Related Rights Act) by means of a computer system. (b) The offence in subsection (a) of this Section is a Class 4 felony.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 80 – Criminal Attempt** (a) Offense Defined. A person attempts to commit an offense if: (1) acting with the culpability required for commission of the offense, (2) he purposely engages in conduct that would constitute a substantial step toward commission of the offense if the circumstances were as he believes them to be. (b) Conduct Constituting a Substantial Step. (1) Corroboration of Purpose to Complete the Offense Required. Conduct constitutes a substantial step toward commission of an offense under Subsection (a)(2) only if it is strongly corroborative of the person's purpose to complete the offense. (2) Conduct That May Be Held to Constitute a Substantial Step. The following conduct, if strongly corroborative of the person's purpose to complete the offense, shall not be held insufficient as a matter of law to constitute a substantial step: (A) lying in wait, searching for, or following the contemplated victim of the offense; (B) enticing or seeking to entice the contemplated victim of the offense to go to the place contemplated for its commission; (C) reconnoitering the place contemplated for the commission of the offense; (D) unlawful entry of a structure, vehicle, or enclosure in which it is contemplated that the offense will be committed; (E)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	possession of materials to be employed in the commission of the offense, if such materials are specially designed for such unlawful use or can serve no lawful purpose of the person under the circumstances; or (F) possession, collection, or fabrication of materials to be employed in the commission of the offense, at or near the place contemplated for its commission, if such possession, collection, or fabrication serves no lawful purpose of the person under the circumstances.
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.	**Act Number 9/2014 (The Penal Code of Maldives)** **Section 70 – Liability of Corporation or Unincorporated Association** (a) A corporation or unincorporated association is liable for the commission of an offense if: (1) the commission of the offense is authorized, requested, commanded, or performed by the board of directors or by a high managerial agent who is acting in behalf of the corporation or association within the scope of his employment, or (2) (A) the offense is committed by a corporate agent acting: (aa) in behalf of the corporation or unincorporated association, and (bb) within the scope of his office or employment, and (B) the statute defining the offense does not otherwise designate the corporate agents for whose conduct the corporation or unincorporated association is accountable or the circumstances under which it is accountable, and [(C) the offense is either graded as a misdemeanor or the statute manifests a legislative purpose to hold corporations responsible for the actions of subordinate employees]2 ; or (3) the offense consists of an omission to discharge a specific duty of affirmative performance imposed on corporations or unincorporated associations by statute. (b) Due Diligence Defense. It is a defense to a prosecution under Subsection (a)(2) that the corporation or unincorporated association proves by a preponderance of the evidence that a high managerial agent having supervisory responsibility over the conduct constituting the offense exercised due diligence to prevent the commission of the offense, unless: (1) such a defense would be inconsistent with the legislative purpose of the statute defining the offense, or (2) the statute defining the offense expressly provides that no culpability is required. (c) Definitions. (1) "Corporation" means a public or private company that has satisfactorily fulfilled the statutorily-defined procedure for incorporation. (2) "Unincorporated association" means a trust, partnership, government or governmental subdivision or agency, or two or more persons having a joint or common economic interest. (3) "High managerial agent" means an officer of the corporation or unincorporated association, or any other corporate agent that holds a position with the authority to formulate policy or supervise subordinate employees in a managerial capacity. (4) "Corporate agent" means any director,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	officer, servant, employee, or other person who is authorized to act in behalf of the corporation or unincorporated association in any capacity. **Act Number 43/2015 (Telecommunications Act of Maldives)** **Section 74 – Administrative Penalties** (b) Where a person who commits an offence under this Act is a body corporate; and it is proven that the offence was committed with the consent, support or participation of a director or other officer concerned in the management of the body corporate, the director or other officer will be guilty of the same offence. **Section 75 – Conduct by Employees, Directors or Agents** (a) If, in a proceeding under this Act in respect of conduct engaged in by a body corporate, it is necessary to establish the state of mind of the body corporate in relation to particular conduct, it is sufficient to show: (1) that the conduct was engaged in by a director (or other officer), employee or agent of the body corporate within the scope of his or her actual or apparent authority; and (2) that the director (or other officer), employee or agent had the state of mind. (b) Any conduct engaged in on behalf of a body corporate by a director (or other officer), employee or agent of the body corporate within the scope of the person's actual or apparent authority; or by any other person at the direction or with the consent or agreement (whether express or implied) of a director (or other officer), employee or agent of the body corporate, if the giving of the direction, consent or agreement is within the scope of the actual or apparent authority of the director (or other officer), employee or agent; is taken for the purposes of this Act to have been engaged in also by the body corporate, unless the body corporate establishes that the body corporate took reasonable precautions and exercised due diligence to avoid the conduct.
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.	*Criminal sanctions mentioned above as stated in the Penal Code of Maldives for the corresponding offences.* **Act Number 43/2015 (Telecommunications Act of Maldives)** **Section 74 – Administrative Penalties** (c) Every contravention or failure to comply with this Act, any direction or written instrument made under this Act or the conditions subject to which any

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	licence has been granted, or assignment issued, constitutes an offence under this Act. For every such offence, where the penalty is not otherwise specifically prescribed under this Act, the offender will, in addition to the forfeiture of anything seized, be liable to a fine not exceeding:- (1) Rf 100,000 (Rufiyaa One Hundred Thousand) for the first occasion on which a penalty is so imposed; (2) Rf 500,000 (Rufiyaa Five Hundred Thousand) for the second occasion on which a penalty is so imposed; and (3) Rf 1,000,000 (Rufiyaa One Million) for any subsequent occasion on which a penalty is so imposed; and (4) an additional fine not exceeding Rf 20,000 (Rufiyaa Twenty Thousand) for each day the offence continues.
