[Nauru]

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Version 14 March 2022

Table of contents

[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	**CYBERCRIME ACT 2015, No. 14 of 2015** **PART 1 – PRELIMINARY** **3) Interpretation** 'access provider' means any natural or legal person providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network; 'caching provider' means any natural or legal person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request; 'computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network; 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer; 'electronic data (or computer data)' means any representation of facts, concepts, information (being either texts, sounds or images) machine readable code or instructions, in a form suitable for processing in an electronic system, including a program suitable to cause an electronic system to perform a function; 'electronic system (or computer system)' means a device or a group of inter-connected or related devices, including the Internet, one or more which, pursuant to a program, performs automatic processing of data or any other function; 'hosting provider' means any natural or legal person providing an electronic data transmission service by storing of information provided by a user of the service; 'hyperlink' means a characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed; 'hyperlink provider' means any natural or legal person providing one or more hyperlinks; 'internet service provider' means a natural or legal person that provides to users, services mentioned in section 32 - 36 of this Act; 'service providers' include, but are not limited to internet service providers, access providers, hosting providers, caching providers, hyperlink providers and search engine providers; 'traffic data' means electronic data that: (a)relates to a communication by means of an electronic system; and (b)is generated by an electronic system that is part of the chain of communication; and (c)shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**CYBERCRIME ACT 2015, No. 14 of 2015** **6) Illegal access** (1) For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program data is used directly in connection with or necessary for: (a) the security, defence, or international relations of the Republic; (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, public utilities or public key infrastructure; or (d) the protection of public safety including system related to essential emergency services. (2) A person, who wilfully, without lawful excuse, accesses the whole or any part of a protected computer, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years. (3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in this section if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data is an offence.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CYBERCRIME ACT 2015, No. 14 of 2015** **7) Illegal interception** A person who intentionally, without right and with dishonest or otherwise unlawful intent, intercepts or attempts to intercept by technical means: (a) a transmission not intended for public reception of electronic data to, from or within an electronic system; or (b) electromagnetic emissions from an electronic system, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**CYBERCRIME ACT 2015, No. 14 of 2015** **8) Illegal data interference** A person who, wilfully or recklessly, without lawful excuse: (a) damages or deteriorates electronic data; or (b) deletes electronic data; or (c) alters electronic data; or (d) renders electronic data meaningless, useless or ineffective; or (e) obstructs, interrupts or interferes with the lawful use of electronic data; or (f) obstructs, interrupts or interferes with any person in the lawful use of electronic data; or (g) denies access to electronic data to any person authorised to access it, commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years.
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	CYBERCRIME ACT 2015, **No. 14 of 2015** **10) Illegal system interference** (1) A person who, wilfully or recklessly, without lawful excuse hinders or interferes: (a) with the functioning of an electronic system if he or she knows or ought to know that danger to life is likely to result; or (b) with a person who is lawfully using or operating an electronic system if he or she knows or out to know that danger to life is likely to result; or (c) with an electronic system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure. commits an offence punishable on conviction, to imprisonment for a period not exceeding 7 years
Article 6 – Misuse of devices	CYBERCRIME ACT 2015, **No. 14 of 2015** **11) Making, selling, distributing or possessing software or device for**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	**committing a crime** (1) A person who does any of the following with the sole purpose or principal use of which the person knows to be the commission of a crime, knowing or being reckless as to whether it will be used for the commission of a crime: (a)invites another person to acquire from the person any software, device or other electronic information that would enable the other person to access an electronic systems without authorisation; (b) offers or exposes for sale or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation; (c)agrees to sell or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation; (d)has in his or her possession for the purpose of sale or supply to another person any software, device or other electronic information that would enable the other person to access an electronic system without authorisation, commits an offence punishable on conviction to imprisonment for a term not exceeding 7 years. (2) A person who: (a)has in his or her possession any software, device or other electronic information that would enable him or her to access an electronic system without authorisation; and (b)intends to use that software, device or other electronic information to commit a crime, commits an offence punishable on conviction to imprisonment for a term not exceeding 7 years.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when 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,	**CYBERCRIME ACT 2015, No. 14 of 2015** **12 Computer-related forgery** A person who wilfully, without lawful excuse, inputs, alters, deletes, or suppresses electronic data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	whether or not the data is directly readable and intelligible commits an offence punishable on conviction, to imprisonment for a period not exceeding 10 years.
