# Antigua and Barbuda

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version [21 February 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":**<br>For the purposes of this Convention:<br>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;<br><br>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;<br>c "service provider" means:<br><br>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and<br>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;<br>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 | **Electronic Crimes Act (2013)**<br><br>**Part I. Preliminary**<br>**Section 2 (Interpretation)**<br>In this Act –<br>"access" in the context of an electronic system means to communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the electronic system;<br>"damage" includes modifying, altering, deleting, erasing, suppressing, changing location or making data temporarily unavailable, halting an electronic system or chocking the networks;<br>"data" includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including electronic program, text, images, sound, video and information within a database or electronic system;<br>"electronic" means relating to technology having electrical, digital, magnetic, optical, biometric, electrochemical, wireless, electromagnetic, or similar capabilities;<br>"electronic database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by an electronic system or electronic network and are intended for use in an electronic system or electronic network;<br>"electronic device" is any hardware that accomplishes its functions using any form or combination of electrical energy;<br>"electronic system" means an electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes an electronic storage medium; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within an electronic system;<br>"service provider" means–<br>(a) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it through an electronic system;<br>(b) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunications services; or<br>(c) any other person that processes or stores data on<br>"subscriber" means a person using the services of a service provider;<br>"subscriber information" means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffi c data and by which can be established,<br>(a) the type of communication service used, the technical provisions taken there to and the period of service;<br>(b) the subscriber's identity, postal or geographic address, telephone and other<br>access number, billing and payment information, available on the basis of the service agreement or arrangement; or<br>(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;<br>"traffic data" means any data relating to a communication by means of an electronic system, generated by an electronic 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; and<br>"unauthorized access" means access of any kind by a person to an electronic system or data held in an electronic system which is unauthorized or done without authority or is in excess of authority, if the person is not himself entitled to control access of the kind in question to the electronic system or data and the person does not have consent to such access from a person so entitled. |
| **Article 2 – Illegal access**<br>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 | **Electronic Crimes Act (2013)**<br><br>**Part II. Offences**<br>**Section 3 (Access and interference)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (1) A person shall not intentionally, without lawful excuse or justification,–<br>(a) access an electronic system or network;<br>(2) A person who contravenes subsection (1) commits an offence and is liable on-<br>(i) summary conviction to a fine not exceeding two hundred thousand dollars or<br>to imprisonment for a term not exceeding three years, or to both; or<br>(ii) conviction on indictment to a fi ne not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both. |
| **Article 3 – Illegal interception**<br>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. | **Electronic Crimes Act (2013)**<br><br>**Part II. Offences**<br>**Section 3 (Access and interference)**<br>(1) A person shall not intentionally, without lawful excuse or justification,–<br>(b) download, copy or extract data, electronic database or information from such electronic system or network including information or data held or stored in a removable storage medium;<br>(c) introduce or cause to be introduced a contaminant or malicious code into an electronic system or network;<br>(2) A person who contravenes subsection (1) commits an offence and is liable on-<br>(i) summary conviction to a fi ne not exceeding two hundred thousand dollars or<br>to imprisonment for a term not exceeding three years, or to both; or<br>(ii) conviction on indictment to a fi ne not exceeding fi ve hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both. |
| **Article 4 – Data interference**<br>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.<br>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. | **Electronic Crimes Act (2013)**<br><br>**Part II. Offences**<br>**Section 3 (Access and interference)**<br>(1) A person shall not intentionally, without lawful excuse or justification,–<br>(i) willfully destroy, delete or alter information residing in an electronic system or diminish its value or utility, or affect it injuriously by any means; or<br>(2) A person who contravenes subsection (1) commits an offence and is liable on- |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (i) summary conviction to a fi ne not exceeding two hundred thousand dollars or<br>to imprisonment for a term not exceeding three years, or to both; or<br>(ii) conviction on indictment to a fi ne not exceeding fi ve hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both. |
