Kiribati

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 03.02.2022

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

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 2021** **PART I – PRELIMINARY MATTERS** **3. Definitions:** ***'access'*** in relation to a computer system means to instruct, communicate with, store computer data in, receive computer data from, or otherwise make use of any of the resources of the computer system; (…) ***'computer data'*** means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a computer program suitable to cause a computer system to perform a function; ***'computer program'*** means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; ***'computer system'*** means any device or a group of interconnected or related devices, one or more of which, pursuant to a computer program, performs automatic processing of computer data; (…) ***'service providers'*** means— (a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service; (…) ***'subscriber's information'*** means any information contained in the form of computer data or any other form that is held by a service provider, relating to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	subscribers of its services other than traffic data 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; and (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement; (…) ***'traffic data'*** means computer data that— (a) relates to a communication by means of a computer system; and (b) is generated by a computer system that formed a part in the chain of communication; and (c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services;
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 2021** **PART III – OFFENCES AND PENALTIES** **7. Unauthorised access** (1) Access of any kind by any person to any computer program or computer data held in a computer system is illegal or unauthorised if that person— (a) is not entitled to control access of the kind in question to the computer program or computer data; and (b) does not have consent to access by him of the kind in question to the computer program or computer data from any person who is so entitled. (2) Any person who knowingly, or recklessly and without authority causes a computer system to perform any function for the purpose of securing access to that computer system or computer data held in any computer system is liable on conviction to a fine not exceeding $10,000 or to imprisonment not exceeding 7 years or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) For the purpose of this section, it is immaterial that the act in question is not directed at any particular- (a) computer program or computer data of any kind; or (b) computer program or computer data held in any computer system.
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 2021** **PART III – OFFENCES AND PENALTIES** **8. Unauthorised interception** (1) A person who knowingly or recklessly and without authority intercepts or attempts to intercept a non-public transmission by technical means of- (a) a computer data to, from or within a computer system; or (b) electromagnetic emissions from a computer system, commits an offence punishable upon conviction, to a fine not exceeding $10,000 or imprisonment for a period not less than 7 years, or to both. (2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular— (a) computer program or computer data of any kind; or (b) computer program or computer data held in any computer system.
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 2021** **PART III – OFFENCES AND PENALTIES** **9. Unauthorised data interference** (1) A person who, knowingly or recklessly, and without authority— (a) damages or deteriorates computer data; (b) deletes computer data; (c) alters computer data; (d) renders computer data meaningless, useless or ineffective; (e) obstructs, interrupts or interferes with the lawful use of computer data; (f) obstructs, interrupts or interferes with any person in the lawful use of computer data; and (g) denies access to computer data to any person authorised to access it, commits an offence punishable upon conviction, to a fine not exceeding $20,000 or imprisonment not exceeding 10 years, or to both. (2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) computer program or computer data of any kind; or (b) computer program or computer data held in any computer system.