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.	**CYBERCRIME ACT 2015, No. 14 of 2015** **13 Computer-related fraud** A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, causes a loss of property to another person by: (a) any input, alteration, deletion or suppression of electronic data; or (b) any interference with the functioning of an electronic system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, the penalty shall be imprisonment for a period not exceeding 10 years.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 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;	**CYBERCRIME ACT 2015, No. 14 of 2015** **14 Child pornography** (1) A person who intentionally, without lawful excuse or justification: (a) produces child pornography material for the purpose of its distribution through an electronic system; (b) offers or makes available child pornography material through an electronic system; (c) distributes or transmits child pornography material through an electronic system; (d) procures or obtains child pornography material through an electronic system for oneself or for another person; (e) possesses child pornography material in an electronic system or on a data storage medium; and (f) knowingly obtains access, through information and communication technologies, to child pornography material, commits an offence punishable on conviction, to imprisonment for a period not exceeding 10 years. (2) It is a defence to a charge of an offence under subsection (1) (b), (c), (d), (e)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	and (f) if the person establishes that the child pornography material was a bona fide law enforcement purpose. If child pornography material was stored for such a purpose, the authorised person needs to ensure that it is deleted as soon as it is not legally required anymore. **15) Solicitation of children** A person, who intentionally, through the use of information and communication technology, proposes to a child to meet him or her, with the intent of committing an offence and where such proposal has been followed by material acts leading to such meeting, commits an offence punishable upon conviction to imprisonment for a period not exceeding 10 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 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	**The Copyright Law of England applies in Nauru because, according to the Custom and Adopted Laws Act 1971 of Nauru, the common law and statutes of general application, which were in force in England on January 31, 1968, are adopted as laws of Nauru.** **Copyright Act 2019 Part 5** **25. Meaning of infringing copy** (1) In this Act, the term infringing copy, in relation to a copyright work, shall be construed in accordance with this section. (2) An object is an infringing copy where its making constitutes an infringement of the copyright in the work. (3) An object that a person imports or proposes to import into the Republic is an infringing copy where: (a) the making of the object constituted an infringement of the copyright in the work in the country in which the object was made; or (b) the importer would infringe the copyright in the work in the Republic had the importer made the object in the Republic. (4) Where in any proceedings the question arises whether an object is an infringing copy and it is shown:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(a) that the object is a copy of the work; and (b) that copyright exists in the work or has existed at any time, — it shall be presumed until the contrary is proved that the object was made at a time when copyright existed in the work. (5) An object that a person imports or proposes to import into the Republic is not an infringing copy under subsection (3)(b) where: (a) it was made by or with the consent of the owner of the copyright, in the work in the country in which the object was made; or (b) where no person owned the copyright in the work in the country in which the object was made. **Copyright Act 2019 Part 5, Section 26** (1) A person infringes copyright in a work by acting in a way described under section 25 in relation to the work in the circumstances where the person: (a) does not own the copyright; (b) does not have the permission of the owner of the copyright to use the work; and (c) is acting in a way not permitted under Part 6. (2) This Act does not limit or affect the requirement to keep one or more copies of the published work in accordance with this Act or any other written law that requires copies to be deposited for the purposes of preserving the documents for heritage purposes.
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	**Crimes Act 2016 , Act No. 18 of 2016** **DIVISION 3.4 – EXTENSIONS OF CRIMINAL RESPONSIBILITY** **29 Aiding, abetting, counselling and procuring** (1) A person commits an offence if: (a) the person's conduct in fact aids, abets, counsels or procures the commission of an offence by another person (the 'other offender'); and (b) the other offender in fact commits the offence; and (c) the person: (i) intends the conduct to aid, abet, counsel or procure the commission of an offence of the type the other offender commits; or (ii) intends the conduct

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	to aid, abet, counsel or procure the commission of an offence and the person is reckless about the commission of the particular offence that the other offender in fact commits. (2) The offence is punishable as if the person had committed the offence mentioned in subsection (1)(b). (3) However, a person is not guilty of the offence if, before the offence is committed, the person: (a) terminates the person's involvement; and (b) takes all reasonable steps to prevent the commission of the offence. (4) This section applies regardless of whether the other offender or another person is prosecuted or found criminally responsible for the offence that the person aids, abets, counsels or procures.