| **Article 5 – System interference**<br>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 | **Electronic Crimes Act (2013)**<br><br>**Part II. Offences**<br>**Section 3 (Access and interference)**<br>(1) A person shall not intentionally, without lawful excuse or justification,–<br>(e) disrupt or causes disruption of an electronic system or network;<br>(f) deny or cause the denial of access to a person authorised to access an electronic system or network by any means;<br>(g) provide assistance to a person to facilitate access to an electronic system or network in contravention of the provisions of this Act;<br>(h) charge the services availed of by a person to the account of another person by tampering with or manipulating an electronic system or network;<br>(2) A person who contravenes subsection (1) commits an offence and is liable on-<br>(i) summary conviction to a fi ne not exceeding two hundred thousand dollars or<br>to imprisonment for a term not exceeding three years, or to both; or<br>(ii) conviction on indictment to a fi ne not exceeding fi ve hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both. |
| **Article 6 – Misuse of devices**<br>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:<br>a the production, sale, procurement for use, import, distribution or otherwise making available of:<br>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; | **Electronic Crimes Act (2013)**<br><br>**Part II. Offences**<br>**Section 9 (Misuse of encryption)**<br>(1) A person shall not intentionally, without lawful excuse or justification for the purpose of commission of an offence or concealment of incriminating evidence, intentionally encrypt any incriminating communication or data contained in an electronic system relating to the offence or incriminating evidence.<br>(2) A person who contravenes subsection (1) commits an offence and is liable on- |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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,<br>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and<br><br>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.<br><br>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.<br><br>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. | (a) summary conviction to a fi ne not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding two years, or to both; or<br>(b) on conviction on indictment to a fine not exceeding two hundred and fifty thousand dollars or to imprisonment for a term not exceeding five years, or to both.<br><br>**Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 8 (Amendment of section 9 – Misuse of encryption)**<br>Section 9 of the principal Act is amended in subsection (1) by repealing all the words appearing after "concealment" and replacing these with the following words:<br>"of evidence of any criminal matter, intentionally encrypt any communication or data contained in an electronic message or an electronic system. |
| | |
| **Article 7 – Computer-related forgery**<br>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. | **Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 5 (Amendment of section 6 – Electronic forgery)**<br>Section 6 of the principal Act is repealed and replaced as follows –<br>"6. Electronic forgery<br>(1) A person commits the offence of electronic forgery if that person with intent to defraud or deceive another –<br>(a) inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with intent that it be considered or acted upon as if it were authentic;<br>(b) creates, operates or presents a false website as the site of an established business entity with intent that it be considered or acted upon as if it were authentic; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (c) assumes a false identity in any electronic message or electronic mail for the purpose of gaining a benefit for himself or some other person; or<br>(d) posts or otherwise publishes any false document on any website with the intent that it be acted upon as if it were the real document.<br>(2) A person who is guilty of the offence of electronic forgery shall be liable on –<br>(a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding two years, or to both such fine and imprisonment; or<br>(b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both such fine and imprisonment.” |
| **Article 8 – Computer-related fraud**<br>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:<br><br>a any input, alteration, deletion or suppression of computer data;<br><br>b any interference with the functioning of a computer system,<br><br>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. | **Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 6 (Amendment of section 7 – Electronic fraud)**<br>Section 7 of the principal Act is repealed and replaced as follows –<br>“7. Electronic fraud<br>“(1) A person commits the offence of electronic fraud if that person intentionally and without lawful excuse, induces another person to enter into a relationship with intent to defraud that person or cause that other person to act to his own detriment, or suffer financial loss or loss of property, by –<br>(a) any input, alteration, deletion, or suppression of computer data; or<br>(b) any interference with the functioning of an electronic system.<br>(2) A person who is guilty of the offence of electronic fraud is liable on –<br>(a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding two years, or to both such fine and imprisonment; or<br>(b) conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding seven years, or to both such fine and imprisonment.” |
| | |