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 2021** **PART III – OFFENCES AND PENALTIES** **10. Unauthorised system interference** (1) A person who, knowingly or recklessly, and without authority hinders or interferes with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data commits an offence punishable upon conviction, to a fine not exceeding $20,000 or imprisonment for a period not exceeding 10 years, or to both. (2) For the purpose of this section, it is immaterial that the act in question is not directed at any particular— (a) computer program or computer data of any kind; or (b) computer program or computer data held in any computer system.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences	**Cybercrime Act 2021** **PART III – OFFENCES AND PENALTIES** **11. Misuse of computer systems and computer program** Any person commits an offence who without authority, knowingly or recklessly produces, sells, possess, procures for use, imports, distributes or otherwise makes available— (a) a computer system or computer program designed or adapted primarily with the intent to committing an offence; or (b) a password, access code or similar computer data by which a computer may be accessed, with the intent that it be used to commit an offence, is punishable upon conviction, to a fine not exceeding $10,000 or imprisonment for a period not exceeding 7 years, or to both.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**Cybercrime Act 2021** **PART III – OFFENCES AND PENALTIES** **12. Computer-related forgery** A person who knowingly or recklessly and without authority, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic computer data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the computer data is directly readable and intelligible commits an offence punishable upon conviction, to imprisonment for a period not exceeding 7 years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 2021** **PART III – OFFENCES AND PENALTIES** **13. Computer-related fraud** A person who knowingly or recklessly, and without authority causes a loss of property to another person by— (a) any input, alteration, deletion or suppression of computer data; or (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, the penalty shall be imprisonment for a period not exceeding 7 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; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct	**Cybercrime Act 2021** **PART III – OFFENCES AND PENALTIES** **14. Sexual abuse material depicting a child** (1) A person who knowingly: (a) produces sexual abuse material depicting a child— (b) offers or makes available sexual abuse material depicting a child through a computer system; (c) distributes or transmits sexual abuse material depicting a child through a computer system; (d) procures or obtains sexual abuse material depicting a child through a computer system for oneself or for another person; (e) possesses sexual abuse material depicting a child in a computer system or on a computer-data storage medium; or (f) obtains access, by means of a computer system to sexual abuse material depicting a child, commits an offence punishable upon 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) and (f) if the person establishes that the sexual abuse material depicting a child was a bona fide law enforcement purpose. If sexual abuse material depicting a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	child 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 through the use of a computer system, communicates to a child, with the intent of committing an offence, including but not limited to; (a) soliciting a child (b) grooming a child; and (c) grooming a third party for the purposes of engaging in a sexual explicit conduct with a child 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.	**Cybercrime Act 2021** **PART VI – MISCELLANEOUS** **39. Copyright infringement** Any person who knowingly breaches the copyright of another person by means of computer system, commits an offence and shall be liable to punishment under the laws related to Copyright (**Copyright Act 2018**).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Cybercrime Act 2021** **PART III – OFFENCES AND PENALTIES** **19. Parties to offences** When an offence is committed, each of the following persons is deemed to have taken part in committing the offence and to be guilty of the offence, and may be charged with actually committing it, that is to say— (a) every person who knowingly aids or abets another person in committing the offence; and (b) any person who counsels or procures any other person to commit the offence.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal	**Cybercrime Act 2021** **PART III – OFFENCES AND PENALTIES** **20. Offences by a body corporate** (1) A body corporate commits an offence if an employee, agent or officer of the body corporate knowingly commits an offence under this Act to the benefit of that body corporate— (a) as a representative of the body corporate; (b) carrying out duties of such responsibility that the person's conduct may fairly be assumed to represent the policies of the body corporate; (c) with authority to exercise control within that body corporate; and (d) where the offence was made possible due to the lack of supervision or control of a person referred to in paragraphs (a), (b) or (c).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(2) An offence committed by a body corporate is punishable by a fine not exceeding $50,000. (3) An employee, agent or officer is guilty of and liable to the penalty provided for that offence.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	[Sanctions are detailed in the above-mentioned provisions]
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.	N/A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Cybercrime Act 2021** **PART IV – PROCEDURAL LAW** **29. Condition and safeguards for protection of rights** (1) The execution of powers and roles under this Act are subject to conditions and safeguards provided for under the Constitution and human rights obligations pursuant to applicable International Conventions. (2) Procedural safeguards for a child: (a) Proceeding for an offence against this Act must not be commenced without the consent of the Attorney-General if the defendant was under 18 at the time he or she allegedly engaged in the conduct constituting the offence. (b) However, a person may be prosecuted for, charged with, or remanded in custody in connection with, such an offence before the necessary consent has been given.