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.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 4 – LIABILITY** **32 Access provider** (1) An Access provider is not criminally liable for providing access and transmitting information on conditions that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; or (c) does not select or modify the information contained in the transmission. (2) The acts of transmission and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is necessary for the transmission. **33 Hosting provider** (1) A Hosting provider is not criminally liable for the information stored at the request of a user of a service, on the condition that: (a) the Hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) the Hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by ways other than by an order from a public authority, expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content. (2) Subsection (1) shall not apply when the user of the service is acting under the authority or the control of the Hosting provider. (3) If the Hosting provider is removing the content after receiving an order pursuant to subsection (1), he is exempted from contractual obligations with his customer to ensure the availability of the service. **34 Caching provider** A Caching provider is not criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on the conditions that: (a) the Caching provider does not modify the information; (b) the Caching provider complies with conditions of access to the information; (c) the Caching provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by the industry; (d) the Caching provider does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain data on the use of the information; and (e) the Caching provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. **35 Hyperlinks provider** A Hyperlink provider who enables the access to information provided by third person by providing an electronic hyperlink is not liable for the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	information if: (a) the Hyperlink provider expeditiously removes or disables access to the information after receiving an order from a court to remove the link; and (b) the Hyperlink provider upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a court, expeditiously informs the court to enable them to evaluate the nature of the information and if necessary issue an order to remove the content. **36 Search engine provider** A provider who makes or operates a search engine that either automatically or based on entries by others, creates an index of Internet-related content or makes available electronic tools to search for information provided by third parties, is not liable for search results on conditions that the provider: (a) does not initiate the transmission; and (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. **Crimes Act 2016, Division 3.5, Section 37** DIVISION 3.5 – CORPORATE CRIMINAL RESPONSIBILITY **37 Act applies to bodies corporate** (1) This Act applies to a corporation in the same way as it applies to an individual with any modifications: (a) set out in this Division; or (b) that are otherwise necessary to apply this Act (or a provision of this Act) to the corporation (rather than an individual). 2) A corporation may be found guilty of any offence (whether under this Act or another written law), including an offence punishable by imprisonment. Note for this section The Interpretation Act 2011, section 80 contains rules about how a penalty applies to corporations.
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	**Cybercrime Act Part 2, Sections 6-23** Part 2 – Substantive Criminal Law Section 6 - Illegal Access

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Section 7 - Illegal Interception Section 8 - Illegal Data Interference Section 9 - Data Espionage Section 10 - Illegal System Interference Section 11 - Making, Selling, Distributing or Possessing Software or Device for Committing a Crime Section 12 - Computer-Related Forgery Section 13 - Computer-Related Fraud Section 14 - Child Pornography Section 15 - Solicitation of Children Section 16 - Publishing of Indecent or Obscene Information or Matter in Electronic Form Section 17 - Identity-Related Crimes Section 18 - Spam Section 19 - Disclosure of Details of an Investigation Section 20 - Failure to Permit Assistance Section 21 - Sending or Publishing Information of Material Through Electronic Communication Section 22 - Harassment Utilising Means of Electronic Communication Section 23 - Racial and Religious Offences
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	**Cybercrime Act Part 3, Sections 24-31** **Part 3 – Procedural Law** Section 24 – Search and Seizure Section 25 – Assistance Section 26 – Production Order Section 27 – Expedited Preservation Section 28 – Partial Disclosure of Traffic Data Section 29 – Collection of Traffic Data Section 30 – Interception of Content Data Section 31 – Forensic Tool **5 Admissibility of electronic evidence** In proceedings for an offence against a law of Nauru, the fact that evidence has been generated from an electronic system does not prevent that evidence from being admissible.