| **Article 9 – Offences related to child pornography**<br>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:<br>a producing child pornography for the purpose of its distribution through a computer system; | **Electronic Crimes Act (2013)**<br><br>**Part I. Preliminary**<br>In this Act –<br>“child pornography” means pornographic material that depicts, presents or represents-<br>(a) a child engaged in sexually explicit conduct; or |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| b offering or making available child pornography through a computer system;<br>c distributing or transmitting child pornography through a computer system;<br>d procuring child pornography through a computer system for oneself or for another person;<br>e possessing child pornography in a computer system or on a computer-data storage medium.<br><br>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:<br>a a minor engaged in sexually explicit conduct;<br>b a person appearing to be a minor engaged in sexually explicit conduct;<br>c realistic images representing a minor engaged in sexually explicit conduct<br><br>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.<br><br>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. | (b) an image representing a child engaged in sexually explicit conduct;<br><br>**Part II. Offences**<br>**Section 10 (Child Pornography)**<br>(1) For the purposes of this section a "child" means a person who is under the age of eighteen years.<br>(2) A person shall not intentionally without lawful justifi cation or excuse–<br>(a) publish, transmit or cause to be published or transmitted material in an electronic form which depicts a child engaged in a sexually explicit act or conduct;<br>(b) create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in an electronic form depicting a child in an obscene or indecent or sexually explicit manner;<br>(c) cultivate, entice or induce a child into an online relationship with another child or an adult for a sexually explicit act or in a manner that may offend a reasonable adult on an electronic system;<br>(d) facilitate the abuse of a child online;<br>(e) record or own in an electronic form material which depicts the abuse of a child engaged in a sexually explicit act;<br>(f) procure or obtain child pornography through a computer system; or<br>(g) obtain access through information and communication technologies, to child pornography.<br>(3) It is a defence to a charge of an offence under subsection (2) paragraphs (f) and (g) where the person can establish that the child pornography was for a bona fi de law enforcement purpose.<br>(4) A person who contravenes subsection (2) commits an offence and is liable on-<br>(a) summary conviction to a fi ne of three hundred thousand dollars or to three years imprisonment, or to both; or<br>(b) conviction on indictment to a fi ne not exceeding five hundred thousand dollars and to imprisonment for a term not exceeding twenty years or to both.<br>(5) Subsection (2) does not apply to a book, pamphlet, paper, drawing, painting, representation or figure or writing in an electronic form–<br>(a) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or<br>(b) which is kept or used for bona fi de heritage or religious purposes. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 10 – Offences related to infringements of copyright and related rights**<br>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.<br>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.<br>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. | **Copyright Act (2003)**<br><br>**Part V. Infringement of rights, General provisions**<br>**Section 31 (Acts infringing copyright)**<br>(1) The copyright in a work is infringed by any person who, without the licence of the copyright owner, does, in relation to that work, any of the acts which the copyright owner has the exclusive right to do pursuant to section 9.<br>(2) Copyright in a work is infringed by a person who, without the licence of the copyright owner, imports into Antigua and Barbuda for any purpose other than for his private and domestic use, an article which he knows or has reason to believe is, an infringing copy of the work.<br>(3) Copyright in a work is infringed by a person who, without the licence of the copyright owner -<br>(a) possesses in the course of a business;<br>(b) sells or lets for hire or offers or exposes for sale or hire;<br>(c) exhibits in public or distributes in the course of a business; or<br>(d) distributes otherwise than in the course of a business, to such an extent as to affect prejudicially the copyright owner, an article which is, and which be knows or has reason to believe is an infringing copy of the work.<br>(4) Copyright in a work is infringed by a person who, without the licence of the copyright owner -<br>(a) makes;<br>(b) imports into Antigua and Barbuda;<br>(c) possesses in the course of a business; or<br>(d) sells or lets for hire or offers for sale or hire, an article specifically designed or adapted for making copies of that work, knowing or having reason to believe that it is to be used to make infringing copies.<br>(6) Copyright in a work is infringed by a person who, without the licence of the copyright owner, transmits the work by means of a telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in Antigua and Barbuda or elsewhere.<br>(7) Where the copyright in a literary, dramatic or musical work is infringed by a performance at a place of public entertainment, any person who gave permission for that place to be used for the performance is also liable for the infringement unless when he gave permission he believed on reasonable grounds that the performance would not infringe copyright. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (8) Where copyright in a work is infringed by a public performance of the work or by the playing or showing of the work in public by means of apparatus for playing sound recordings or showing films or receiving visual images or sounds conveyed by electronic means, the persons specified in subsection (8) are also liable for the infringement.<br>(9) The persons referred to in subsection (7) are -<br>(a) persons who supplied the apparatus or any substantial part of it, if when he supplied the apparatus or part -<br>(i) he knew or had reason to believe that the apparatus was likely to be so used as to infringe copyright; or<br>(ii) in the case of apparatus whose normal use involves a public performance, playing or showing, he did not believe on reasonable grounds that it would not be so used as to infringe copyright;<br>(b) an occupier of premises who gave permission for the apparatus to be brought onto the premises, if when he gave permission he knew or had reason to believe<br>that the apparatus was likely to be so used as to infringe copyright; and<br>(c) a person who supplied a copy of a sound recording or film used to infringe copyright, if when he supplied it he knew or had reason to believe that what he supplied or a copy made directly or indirectly from it, was likely to be so used as to infringe copyright. |