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.	*Procedures as stated below contain conditions and safeguards that protects the fundamanetal rights of the accused and promotes the rights of the victims. Evidentiary standards, court orders and law enforcement oversight stated in the relevant procedures.* **Criminal Procedure Code - Section 47** (a) An accused being questioned for committing a criminal act, has the right to remain silent without giving any information, at any time, except those information that is required to establish identity. If the accused chooses to use this right to remain silent, the accused must announce this and it should be recorded in writing. (b) Once the accused announces that he chooses to remain silent under sub-section (a) of this Section, he must not be further questioned regarding the act of which he is being accused of. If the accused chooses to remain silent while he was being questioned, the interrogation must stop immediately. (c) The accused has the right to be informed and choose the right to remain silent without giving any information. And he should be informed that any answer he gives afterwards can be used as evidence against him. (d) If the information that could be submitted to Court by a law enforcement authority can be used against the accused to prove that he committed a crime, the accused can choose to withhold such information and will have the right to remain silent in such situations. (e) Notwithstanding sub-section (d) of this Section, if the information given by the accused cannot be used against him as evidence, he must reveal such information to the law enforcement authority. The accused cannot use the right to remain silent in such situations.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(f) If a person is accused of a crime in in Law No 09/2014 (Maldives Penal Code) or crimes defined in other relevant law related to national security or if the person is accused of a crime stated under Article 110, 610 and 611 of Law No 09/2014 (Maldives Penal code), and although remaining silent itself cannot be considered as a reason to believe that the accused has committed the crime, if the person uses the right to remain silent without trying to prove otherwise, on condition that the evidences obtained in that case relates the criminal act to the accused, then the judge can consider remaining silent as a deciding factor to believe there is a relationship between the accused and the crime. **Criminal Procedure Code - Section 49** (a) During a criminal investigation or a criminal trial, if answering a specific question causes the accused shame, or difficulty in life, or changes other people's perception of him, but does not lead to a criminal charge being brought against him or prove an offence, then answering such a question is obligatory and is not within his right to remain silent. (b) An accused cannot use his right to remain silent when answering a question regarding a crime for which he has previously been convicted, as Article 60 of the Constitution prohibits double jeopardy. (c) In a situation other than that mentioned in subsection 48(b) of this Act, refusing to give a handwriting sample, or a fingerprint sample, or a sample from the outside of the accused's body, or a sample from the inside of the accused's body is not within his right against self-incrimination. (d) In a situation other than that mentioned in subsection 48(b) of this Act, an accused's right to remain silent or his right against self-incrimination does not include the duty to disclose the location of an object, or how to open a specific place, or a lock, or a password, or numbers that open a specific lock, or disclose an account. (e) An accused's right to remain silent or his right against self-incrimination does not include the duty to give a fingerprint sample, or a voice recording sample, or a hair sample, or a D.N.A sample, or a handwriting sample, or a signature sample or a photo or an x-ray or a measure, in order to establish the owner of a specific object, and it cannot be used as evidence against that person. **Criminal Procedure Code – Section 107**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) The accused may respond to the charge in the preliminary hearing in the following ways – (1) Plead guilty ; (2) Plead not guilty (b) If the accused chooses not to respond in any of the ways stated in subsection (a) of this Section, or if he does not attend the preliminary hearing, the Court shall deem that the accused has pleaded not guilty. In those circumstances, the preliminary hearings shall be brought to an end and the proceedings for trial shall commence according to the Act. (c) The Judge shall do the following, before the accused is summoned to respond to the claim as stated in subsection (a) of this Section. (1) Ensure that the accused has received a copy of the charge sheet and any relevant documents ; (2) Question whether the accused is aware of what the charges are, and explain the charges to the accused if it is unclear ; (3) Inform the accused that he has a right to plead not guilty ; (4) Inform the accused that he has the right to receive sufficient time and resources to work on exonerating himself within the scope provided by this Act or another Act ; (5) Inform the accused that he has a right to work on exonerating himself with the help of any lawyer of his choice, and in the event that the accused has been charged with a serious criminal offence, if he does not have the financial capacity to obtain legal counsel, such shall be appointed for him by the State according to the set guidelines ; (6) Inform the accused that he has a right to trial in his presence ; (7) Inform the accused that if he does not know Dhivehi language, he has a right to have a translator appointed for him according to Section 167 of the Act. (8) Inform that he has a right against self-incrimination, and any statements given by him to the Court can be used against him, and if he provides any false evidence, he may be charged with the offence of giving false evidence (9) Inform the accused that he has a right to cross-examine any witnesses presented by the State, and the right to present his own witnesses in Court; (10) Inform the accused that if he pleads guilty as stated in subsection (a)(1) of this Section, the case shall sent for fast track according to Section 162 of this Act. (d) Explain the charges against the accused and the penalty determined by the law against a person who commits a crime, is about to commit a crime, or assists another in committing a crime, according to subsection(c)(2) of this Section. If the charges against the accused are not proved, to the extent that he has evidence to prove that he was about to commit, or he assisted another in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	committing the crime, it can be established that he was about to commit, or assisted another in committing such crime. **Criminal Procedure Code - Section 198** (a) Unless otherwise stated in this Act or another Act establishing offences, a sentence by a court, or a court order or a decision made by the courts, or a decision made during the pre-trial motion stage, can be appealed if the party is of the view that such decision, court order or sentence violates the Constitution or law or judicial principle. (b) A decision made under subsection (a) of this Section, can be submitted for appeal within a maximum of 60 (sixty) days from the date of the decision. (c) A court order or a decision made in the pre-trial motion stage can be submitted for appeal within a maximum of 10 (ten) days from the date of issuing an order or decision. (d) Notwithstanding subsection (c) of this Section, a court order or a decision made in the pre-trial motion stage must be submitted for appeal by the prosecution within 48 hours from the date of issuing an order or decision. (e) If an order or decision of the court is submitted for appeal as per subsections (c) and (d) of this Section, the court shall make a judgment within a maximum of 7 (seven) days from the date of submission of appeal. **Act Number 43/2015 (Telecommunications Act of Maldives)** **Section 74 –** Administrative Penalties (d) A fine under this Act must not be imposed by the Authority unless:- (1) in all the circumstances of the case, the fine is proportionate and reasonable in relation to the failure or series of failures concerned giving rise to that fine; (2) the Authority is satisfied that the licensee or person, as the case may be, has been afforded a reasonable opportunity of complying with the relevant requirement of any licence condition, provision of this Act, or direction, in respect of which the fine is sought to be imposed; and (3) the Authority has afforded the licensee or person concerned, as the case may be, a reasonable opportunity to make representations and has considered all representations made before the Authority before making its decision whether or not to impose that fine.