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	THE CONSTITUTION OF NAURU* safeguards the fundamental rights and freedoms of the citizen (articles 3 – 15) Cybercrime Act Part 4, Section 38 Act to have overriding effect The provisions of this Act shall have effect even if there is anything inconsistent contained in any other law for the time being in force in Nauru. Cybercrime Act Part 4, Section 39 Regulations The Cabinet may make regulations, not inconsistent with this Act, prescribing all matters that are necessary or convenient to be prescribed for carrying out or giving effect to the provisions in this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **27 Expedited preservation** (1) Where a police officer is satisfied that: (a) electronic data is stored in an electronic device is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the data may be destroyed or rendered inaccessible, the police officer may, by written notice given to a person in control of the electronic device, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days. (2) A judge, magistrate or registrar may upon application authorise an extension not exceeding 14 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.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **28 Partial disclosure of traffic data** If a judge, magistrate or registrar is satisfied on the basis of an application by a police officer that specified data stored in an electronic device or system of electronic devices is required for the purpose of a criminal investigation or criminal proceedings, the judge, magistrate or registrar may order such person to disclose sufficient traffic data about a specified communication to identify: (a) the service providers; and (b) the path through which the communication was transmitted.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **26 Production order** If a Court on application by a police officer is satisfied on the basis of information that specified electronic data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order: (a) a person in control of an electronic device or network of electronic devices to produce specified electronic data or printout of such information; and (b) an Internet service provider to produce information about persons who subscribe to or use their services.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **24 Search and seizure** (1) If a Court on application by a police officer, is satisfied on the basis of information that there are reasonable grounds to suspect that there may be in a place, an electronic system or electronic data: (a) that may be material as evidence in proving an offence; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to 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.	(b) that has been acquired by a person as a result of an offence, a judge, magistrate or registrar may issue a warrant authorising a police officer, with such assistance as may be necessary to enter the place to search and seize the thing or electronic data including search or similarly access: (i) an electronic system or part of it and electronic data stored within; and (ii) an electronic-data storage medium in which electronic data may be stored in the territory of the country. (2) Any person who exercises a search or seizure under this section, shall at the time or as soon as practicable: (a) make a list of what has been seized, with the date and time of seizure; and (b) give a copy of that list to the Director of Public Prosecutions; and (c) the occupier of the premises; or (d) the person in control of such electronic devices. (3) Subject to subsection (4), on request, any police officer or another authorised person shall: (a) permit a person who had the custody or control of the electronic devices, or someone acting on their behalf to access and copy electronic data on the system; or (b) give the person a copy of the electronic data (4) The police officer or another authorised person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies may: (a) constitute a criminal offence; or (b) prejudice: (i) the investigation in connection with which the search was carried out; or (ii) another ongoing investigation; or any criminal proceedings that are pending or that may be brought in relation to any of those investigations. (5) If a police officer who is undertaking a search based on subsection (1), has grounds to believe that the data sought is stored in another electronic device or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he or she shall be able to expeditiously extend the search or similar accessing to the other system.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) A police officer who is undertaking a search is empowered to seize or similarly secure electronic data accessed according to subsections (1) or (2). (7) In order to properly execute a search and seizure order, a police officer may employ the assistance of a person considered an expert in the area of information technology, computing and computers and other similar experience.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **29 Collection of traffic data** (1) If a judge, magistrate or registrar on application by police officer is satisfied on the basis of information that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may, by written notice given to a person in control of such data, request that person to: (a) collect or record traffic data associated with a specified communication during a specified period; and (b) permit and assist the police officer to collect or record that data. (2) If a judge, magistrate or registrar on application by a police officer, is satisfied on the basis of information that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may authorise the police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.