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	**Cybercrime Act 2021** **PART IV – PROCEDURAL LAW** **25. Expedited preservation**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) Where a police officer is satisfied that— (a) the specified computer data including content data and traffic data is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the computer data including content data and traffic data may be destroyed or rendered inaccessible, a police officer may write a notice to a person or a service provider in control of the computer system, ordering the person to ensure that the computer data, content data, traffic data and their integrity specified in the notice be preserved and maintained for a period of up to 60 days. (2) Any person who is served with a written notice (subsection 1) shall comply with the content of such notice. Failure to comply with the notice amounts to an offence punishable to 2 years imprisonment or $3,000 fine or both. (3) A police officer may extend the notice to a period not exceeding 100 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.	**Cybercrime Act 2021** **PART IV – PROCEDURAL LAW** **25. Expedited preservation** (1) Where a police officer is satisfied that— (a) the specified computer data including content data and traffic data is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the computer data including content data and traffic data may be destroyed or rendered inaccessible, a police officer may write a notice to a person or a service provider in control of the computer system, ordering the person to ensure that the computer data, content data, traffic data and their integrity specified in the notice be preserved and maintained for a period of up to 60 days. (2) Any person who is served with a written notice (subsection 1) shall comply with the content of such notice. Failure to comply with the notice amounts to an offence punishable to 2 years imprisonment or $3,000 fine or both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) A police officer may extend the notice to a period not exceeding 100 days. **26. Partial disclosure of traffic data** If a Police officer is satisfied that specified traffic data stored in a computer system is required for the purpose of a criminal investigation or criminal proceedings, the Police officers may order on a written notice the disclosure of sufficient traffic data about a specified communication to identify— (a) the service providers; and (b) the path through which the communication was transmitted.
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 2021** **PART IV – PROCEDURAL LAW** **24. Production order** If a Court on application by a police officer is satisfied that a person or service provider has in his possession or have control to a computer data in, on or of a computer system required for the purpose of a criminal investigation or criminal proceedings, it may order that person or service provider to provide that specified computer data or subscriber information.
Article 19 – Search and seizure of stored computer data	**Cybercrime Act 2021** **PART IV – PROCEDURAL LAW**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; 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.	**22. Search and seizure** (1) If a Court on application by a police officer, is satisfied that there are reasonable grounds to suspect that there may be in a place, a computer system or computer data— (a) that may be material as evidence in proving an offence under this Act; or (b) any other criminal offences committed by means of a computer system; (c) that has been acquired by a person as a result of an offence, a Court 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 computer data including search or similarly access: (i) a computer system or part of it and a computer data stored within; and (ii) a computer-data storage medium in which computer 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; (b) give a copy of that list to the Director of Public Prosecutions; (c) the occupier of the premises; and (d) the person in control of such computer system. (3) A police officer may refuse to give access or provide copies to the service provider or the owner if he or she has reasonable grounds to believe 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 (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations. (4) If a police officer who is undertaking a search based on subsection (1), has grounds to believe that the computer data sought is stored in another computer system or part of it in its territory, and such computer data is lawfully accessible

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	from or available to the initial computer system, he or she shall be able to expeditiously extend the search or similar accessing to the other computer system. (5) A police officer who is undertaking a search is empowered to seize or similarly secure computer data accessed according to subsections (1) or (2).
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 2021** **PART IV – PROCEDURAL LAW** **27. Collection of traffic data** If a Court on application by a police officer is satisfied that a person is engaged in conduct which may contravene this Act or constitute any other criminal offences committed by means of a computer system, a Court may issue a warrant authorising a police officer to: (a) collect or record through the application of technical means; and (b) compel a service provider, by written notice to that person or service provider, within its existing technical capability— (i) to collect or record through the application of technical means; or (ii) to assist the Police officer by all means to facilitate an investigation in the collection or recording of traffic data, in real-time, associated with specified communications transmitted in Kiribati by means of a computer system.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:	**Cybercrime Act 2021** **PART IV – PROCEDURAL LAW** **28. Interception of content data**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	If a Court on application by a police officer is satisfied that the content data of a communication is required for the purposes of a criminal investigation, a Court may issue a warrant authorising a police officer to: (a) collect or record through the application of technical means; and (b) compel a service provider or a person, within its existing technical capability: (i) to collect or record through the application of technical means, or (ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in Kiribati transmitted by means of a computer system.