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,	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74-2**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(a) Where a law enforcement authority has reasonable grounds to believe that the following circumstances exist, it may order the immediate preservation of computer data in the possession or custody of a particular person or entity. (1) a specified computer data stored in a computer system or computer data storage medium is required for the purposes of a particular criminal investigation; and (2) there is a risk that the data might intentionally or accidentally be deleted or erased, lost, rendered inaccessible or modified; (b) The order under subsection (a) of this Section shall be issued in writing. If a foreign entity offering its services in the Maldives is subject to the order, such order may be issued in English. (c) The order issued under subsection (a) of this Section can be delivered electronically to the person(s) subject to the order. (d) The person to whom the order under subsection (a) of this Section is issued shall, upon receiving it, comply with the following procedures. 1. immediately undertake measures necessary to ensure that data specified in the Order is not deleted, lost, rendered inaccessible or modified; 2. undertake preservation according to the technical requirements specified by the law enforcement authority; 3. cooperate with the law enforcement authority and notify it about the fulfilment of the order and any other circumstances relevant for the preservation of data; and 4. maintain confidentiality of the order and its implementation. (e) If the order under subsection (a) of this Section is issued for traffic data, the person to whom it is issued shall, in addition to obligations under subsection (d) of this Section, immediately disclose a sufficient amount of traffic data to enable

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the law enforcement authority to identify service providers and the path through which the communication was transmitted (f) The order issued under subsection (a) of this Section shall be valid for a duration specified by the law enforcement authority. In the first instance, it shall be for a period not longer than 90 (ninety) days. However, if necessary, the duration can be extended for another period of up to 90 (ninety) days.
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.	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74-2** (a) Where a law enforcement authority has reasonable grounds to believe that the following circumstances exist, it may order the immediate preservation of computer data in the possession or custody of a particular person or entity. (1) a specified computer data stored in a computer system or computer data storage medium is required for the purposes of a particular criminal investigation; and (2) there is a risk that the data might intentionally or accidentally be deleted or erased, lost, rendered inaccessible or modified; (b) The order under subsection (a) of this Section shall be issued in writing. If a foreign entity offering its services in the Maldives is subject to the order, such order may be issued in English. (c) The order issued under subsection (a) of this Section can be delivered electronically to the person(s) subject to the order. (d) The person to whom the order under subsection (a) of this Section is issued shall, upon receiving it, comply with the following procedures.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	5. immediately undertake measures necessary to ensure that data specified in the Order is not deleted, lost, rendered inaccessible or modified; 6. undertake preservation according to the technical requirements specified by the law enforcement authority; 7. cooperate with the law enforcement authority and notify it about the fulfilment of the order and any other circumstances relevant for the preservation of data; and 8. maintain confidentiality of the order and its implementation. (e) If the order under subsection (a) of this Section is issued for traffic data, the person to whom it is issued shall, in addition to obligations under subsection (d) of this Section, immediately disclose a sufficient amount of traffic data to enable the law enforcement authority to identify service providers and the path through which the communication was transmitted (f) The order issued under subsection (a) of this Section shall be valid for a duration specified by the law enforcement authority. In the first instance, it shall be for a period not longer than 90 (ninety) days. However, if necessary, the duration can be extended for another period of up to 90 (ninety) days.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74-3** (a) Upon application by the law enforcement authority, the Court may order–– 1. any person, including service provider, in the Maldives to submit to the law enforcement authority any computer data or subscriber information in their possession or control, or 2. any service provider based outside of the Maldives, but offering its services in Maldives, to submit to the law enforcement authority any

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	computer data or subscriber information relating to such services in that service provider's possession or control. (b) The application by the law enforcement authority to the Court for a production order shall include the following information— 1. information pertaining to the person, or service provider; 2. information identifying the computer data or subscriber information sought; 3. identity of person(s) to whom the computer data or subscriber information relate, if available; 4. reasons for the belief that computer data or subscriber information are within the possession or control of the person(s) subject to the order; 5. reasons explaining why and how the computer data or subscriber information sought are relevant for the investigation of a criminal offence; and 6. information whether the data or information are needed urgently. (c) The Court shall issue the order under subsection (a) of this Section if there are reasonable grounds to believe that the computer data or subscriber information are required for the purposes of a criminal investigation. (d) The order under subsection (a) of this Section shall not be issued against the suspect or the accused. (e) Where the law enforcement authority requests the production of computer data containing the following information, the Court shall issue an order under

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	subsection (a) of this Section if and to the extent that access to such information is permissible under the relevant law. 1. information stored in the context of activities pertaining to legal, medical, journalistic, religious, banking or any other regulated profession; and 2. information which is subject to professional secrecy or otherwise privileged on the basis of law. (f) If the law enforcement authority stipulates in the application that the data or information are urgently needed, the Court shall decide on the application within 24 (twenty-four) hours. (g) Upon receipt of the order issued under subsection (a) of this Section, the person or service provider subject to such order shall comply with the following procedures. 1. expeditiously submit to the law enforcement authority the computer data or subscriber information specified in the order; 2. submit data or information in the form and according to the technical requirements specified by the law enforcement authority; and 3. maintain confidentiality of the order and its implementation.