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	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 3 – PROCEDURAL LAW** **30 Interception of content data**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	If a judge, magistrate or registrar on application by a police officer is satisfied on the basis of information that content of electronic communication is reasonably required for the purposes of a criminal investigation, the judge, magistrate or registrar may: (a) order an Internet service provider whose service is available in Nauru through application of technical means to collect or record, to permit or assist competent authorities with the collection or recording of content 15 data associated with specified communications transmitted by means of an electronic system; or (b) authorise a police officer to collect or record that data through application of technical means.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and	CYBERCRIME ACT 2015**, No. 14 of 2015** **PART 1 - PRELIMINARY** **4 Jurisdiction** (1) Where an offence under this Act is committed by any person outside the Republic, he shall be deemed to have committed the offence within the Republic. (2) For the purposes of this section, this Act shall apply as if, for the offence in question; (a) the accused; or (b) the computer, program or data, was in the Republic at the material time

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis 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.	Extradition Act 1973 (2011) **5. Relevant offences** (1) For the purposes of this Act, an offence of which a person is accused or has been convicted in a designated country is a relevant offence if: (a) it is an offence which, however described in that law, falls within any of the descriptions set out in the Schedule and is punishable under that law with imprisonment for a term of 12 months or any greater punishment; and (b) the act or omission constituting the offence, or the equivalent act or omission, would constitute an offence against the law of the Republic if it took place within the Republic or, in the case of an extra-territorial offence, in corresponding circumstances outside the Republic. (2) In determining for the purposes of this Section, whether an offence against the law of a designated country falls within a description set out in the said Schedule, any special intent or state of mind or special circumstances of aggravation which may be necessary to constitute that offence under the law shall be disregarded. (3) The descriptions set out in the said Schedule include in each case offences of attempting or conspiring to commit, of assisting, counselling or procuring the commission of, or being accessory before or after the fact to, the offences therein described, and of impeding the apprehension or prosecution of persons guilty of those offences. (4) References in this Section to the law of any country include references to the law of any part of that country. **SCHEDULE (Annex to Extradition Act 1973 (2011))**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	**Description of Relevant Offences** 18 An offence against the law relating to forgery 19 Stealing, embezzlement, fraudulent conversion, fraudulent false accounting, obtaining property or credit by false pretences, receiving stolen property or any other offence in respect of property involving fraud
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	Mutual Assistance in Criminal Matters Act 2004, **Act No. 16 of 2004** 'criminal matter' means an offence against a provision of: (a) any law of the Republic for which the penalty is imprisonment for a term not less than 12 months or a fine of no less than $5,000; (b) a law of a foreign country, in relation to acts or omissions, which had they occurred in the Republic, would have constituted an offence for which the penalty is imprisonment for a term not less than 12 months or a fine of no less than $5,000; **PART 2 – REQUESTS FOR ASSISTANCE GENERALLY** **6 Requests by Nauru for assistance generally**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	A request for international assistance in a criminal matter that Nauru is authorised to make under this Act may be made only by the Minister. **7 Requests by foreign countries for assistance generally** (1) Under this Act a request by a foreign country for international assistance in a criminal matter may be made to the Minister. (2) A request must be in writing or by e-mail and must include, or be accompanied by, the following information: (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; (d) any information that may assist in giving effect to the request. (3) Failure to comply with subsection (2) is not a ground for refusing the request, but the Minister is not obliged to consider the request until that subsection is complied with. (4) If a foreign country makes a request to the Court for international assistance in a criminal matter: Mutual Assistance in Criminal Matters Act 2004 As certified, and in force from 3 November 2004 6 (a) the Court must refer the request to the Minister; and (b) the request is then taken, for this Act, to have been made to the Minister
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.	**Mutual Assistance in Criminal Matters Act 2004**, **Act No. 16 of 2004** **PART 2 – REQUESTS FOR ASSISTANCE GENERALLY** **6 Requests by Nauru for assistance generally** A request for international assistance in a criminal matter that Nauru is authorised to make under this Act may be made only by the Minister. **7 Requests by foreign countries for assistance generally** (1) Under this Act, a request by a foreign country for international assistance in a criminal matter may be made to the Minister. (2) A request shall be in writing or by electronic mail and shall include, or be accompanied by, the following information: (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; and (d) any information that may assist in giving effect to the request. (3) Failure to comply with subsection (2) is not a ground for refusing the request, but the Minister is not obliged to consider the request until that subsection is complied with. (4) Where a foreign country makes a request to the court for international assistance in a criminal matter: (a) the court shall refer the request to the Minister; and (b) the request is then taken, for this Act, to have been made to the Minister. **9 Refusal or postponement of assistance** The Minister may, in respect of any request from a foreign country for mutual assistance in any investigation commenced or proceeding instituted in that foreign country relating to a serious offence:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	(a) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty, security or other essential public interest of the Republic; or (b) after consulting with the relevant authority of the foreign country, postpone the request, in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in the Republic.