| | |
| **Article 11 – Attempt and aiding or abetting**<br>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.<br>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.<br>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 12 – Corporate liability**<br>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:<br>a a power of representation of the legal person;<br>b an authority to take decisions on behalf of the legal person;<br>c an authority to exercise control within the legal person.<br>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.<br>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.<br>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. | |
| **Article 13 – Sanctions and measures**<br>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.<br>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. | Each offence in the Electronic Crimes Act (2013) contains sanctions including deprivation of liberty and monetary sanctions.<br><br>**Electronic Crimes Act (2013)**<br><br>**Part IV Miscellaneous**<br>**29. Order for compensation**<br>(1) A Court before which a person is convicted of an offence under this Act may make an order against that person for the payment by that person of a sum of money fixed by the Court by way of compensation to a person for damage caused to his or her electronic system, program or data by the offence in respect of which the sentence is passed.<br>(2) A claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him or her under an order for compensation, except that the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) An order for compensation under this section shall be recoverable as a civil debt. |
| | |
| **Article 14 – Scope of procedural provisions**<br>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.<br>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:<br>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;<br>b other criminal offences committed by means of a computer system; and<br>c the collection of evidence in electronic form of a criminal offence.<br>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.<br>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:<br>i is being operated for the benefit of a closed group of users, and<br>ii does not employ public communications networks and is not connected with another computer system, whether public or private,<br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 15 – Conditions and safeguards**<br>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.<br>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.<br><br>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. | **Constitution of Antigua and Barbuda (1981)**<br><br>**Chapter II. Protection of Fundamental Rights and Freedoms of the Individual**<br>**Section 4 (Protection of right to life)**<br>(1) No person shall be deprived of his life intentionally save in execution of the sentence of a court in respect of a crime of treason or murder of which he has been convicted.<br>(2) A person shall not be regarded as having been deprived of his life in contravention of this section if he dies as the result of the use, to such extent and such circumstances as are permitted by law, of such force as is reasonably justifiable -<br>(a) for the defence of any person from violence or for the defence of property;<br>(b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained;<br>(c) for the purpose of suppressing a riot, insurrection or mutiny; or<br>(d) in order lawfully to prevent the commission by that person of a criminal offence,<br>or if he dies as the result of a lawful act of war.<br><br>**Section 9 (Protection from deprivation of property)**<br>(1) No property of any description shall be compulsorily taken possession of, and no interest in or right to or over property of any description shall be compulsorily acquired, except for public use and except in accordance with the provisions of a law applicable to that taking of possession or acquisition and for the payment of fair compensation within a reasonable time.<br>(4) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of subsection (1) of this section –<br>(a) to the extent that the law in question makes provision for the taking of possession or acquisition of any property, interest or right<br>(i) in satisfaction of any tax, rate or due;<br>(ii) by way of penalty for breach of the law or forfeiture in consequence of breach of the law;<br>(iii) as an incident of a lease, tenancy, mortgage, charge, bill of sale, pledge or<br>contract; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| | (iv) in the execution of judgements or orders of a court in proceedings for the determination of civil rights or obligations;<br>(v) in circumstances where it is reasonably necessary so to do because the property is in a dangerous state or likely to be injurious to the health of human beings, animals or plants;<br>(vi) in consequence of any law with respect to the limitation of actions;<br>(vii) for so long as may be necessary for the purposes of any examination, investigation, trial or enquiry or, in the case of land, for the purposes of the carrying out thereon of work of soil conservation or the conservation of other natural resources or work relation to agricultural development or improvement (being work relating to such development or improvement that the owner or occupier of the land has been required, and has without reasonable excuse refused or failed, to carry out),<br>and