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	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74-4**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(a) If there are reasonable grounds to believe that a particular computer data within a computer system or a computer data storage medium which may be required for the purposes of a specific criminal investigation, upon application by the law enforcement authority, the Court shall have the power to issue an order empowering the authority to–– (1) search, or similarly access–– (i) computer system, or part thereof, and the computer data stored therein; (ii) a computer data storage medium wherein computer data is stored. (2) seize, or similarly secure, computer data, which includes the powers to–– (i) seize, or similarly secure, a computer system, or part thereof, or a computer data storage medium; (ii) make and retain a copy of that computer data; (iii) maintain the integrity of the relevant stored computer data; (iv) render inaccessible or remove that computer data in the accessed computer system. (b) The application by the law enforcement authority to the Court for an order to search and seize stored computer data shall include the following information— 1. information pertaining to the computer systems, or computer data storage mediums to be searched; 2. information pertaining to the owner(s) of computer systems, or computer data storage mediums to be searched; 3. reasons for the belief that the evidence required for the investigation is in the computer systems or storage medium specified; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	4. reasons for the belief that the necessary evidence cannot be obtained by less intrusive measures. (c) The Court shall issue the order under subsection (a) of this Section if there are reasonable grounds to believe that the computer data within a computer system, or part thereof, or a computer data storage medium, are required for the purposes of a criminal investigation. (d) In issuing an order under subsection (c) of this Section, the Court shall consider whether the measure is adequate and proportionate, taking due account of the nature and seriousness of the crime and the existence, or absence, of other less intrusive measures to gather the evidence. (e) If the application for an order under subsection (a) of this Section is in relation to computer data containing information collected or stored in the context of activities pertaining to legal, medical, journalistic, religious, banking or any other regulated profession, and protected by law as such, the Court shall, in addition to requirements under subsection (d) of this Section, consider the nature and the scope of the legal privileges applicable to relevant information, and the possible commission of criminal offence, or contribution to it, by the data holder. If, upon careful consideration of these factors, the Court decides to issue an order under subsection (a) of this Section, it shall–– (1) order that the search be done in the presence of a representative of the relevant professional organization; (2) order that all reasonable measures be undertaken to ensure that only the data which is strictly necessary for the purposes of investigation is accessed or seized.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(f) When implementing the order issued under subsection (a) of this Section, the law enforcement authority shall–– (1) have the right to execute it using such assistance as may be necessary; (2) have the right to order any person other than the suspect or the accused, who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein, to provide the information and assistance necessary to enable the undertaking of the measures stated to in subsection (a) of this Section; (3) have the right to extend the search to other computer system(s) which are accessible from or available to the system which is subject to an order under subsection (a) of this Section. (g) Although stated in subsection (f) of this Section, an order under subsection (a) of this Section shall not be issued against the suspect or the accused. (h) In implementing an order issued under subsection (a) of this Section, the law enforcement authority shall take the action stated in subsection (a)(2)(i) of this Section, only upon considering whether the purpose of the investigation can be achieved using the other measures stated in subsection (a)(2), and if it cannot be achieved that way.
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:	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74-5** (a) If there are reasonable grounds to believe that traffic data associated with specified communications is reasonably required for the purposes of a specific

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	criminal investigation, the Court may, on an application of the law enforcement authority, authorize real-time collection of that data. (b) In issuing an order under subsection (a) of this Section, the following procedures shall be followed by the Court. 1. Empower the law enforcement authority to collect or record in real-time traffic data associated with specified communications; 2. order the service provider to assist the law enforcement authority in real-time collection or recording of traffic data associated with specified communications; 3. order the service provider to collect or record in real-time traffic data associated with specified communications and submit that data to the law enforcement authority upon their request(s) during the validity of the order. (c) The application by the law enforcement authority to the Court for an order to collect traffic data in real time, shall include the following information–– 1. information specifying the communications for which it is necessary to collect associated traffic data; 2. information pertaining to the owner(s) of the devices involved in the communication; 3. reasonable belief that real-time collection of traffic data can provide evidence required for the criminal investigation; 4. reasonable belief that the necessary evidence cannot be obtained by less intrusive measures; and 5. the period for which the real-time collection of traffic data is requested. (d) In issuing the order under subsection (a) of this Section, the Court shall consider whether the measure is adequate and proportionate, taking due account of the nature and seriousness of the crime and the existence, or absence, of other less intrusive measures to gather the evidence. (e) The Court shall authorize real-time collection of traffic data for a period as necessary, but in any case, no longer than 90 (ninety) days. The order can be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	extended upon application of the law enforcement authority if, after a fresh examination of the facts, the Court reasonably believes that the conditions for the order continue to exist. The order can be extended for periods of up to 90 (ninety) days each.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Act Number 12/2016 (Criminal Procedure Code)** **Section 74 - Interception of private communications** **(a)** Unless otherwise stated in any other Act, the law enforcement authority can intercept private communications stated under subsection (b) of this Section, with a Court order, if there is sufficient evidence to believe that it relates to the offences mentioned below. 1. Murder; 2. Serious organized crime; 3. Offence of terrorism; 4. Offence of money laundering and terrorism financing; 5. Human trafficking offences; 6. Drug trafficking offences; 7. Any criminal offences that relate to national security as stated in Law Number 9/2014 (Maldives Penal Code), or a criminal offence under any relevant law; 8. Sexual offences against children; 9. Offences stated in Section 246 of Law Number 9/2014 (Maldives Penal Code). (b) The law enforcement authority shall have the discretion to intercept the private communications mentioned below under the circumstances stated in subsection (a) of this Section. 1. Private communications made by post; 2. Private communications made via any communication device, electronic or otherwise.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) Before requesting a Court order to intercept the private communications stated in subsection (b) of this Section, the requirements stated below shall be fulfilled. 