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	**Cybercrime Act 2021** **PART I - PRELIMINARY MATTERS** **4. Application of this Act** This Act applies to: (1) Act or omission done or made in the territory of the Republic of Kiribati; and (2) Act or omission done or made— (a) on a ship or aircraft registered in the Republic of Kiribati; or (b) by a national of the Republic of Kiribati outside the territory of the Republic of Kiribati if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or (c) by a national of the Republic of Kiribati in any place or elsewhere.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis 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.	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **36. Extradition** The offences under this Act are extraditable offences under the laws relating to Extradition [**Laws of the Republic of Kiribati - revised edition 1981 - Chapter 32A EXTRADITION**]

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	
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	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **30. Cooperation with foreign Government** (1) The Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the following purposes— (a) investigations or proceedings concerning offences related to computer systems; (b) computer data, including content data and traffic data; (c) the collection of evidence in electronic form of an offence; (d) obtaining expeditious preservation and disclosure of traffic data or content data by means of a computer system or real-time collection of traffic data associated with specified communications, or interception of content data or any other means, power, function or provision under this Act.

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.	(2) Subject to the **Mutual Assistance in Criminal Matters Act 2003**, the Attorney General may— (a) make requests on behalf of Kiribati to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Kiribati, relating to any serious offence; (b) in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence— (i) grant the request, in whole or in part, on such terms and conditions as the Government thinks fit; (ii) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty or security of Kiribati or would otherwise be against the public interest; (iii) after consulting with the appropriate authority of the foreign State, 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 Kiribati; or (iv) postpone action on a request if such action would prejudice an investigation or proceeding in Kiribati.
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.	N/A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **31. Mutual Assistance Act not applicable** (1) Where the Mutual Assistance Act is not applicable to a foreign State, the Government may require the foreign State to— (a) keep confidential the contents of any information or material provided by the Government; (b) only use the contents and any information and material provided by the Government for the purpose of a specified criminal investigation; and (c) comply with any such other conditions of use as specified by the Government. (2) A request made on behalf of Kiribati to a foreign State for assistance under this provision must be made only by or with the authority of the Attorney-General.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **31. Mutual Assistance Act not applicable** (1) Where the Mutual Assistance Act is not applicable to a foreign State, the Government may require the foreign State to—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC 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.	(a) keep confidential the contents of any information or material provided by the Government; (b) only use the contents and any information and material provided by the Government for the purpose of a specified criminal investigation; and (c) comply with any such other conditions of use as specified by the Government. (2) A request made on behalf of Kiribati to a foreign State for assistance under this provision must be made only by or with the authority of the Attorney-General. or to imprisonment not exceeding 2 years or to both. **34. Request for assistance from the investigating agency** (1) Subject to any limitations specified by the Government, a foreign government, foreign agency or international agency may request the investigating agency to search or similarly access, seize or similarly secure, and disclose the computer data located within Kiribati, including the computer data that has been preserved pursuant to section 32. (2) A request for mutual assistance regarding accessing stored computer data must as far as practicable— (…) (f) include a statement setting out any requirements of the requesting State concerning any confidentiality relating to the request and the reasons for those requirements; (…)
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;	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **32. Request in relation to the expeditious preservation of data** (1) Subject to any limitations specified in this Part, a foreign government, foreign agency or any international agency may make a request to the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of a computer data, located within Kiribati or under the control of the Government and in respect of which the requesting foreign government, foreign agency or international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the computer data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 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	(2) A request for preservation made under subsection (1) must 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 that the foreign government, foreign agency or international agency 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) On receiving the request under subsection (1), the Attorney-General or 24/7 network must take all appropriate measures to preserve expeditiously the specified computer data in accordance with the procedures and powers provided under this Act. (4) Any preservation effected in response to the request referred to under this section must be for a renewable period of not less than 60 days, in order to enable the foreign government, foreign agency or international agency to submit a request for the search or similar access, seizure or similar securing, or disclosure of the computer data and following the receipt of such a request, the computer data must continue to be preserved until a final decision is taken on the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **33. Disclosure of service provider for transmission of specified communication** Where during the course of executing a request under this Act with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Attorney-General or 24/7 network, must expeditiously disclose to the requesting foreign government, foreign agency or 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.	**Mutual Assistance in Criminal Matters Act 2003** **Requests by Kiribati for search and seizure** 20. (1) This section applies if: (a) a proceeding or investigation for a criminal matter involving a serious offence against the law of Kiribati has commenced; and (b) the Attorney-General believes, on reasonable grounds, that a thing relevant to the proceeding or investigation may be located in a foreign country. (2) The Attorney-General may ask 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) the seizure of the thing or any other thing that is or may be relevant to the proceeding or investigation and is found as a result of the search. (3) A 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, if it: (a) is relevant to the proceeding or investigation; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 Kiribati) of a warrant or other instrument authorising the seizure of the thing. **Requests by foreign countries for search and seizure** 21. (1) The Attorney-General may direct a police officer to apply to the Court for a search warrant if: (a) a proceeding for, or investigation of, a criminal matter involving a serious offence has commenced in a foreign country; and (b) the Attorney-General believes, on reasonable grounds, that a thing relevant to the investigation or proceeding is located in Kiribati; and (c) the foreign country asks the Attorney-General to arrange for the issue of a search warrant for that thing. (2) The police officer must apply to the Court for the issue of a warrant to search land or premises in Kiribati for a thing relevant to the proceeding or investigation.