Article 28 – Confidentiality and limitation on use	**Mutual Assistance in Criminal Matters Act 2004, Act No. 16 of 2004**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**PART 2 – REQUESTS FOR ASSISTANCE GENERALLY** **8 Assistance may be provided in whole or in part and subject to conditions** Assistance under this Act may be provided to a foreign country in whole or in part and subject to any conditions that the Minister determines. **PART 10 – MISCELLANEOUS** **60 Restriction on use of information, etc.** (1) Any material (whether it is evidence, a document, an article or a thing) that is sent to Nauru by a foreign country: (a) because of a request made by the Minister under this Act; and (b) for a proceeding or investigation in a criminal matter, must not be used intentionally for any other purpose without the approval of the Minister. (2) The material is inadmissible in evidence in any proceeding other than the proceeding for which it was obtained unless the Minister approves its use for that other proceeding. (3) Any information, document, article or thing obtained directly or indirectly from a person by making use of the material: (a) otherwise than for the proceeding or investigation for which it was obtained; and (b) without the approval of the Minister, is inadmissible in evidence in any other proceeding and may not be used for any other investigation. (4) A person who contravenes subsection (1) or (3) is guilty of an offence punishable by: (a) if the person is a natural person – a fine of up to $10,000 or a term of imprisonment up to 2 years, or both; or (b) if the person is body corporate – a fine of up to $50,000. (5) For this section, disclosure of any material is taken to be a use of that material. **61 Requests for international assistance must not be disclosed** (1) Subsection (2) applies to a person who, because of his or her office or employment, has knowledge of:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the contents of a request for international assistance made by a foreign country to Nauru under this Act; or (b) the fact that a request has been made; or (c) the fact that a request has been granted or refused. (2) The person must not intentionally disclose those contents or that fact unless: (a) it is necessary to do so in the performance of his or her duties; or (b) the Minister has given his or her approval to the disclosure of those contents or that fact. (3) A person who contravenes subsection (2) is guilty of an offence punishable by: (a) if the person is a natural person – a fine of up to $10,000 or a term of imprisonment of up to 2 years, or both; or (b) if the person is a body corporate – a fine of up to $50,000.
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; 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: 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.	**Mutual Assistance in Criminal Matters Act 2004**, **Act No. 16 of 2004** **PART 3** **17 Requests by the Republic for search and seizure** (1) This Section applies to a proceeding or investigation for a criminal matter involving a serious offence against the laws of the Republic if the Minister believes, on reasonable grounds, that a thing relevant to the proceeding or investigation may be located in a foreign country. (2) The Minister may request the appropriate authority of the foreign country to obtain a warrant or other instrument that, under the law of the foreign country, authorises: (a) a search for a thing relevant to the proceeding or investigation; and (b) if that thing or any other thing that is or may be relevant to the proceeding or investigation is found as a result of the search, the seizure of that thing. (3) A thing that: (a) is relevant to the proceeding or investigation; and (b) has been obtained by the appropriate authority of the foreign country, by a process authorised by the law of that country other than the issue as requested by the Republic of a warrant or other instrument authorising the seizure of the thing, may be admissible in evidence in the proceeding or used in the investigation despite having been obtained otherwise than in accordance with the request. **18 Request by foreign countries for search and seizure** (1) The Minister may direct an authorised officer to apply to a Judge for a search warrant, if: (a) a proceeding or investigation for a criminal matter involving a serious offence has commenced in a foreign country; (b) the Minister believes, on reasonable grounds, that a thing relevant to the investigation or proceeding is located in the Republic; and (c) the foreign country requests the Minister to arrange for the issue of a search warrant for that thing.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) The authorised officer may apply to the court for the issue of a warrant to search land or premises in the Republic for a thing relevant to the proceeding or investigation. **19 Search warrants** (1) Where an application is made under Section 18 for a warrant for a thing relevant to an investigation or proceeding in a foreign country, the court may issue the warrant authorising the authorised officer, with any assistance, and by any force, that is necessary and reasonable: (a) to enter the land or premises; and (b) to search the land or premises for that thing and to seize it. (2) A warrant issued under this Section shall include: (a) a statement of the purpose for which the warrant is issued, including a reference to the nature of the relevant offence; (b) a description of the kind of thing authorised to be seized; (c) a time at which the warrant ceases to have effect; and (d) a statement as to whether entry is authorised at any time or at specified times. (3) Where, in the course of searching under a warrant issued under Section 18 for a thing of a kind specified in the warrant, an authorised officer finds another thing, the warrant is taken to authorise the authorised officer to seize the other thing if the officer believes, on reasonable grounds, the other thing: (a) to be relevant to the proceeding or investigation in the foreign country or to provide evidence about the commission of a criminal offence in the Republic; and (b) to be likely to be concealed, lost or destroyed if it is not seized.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.	No established international Point of Contact.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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