1. Sufficient evidence that proves that the person(s) subject to interception has committed, is committing, or is about to commit the offence; 2. Reasonable grounds that without interception, evidence of the offences mentioned in subsection (a) of this Section cannot be obtained; 3. The head of the law enforcement authority, or a person appointed by him, has given authorization to request the interception of a private communication. (d) The information stated below shall be submitted to the Court when requesting to obtain an Order for interception under subsection (b)(1) of this Section: 1. Name and address of the person(s) whose communication should be intercepted; 2. The offence that person(s) has committed, is committing, or is about to commit; 3. Evidence of the offence that the person has committed, is committing, or is about to commit; 4. Duration of interception under the order; 5. Name, rank and service number of the officer who shall discharge the responsibility for undertaking the interception authorized under the order; 6. The type of communication requested to be intercepted under the order. (e) In addition to the information stated in subsection (d) of this Section, the following information shall be submitted to request for a Court order authorizing the interception of a person's private communications stated in subsection (b)(2) of this Section. 1. Where the information stated under subsection (d) (1) of this Section is not known,, the Unique Identifier (U.I.D) of the device used for the communication; 2. The type of device or devices that will be used for interception under this court order; 3. The reasonable belief that any evidence pertaining to the offence can be obtained by this interception; 4. The service provider of the communication device required to carry out the interception under the court order;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	5. The location of the communication device, if it is located at a specific place, or if it can only be obtained upon entry into a specified place. (f) In issuing a Court order under subsection (a) of this Section, the Judge shall ensure the following— 1. That the institution has the authority to investigate the offence committed, is being committed, or is about to be committed by the person who is subject to the interception; 2. The offence committed, or being committed, or about to be committed by the person(s) who are subject to the interception is an offence stated under subsection (a) of this Section; 3. There is reasonable evidence to believe that the offence committed, is being committed, or is about to be committed by the person(s) who are subject to the interception; 4. The offence stated under subsection (a) of this Section can only be retrieved through interception; 5. The head of the law enforcement authority, or the person appointed by the head, has given authorization to the officer to undertake the interception; 6. The duration for the interception requested is reasonable; and 7. The Judge has the information obtained by the law enforcement authority and other information to determine that there is reasonable cause to issue the court order. (g) An order for the interception of private communications can be issued for a period as necessary, but in any case, no longer than 90 (ninety) days. (h) The order issued under subsection (g) of this Section can be extended upon application of the law enforcement authority, after a fresh examination of the facts provided the Court reasonably believes that the conditions for the order continue to exist. The order can be extended for periods of up to 90 (ninety) days each. (i) The court order issued under subsection (a) of this Section shall include the following–– 1. Name, address and national ID card number of the person(s) subject to the court order, or name, address, passport number and nationality if a foreigner(s) are the person(s) subject to the court order; 2. Where a communication is intercepted under subsection (b) (2) of this Section, in addition to the information in part (1) of this Section, the Unique Identifier (U.I.D) of the device to be used for the communication;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3. The offence the person is committing, or is about to commit; 4. The type of the communication, and the addresses or communication devices, under that court order; 5. The authorized date(s), or duration to undertake the interception of private communications; 6. Name, rank and service number of the officer in charge of taking responsibility for undertaking the interception authorized under that order; 7. That the court order shall not be executed otherwise or for other purposes; 8. The date issued, the signature and the name of the issuing judge and the Court's stamp; 9. The detailed information of the location of the communication device, if it is at a certain place, or the detailed information of the location if the information of the device cannot be reached except by entering a particular location. (j) The powers vested in the law enforcement authority under subsection (a) of this Section shall only be exercised in accordance with the court order issued under this Section. (k) Any information obtained by the interception stated in subsection (a) of this Section shall not be disclosed to any other persons, other than for the investigation for which the interception has been carried out and for the purposes of the Court proceedings.
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	**Penal Code – Section 13** (a) Statement of Jurisdiction. The State has jurisdiction to prosecute: (1) (A) any offense for which any conduct, described as an element of that offense, is committed in the Maldives; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(B) any offense in which the results cause substantial harm, described as an element of that offense, in the Maldives; or (C) any inchoate offense that, if completed, would include the conduct or result described above in the Maldives; or (D) any inchoate offense for which: (aa) an element of such an offense is committed in the Maldives, and (bb) the intended place for the completion or the effect of the offense is outside the Maldives, and (cc) the offense would be illegal both in the intended place of completion or effect, if completed, and in the Maldives, if it were performed there; and (2) any offense that results in substantial harm to citizens, agents, or property of the State, and any inchoate offense that, if completed, would have likely resulted in substantial harm to citizens, agents, or property of the State; and (3) any offense committed by or in cooperation with a citizen of the Maldives or a person domiciled in the Maldives regardless of the location of the offense; and (4) [any offense committed in gross violation of international law, regardless of the site of such offenses or the domiciles of the parties involved, and any offense over which the State is required to assume jurisdiction due to the State's adoption of an international treaty, though, unless stipulated otherwise, such a treaty shall not limit the jurisdiction of the State over such offenses; and (5) any offense committed against or on-board vessels or aircraft flagged or registered in the Maldives. (b) Jurisdiction Not an Element of an Offense. Establishing jurisdiction is a prerequisite to prosecution and not an element of an offense. The prosecution need not prove the culpability of the defendant as to any of the criteria for jurisdiction. (c) Power of the Court. This Section does not affect the power of a court to punish for contempt or to employ any sanction authorized by law for the enforcement of an order or civil judgment. (d) Claims for Extradition. Unless explicitly stipulated in an international treaty, a defendant has no standing to challenge a failure of the State to extradite him to another country.