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.	**Cybercrime Act 2021** **PART VI – MISCELLANEOUS** **37. Trans-border access to stored computer data with consent or where publicly available** A Police officer may, without authorisation: (a) access publicly available stored computer data, regardless of where the computer data is located geographically; or (b) access or receive, through a computer system, stored computer data located in other Jurisdictions, if the Police officer obtains the lawful and voluntary consent of a person who has the lawful authority to disclose the computer data through that computer system.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**Cybercrime Act 2021** **PART V—INTERNATIONAL COOPERATION** **35. Mutual assistance regarding real-time collection of traffic data** (1) Subject to any limitations specified by the Government, a foreign government, foreign agency or any international agency may request the Attorney-General to provide assistance in real-time collection of traffic data associated with specified communications in Kiribati transmitted by means of a computer system. (2) A request for assistance under subsection (1) must so far as practicable specify—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant traffic data; (d) the location at which the traffic data may be held; (e) the intended purpose for the required traffic data; (f) sufficient information to identify the traffic data; (g) any further details relevant traffic data; (h) the necessity for use of powers under this section; and (i) the terms for the use and disclosure of the traffic data to third parties. (3) On receiving the request under subsection (1), the Attorney-General must take all appropriate measures to obtain necessary authorisation including any warrants to execute the request in accordance with the procedures and powers provided under Part 5. (4) On obtaining necessary authorisation including any warrants to execute the request, the Attorney-General may seek the support and cooperation of the foreign government, foreign agency or the international agency during the search and seizure. (5) On conducting the measures under this section, the Attorney-General must provide the results of such measures and real-time collection of traffic data associated with specified communications to the foreign government, foreign agency or the international agency.
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.	**Cybercrime Act 2021** **PART V - INTERNATIONAL COOPERATION** **30. Cooperation with foreign Government** (1) The Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the following purposes— (…) (b) computer data, including content data and traffic data; (…) (d) obtaining expeditious preservation and disclosure of traffic data or content data by means of a computer system or real-time collection of traffic data associated with specified communications, or interception of content data or any other means, power, function or provision under this Act.
Article 35 – 24/7 Network	**Cybercrime Act 2021**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**PART II – ESTABLISHMENT OF A CYBERCRIME UNIT** **6. 24/7 Network** (1) The Cybercrime Unit shall be a point of contact available on a twenty-four hour, seven-day- a-week basis. (2) The Unit shall provide assistance including facilitating, carrying out the following measures— (a) the provision of technical advice; (b) preservation of computer data pursuant to request from the requesting countries. (c) the collection of evidence, the provision of legal information, and locating of suspects. (3) The Unit shall have the capacity to carry out communications with the point of contact of other countries on an expedited basis. The Unit shall work collaboratively with the Office of the Attorney-General for international mutual assistance or extradition on an expedited basis. (4) The Unit 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