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**Act Number 1/2015 (Extradition Act)** **Section 13** **(a)** An offence is an extraditable offence under this Act where: (1) it is an offence for which a penalty of imprisonment or other deprivation of liberty for a period of not less than one year, or a more severe penalty has been prescribed in the laws of the Requesting State; (2) the conduct that constitutes the offence, if committed in the Maldives, would constitute an offence against the laws of Maldives, carrying a penalty of imprisonment or other deprivation of liberty for a period of not less than one year, or a more severe penalty. **In absence of extradition treaty:** **Section 36** **(a)** If a request for extradition of a person of a foreign State is made by a State other than that stated in Section 35 (treaty states), the Minister of Foreign Affairs may, in accordance with this Section, ordain and list the State in the Government Gazette as an Extradition Country. (b) In determining to ordain and list a country in the Government Gazette as an Extradition Country, the Minister of Foreign Affairs shall seek the Prosecutor General's opinion and take into account: (1) the general benefit to the Maldives; (2) severity of the offence the extradition request relates to; (3) the general benefit to the foreign country. (c) Unless stated otherwise in this Act, this Act shall apply to a State under this Section upon its publication as an Extradition Country in the Government Gazette. (d) This Act shall be applicable to a State listed as an Extradition Country under this Section to the extent provided in the respective announcement published in the Government Gazette. **Grounds for refusal:** **Section 14.** Under the following circumstances, authorization for extradition shall not be granted for a person of a foreign State in the Maldives. (a) Where the offence for which extradition is sought is a political offence, or with regards to the facts surrounding the offence, there are grounds to believe that offence is of a political nature; (b) Where there are substantial grounds to believe that the request for extradition was made for the purpose of prosecuting or punishing a person on account of the person's race, religion, sex, nationality or political opinions;

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	(c) There are grounds to believe that if extradited, the person may be prejudiced in a proceeding against him in the Requesting State on account of the person's race, religion, sex, nationality or political opinions; (d) The act or omission by the person sought, if it had occurred in Maldives, would have constituted a military offence under the laws of Maldives, which is however not an offence under the ordinary criminal laws of the Maldives; (e) the request for extradition relates to an offence for which final judgment has been rendered and enforced in the Maldives or another country, against the person sought; (f) prosecution against the person for the offence committed is barred by lapse of time or other reasons under the laws of Maldives and/or the Requesting State; (g) Person sought has been prosecuted under the laws of Maldives or the Requesting State in respect of the offence or conduct constituting the offence for which extradition is sought, and the person sought has been acquitted, has served the sentence, or has been pardoned by a competent court or other authority.
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	**Act Number 2/2015 (Mutual Assistance in Criminal Matters Act)** **Section 3 : Scope of Assistance** 1) Mutual legal assistance includes providing and obtaining the following things required in a criminal proceeding or criminal investigation: a) taking evidence or statements from persons; b) assisting in the availability of detained persons or others to give evidence or assist in investigations; c) effective service of judicial documents; d) Executing searches and seizures; e) Prevent dealing in any property and seizure of properties f) Examining objects and sites g) Providing information and evidentiary items; h) Providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records; i) Recovery of proceeds of crime as evidence. j) Nothing in the Act prevents the granting of any other form or nature of assistance that may lawfully be afforded to foreign States under any other written law or international agreement. **SECTION 6: Request to Maldives**

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.	1) A request by a foreign State to Maldives for assistance in a criminal matter under this Act shall be made to the Prosecutor General or to an authority authorized by the Prosecutor General to receive such requests. 2) Any request made to an authorized authority under subsection (1) shall be deemed as a request made to the Prosecutor General. 3) Request for assistance under this Act by foreign states shall be in writing in English language. Where the original request is not in English, it shall be accompanied with a certified translation of the original request. 4) Every request shall specify the following: a) Name of the requesting authority; b) Nature of assistance being sought and details of the procedure which that the foreign State wishes Maldives to follow in giving effect to the request; c) the name an description of the main function of the authority conducting the investigation, prosecution or judicial proceeding to which the request relates; d) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; e) where the request relates to a person, the name, nationality and location of that person; f) the purpose of the request; g) any other information the Prosecutor General requires to give effect to the request. 5) Failure to comply with subsection (3) and (4) shall not be a ground to refuse assistance. However, the Prosecutor General shall not proceed with the request unless the said provisions are complied with. 6) The regulation prescribed under this Act shall provide a template of form of request in accordance with this section. **SECTION 8: Refusal of assistance** 1) A request by a foreign State for assistance shall be refused if, in the opinion of the Prosecutor General:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a) There are substantial grounds for believing that the request relates to the prosecution or punishment of a person for an offence of a political nature; b) There are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, religion, sex, ethnic origin, nationality or political opinions; c) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Maldives, would have constituted a military offence under the laws of Maldives which is not also an offence under the ordinary criminal law of Maldives; d) the provision of the assistance would affect the sovereignty, security, public order or other essential public interest of Maldives; e) the request relates to the investigation, prosecution or punishment of a person for an offence in a case where the person has been convicted, acquitted or pardoned by a competent court or other authority in that prescribed foreign State; or has undergone the punishment provided by the law of that foreign State, in respect of that offence or of another offence constituted by the same act or omission as the first-mentioned offence; f) the request does not relate to types of assistance that may be provided under this Act. 2) A request by a foreign State for assistance under this Act may be refused by the Prosecutor General: a) the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Maldives, would not have constituted an offence against the laws of Maldives; b) the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission which occurred outside the foreign State, and Maldives would have no jurisdiction if such act or omission were committed out of Maldives; c) the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Maldives, would have constituted an offence against the laws of Maldives, but prosecution of such offence would be barred in Maldives due to passing of limitation period or such other bar to prosecution; d) the provision of the assistance could prejudice a criminal investigation or proceeding in Maldives; e) the provision of the assistance would, or would be likely to, prejudice the safety of any person;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	f) the provision of the assistance would impose an excessive burden on the resources of Maldives; g) The provision of assistance would result in an unjust treatment towards a person or violation of human rights of a person; h) Considering facts of the case, Prosecutor General is of the opinion that it is in the best interest to refuse request for assistance. 3) Assistance under this Act shall not be refused on the ground of bank secrecy. 4) The foreign State shall be informed if request for assistance is refused or provision of assistance is delayed, and the reasons shall be provided for any such refusal or delay.
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.	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)** **14-1. General Provisions** (a)Maldives may cooperate with any foreign State, 24 x 7 network, any foreign agency, or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems or computer data or for the collection of evidence in electronic form of any offence in accordance with the provisions of this Act. (b)The Prosecutor General may, without prior request, forward to such foreign State, 24 x 7 network, any foreign agency, or any international agency any information obtained from its own investigations if it considers that the disclosure of such information might assist the foreign State or agency in initiating or carrying out investigations or proceedings concerning any offence. (c)An investigating authority may, without the authorization of a foreign State– (1) access or receive, through a computer system in the Maldives, stored computer data located outside the Maldives, after obtaining the lawful and voluntary consent of the person who has the lawful authority to disclose the data located on that computer system. (2) access or receive, through a computer system in the Maldives, stored computer data located outside the Maldives, where there is a situation in which–– (ii) there is a significant and imminent risk to the life or safety of individuals; or (ii) there has been a significant economic harm, either in terms of quantum or the number of victims in the Maldives (d) The discretion granted under subsection (c) of this Section, shall be exercised by investigative authorities only in instances where the use of mutual assistance procedures under this Act would irreparably prejudice the ability of Maldives to investigate and prosecute an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(e) Upon receiving computer data or accessing data under subsection (c) of this Section, the authority that received or accessed the data shall notify relevant foreign state as soon as practicable. (f) Unless stated otherwise in another Act, This Section does not prohibit the access to publicly available (open source) stored computer data, regardless of where the data is located geographically. (g) The Prosecution General shall prescribe in the regulation under this act, the procedure to be followed in receiving or accessing data in a foreign state without their authorisation pursuant to subsection (c) of this Section. (h) The Prosecutor General or investigating authorities exercising their discretion under this chapter in carrying out the procedures under this Act, or providing mutual legal assistance to a foreign State, 24 x 7 network, any foreign agency, or any international agency shall ensure that it does not contravene Section 8 of this Act.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.	**MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT** **Section 4: Application of this Act** This Act is applicable to any foreign State. **Central authority** **SECTION 6**: A request by a foreign State to Maldives for assistance in a criminal matter under this Act shall be made to the Prosecutor General or to an authority authorized by the Prosecutor General to receive such requests. **SECTION 47**: **Request for assistance by international organization** 1) An international organization may request the Prosecutor General to provide assistance in criminal matters. 2) For the purpose of this section, an international organization is the International Criminal Police Organization (INTERPOL) or an organization authorized to make requests for assistance pursuant to a treaty the Maldives is party to.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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). 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	3) Unless stated otherwise in this Act, the sections relating to requests by foreign States apply to requests by international organizations.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 50**: **Foreign law immunity certificate** A duly certified foreign law immunity certificate is admissible in proceedings under this section as prima facie evidence of the matters stated in the certificate. **SECTION 51: Limitation on use of information** 1) Except with authorization of the Prosecutor General, any evidence, document or other thing obtained and provided pursuant to a request by the Prosecutor General under this Act shall not be used for any other purpose than related to the request. 2) Except with authorization of the Prosecutor General, anything requested shall not be used in a proceeding other than that stated at the time of the request. 3) Where an information, document or other thing is obtained pursuant to a thing stated in subparagraph (1), except with authorization of the Prosecutor General, such thing shall not be used in a proceeding other than that stated at the time of the request for things stated under subparagraph (1). 4) Any person who contravenes subparagraphs (1) (2) and (3) commits an offence. 5) Any person found guilty of the offence under subparagraph (4) is liable to a fine of MVR 5000 to MVR 10,000. 6) If the offender under subparagraph (4) is a legal entity, it shall be punishable with a fine of MVR 10,000 to MVR 25,000.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	7) For the purpose of this section, any disclosure of information of anything stated under this section shall be deemed as usage of such information. **SECTION 52: Confidentiality of information** 1) A person who, because of his or her official capacity or office, and being aware of the confidential nature of the request has knowledge of the contents of such request made under this Act; or the fact that such request has been, or is about to be, made; or the fact that such request has been granted or refused; shall not disclose those contents or these facts except to the extent that the disclosure is necessary to execute the foreign request or to the extent authorized by the Prosecutor General. 2) Any person who contravenes subsection (1) commits an offence. 3) Any person found guilty of the offence under subsection (1) is liable to a fine of MVR 5000 to MVR 10,000. If the offender under subparagraph (4) is a legal entity, it shall be punishable with a fine of MVR 10,000 to MVR 25,000
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;	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)** **Section 14-2. Expedited preservation of stored computer data** (a) A foreign State, 24 x 7 network, any foreign agency or any international agency may request the Prosecutor General to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within Maldives and in respect of which the foreign State, 24 x 7 network, any foreign agency, or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data pursuant to Section 14-4 of this Act. (b) Upon receiving the request under subsection (a) of this Section, the Prosecutor General, or an investigative authority designated by him shall take

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under Act Number 12/2016 (Criminal Procedure Act). (c) Any preservation effected in response to the request referred to under this Section shall be for a period no less than 60 (sixty) days, in order to enable the foreign State, 24 x 7 network, any foreign agency, or any international agency 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 until a final decision is taken on that pending request.
Article 30 – Expedited disclosure of preserved traffic data	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**14-3 Expedited disclosure of preserved traffic data** Where during the course of executing a request under Section 14-2, or otherwise concerning a specified communication, the Prosecutor General discovers that a service provider in another State was involved in the transmission of the communication, Maldives shall, without receiving a request, expeditiously disclose to the requesting foreign State, 24 x 7 network, any foreign agency, or any international agency a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**<u>Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)</u>** **14-4 Mutual assistance regarding accessing of stored computer data** (a) A foreign State, 24 x 7 network, any foreign agency, or any international agency may request the Prosecutor General to order or otherwise to search or similarly access, seize, or similarly secure, and disclose data stored by means of a computer system located within Maldives, including data that has been preserved pursuant to Section 14-2 of this Act. (b) A request for assistance under subsection (a) of this Section shall specify–– (1) the authority seeking the measure; (2) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (3) the computer system or other device to be searched or similarly accessed, seized or similarly secured or disclosed; (4) the stored computer data or program to be searched or similarly accessed, seized or similarly secured or disclosed, and its relationship to the offence; (5) any available information identifying the custodian of the stored computer data or the location of the computer system or other device;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) the significance of the search and seizure of data; (c) Upon receiving the request under this Section, the Prosecutor General or an investigative authority designated by the Prosecutor General shall take all appropriate measures to obtain necessary authorization, including any orders or warrants to execute the request in accordance with the powers and procedures provided under Act Number 12/2016 (Criminal Procedure Act). (d) Upon obtaining necessary authorization as required under subsection (c) of this Section, the Prosecutor General may seek the support and cooperation of the requesting authority during the search and seizure. (e) Upon executing the search and seizure request under subsection (a) of this Section, the Prosecutor General shall disclose the evidence seized or similarly secured to the requesting authority.
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.	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)** **14-1. General Provisions** (a)Maldives may cooperate with any foreign State, 24 x 7 network, any foreign agency, or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems or computer data or for the collection of evidence in electronic form of any offence in accordance with the provisions of this Act. (b)The Prosecutor General may, without prior request, forward to such foreign State, 24 x 7 network, any foreign agency, or any international agency any information obtained from its own investigations if it considers that the disclosure of such information might assist the foreign State or agency in initiating or carrying out investigations or proceedings concerning any offence. (c)An investigating authority may, without the authorization of a foreign State– (1) access or receive, through a computer system in the Maldives, stored computer data located outside the Maldives, after obtaining the lawful and voluntary consent of the person who has the lawful authority to disclose the data located on that computer system. (2) access or receive, through a computer system in the Maldives, stored computer data located outside the Maldives, where there is a situation in which– – (ii) there is a significant and imminent risk to the life or safety of individuals; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(ii) there has been a significant economic harm, either in terms of quantum or the number of victims in the Maldives (d) The discretion granted under subsection (c) of this Section, shall be exercised by investigative authorities only in instances where the use of mutual assistance procedures under this Act would irreparably prejudice the ability of Maldives to investigate and prosecute an offence. (e) Upon receiving computer data or accessing data under subsection (c) of this Section, the authority that received or accessed the data shall notify relevant foreign state as soon as practicable. (f) Unless stated otherwise in another Act, This Section does not prohibit the access to publicly available (open source) stored computer data, regardless of where the data is located geographically. (g) The Prosecution General shall prescribe in the regulation under this act, the procedure to be followed in receiving or accessing data in a foreign state without their authorisation pursuant to subsection (c) of this Section. (h) The Prosecutor General or investigating authorities exercising their discretion under this chapter in carrying out the procedures under this Act, or providing mutual legal assistance to a foreign State, 24 x 7 network, any foreign agency, or any international agency shall ensure that it does not contravene Section 8 of this Act.
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.	**Section 14-5. Mutual assistance regarding the real-time collection of traffic data** (a) A foreign State, 24 x 7 network, any foreign agency, or any international agency may request the Prosecutor General to order, direct, or otherwise provide assistance with the real-time collection of traffic data associated with specified communications in Maldives transmitted by means of a computer system. (b) Upon receiving the request under subsection (a), the Prosecutor General or an investigative authority designated by the Prosecutor General shall take all appropriate measures to obtain necessary authorization, including any orders or warrants to execute the request in accordance with the powers and procedures provided under Act Number 12/2016 (Criminal Procedure Act). (c) Upon obtaining necessary authorization as required under subsection (b) of this Section, the Prosecutor General may seek the support and cooperation of the requesting authority during the real-time collection of traffic data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(d) Upon executing the request for real-time collection of traffic data, the Prosecutor General shall disclose the traffic data collected to the requesting authority.
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.	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)** **Section 14-6. Interception of content data** (a) A foreign State, 24 x 7 network, any foreign agency, or any international agency may request the Prosecutor General to order, direct, or otherwise provide assistance with the real-time collection or recording of content data associated with specified communications in Maldives transmitted by means of a computer system. (b) Upon receiving the request under subsection (a), the Prosecutor General shall take all appropriate measures to obtain necessary authorization including any orders or warrants to execute the request in accordance with the powers and procedures provided under Act Number 12/2016 (Criminal Procedure Act). (c) Upon obtaining necessary authorization as required under subsection (b) of this Section, the Prosecutor General may seek the support and cooperation of the requesting authority during the interception of content data. (d) Upon executing the request for real-time collection of content data, the Prosecutor General shall disclose the content data collected to the requesting authority.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.	**Act Number 2/2015 (Mutual Legal Assistance in Criminal Matters Act)** **Section 14-7. 24/7 Network** (a) The Maldives Police Service shall designate a point of contact available on a twenty-four hour, seven-days-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or judicial proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. (b) The 24/7 Network established under subsection (a) of this Section shall include assistance in facilitating the following measures–– (1) the preservation of data pursuant to Section 14-2 and Section 14-3; (2) the collection of electronic evidence; (3) the provision of legal information; (4) locating of suspects; (5) provision of technical advice.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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