except so far as the provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society;<br>(b) to the extent that the law in question makes provision for the taking of possession or acquisition of any of the following property (including and interest in or right to or over property), that is to say –<br>(i) enemy property;<br>(ii) property of a deceased person, a person of unsound mind or a person who had not attained the age of eighteen years, for the purpose of its administration for the benefit of the persons entitled to the beneficial interest therein;<br>(iii) the property of a person adjudged bankrupt or a body corporate in liquidation, for the purpose of its administration for the benefit of the creditors of the bankrupt or body corporate and, subject thereto, for the benefit of other persons entitled to the beneficial interest in the property; or<br>(iv) property subject to a trust, for the purpose of vesting the property in persons appointed as trustees under the instrument creating the trust or by a court or by order of a court for the purposes of giving effect to the trust. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | **Section 10 (Protection of person or property from arbitrary search of entry)**<br>(1) Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on his premises.<br>(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision –<br>(a) that is reasonably required in the interests of defence, public safety, public order, public morality, public health, public revenue, town and country planning or the development and utilisation of property in such a manner as to promote the public benefit;<br>(b) that authorises an office or agent of the Government, a local government authority or a body corporate established by law for public purposes to enter on the premises of any person in order to inspect those premises or anything thereon for the purpose of any tax, rate or due in order to carry out work connected with any property that is lawfully on those premises and that belongs to the Government, or to that authority or body corporate, as the case may be;<br>(c) that is reasonably required for the purpose of preventing or detecting crime;<br>(d) that is reasonably required for the purpose of protecting the rights or freedoms of other persons; or<br>(e) that authorises, for the purpose of enforcing the judgement or order of a court in any proceedings, the search of any person or property by order of a court or entry upon any premises by such order,<br>- and except so far as that provision or, as the case may be, anything done under the authority thereof is shown not to be reasonably justifiable in a democratic society.<br><br>**Section 15 (Provision to secure protection of the law)**<br>(1) If any person is charged with a criminal offence then, unless the charge is withdrawn, he shall be afforded a fair hearing within a reasonable time by a independent and impartial court established by law.<br>(2) Every person who is charged with a criminal offence –<br>(a) shall be presumed to be innocent until he is proved or has pleaded guilty; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (b) shall be informed orally and in writing as soon as reasonably practicable, in language that he understands, of the nature of the offence with which he is charged;<br>(c) shall be given adequate time and facilities for the preparation of his defence;<br>(d) shall be permitted to defend himself before the court in person or by a legal practitioner of his own choice;<br>(e) shall be afforded facilities to examine in person or by his legal representative the witnesses called by the prosecution before the court and to obtain the attendance and carry out the examination of witnesses to testify on his behalf before the court on the same conditions as those applying to witnesses called by the prosecution; and<br>(f) shall be permitted to have without payment the assistance of an interpreter if he cannot understand the language used at the trial of the charge, and except with his own consent the trial shall not take place in his absence –<br>(i) except where, under the provisions of any law entitling him thereto, he is given adequate notice of the charge, the date, time and place of the trial or continuance thereof and afforded a reasonable opportunity of appearing before the court;<br>Provided that where the foregoing conditions have been complied with, and the court is satisfied that owing to circumstances beyond his control he cannot appear, the trial shall not take place or continue in his absence; or<br>(ii) unless he so conducts himself as to render the continuance of the proceedings in his presence impracticable and the court has ordered him to be removed and the trial to proceed in his absence.<br>(3) When a person is tried for any criminal offence the accused person or any person authorised by him in that behalf shall, if he so requires and subject to payment of such reasonable fees as may be prescribed by law, be given within a reasonable time after judgement a copy of any record of the proceedings made by or on behalf of the court.<br>(4) No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence that is more severe in degree or description than the maximum penalty that might have been imposed for that offence at the time when it was committed. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (5) No person who shows that he has been tried by a competent court for a criminal offence and either convicted or acquitted shall again be tried for that offence or for any criminal offence of which he could have been convicted at the trial for the offence, save upon the order of a superior court in the course of appeal or review proceedings relating to the conviction or acquittal.<br>(6) No person shall be tried for a criminal offence if he shows that he has been pardoned for that offence.<br>(7) No person who is tried for a criminal offence shall be compelled to give evidence at the trial.<br>(8) Any court or other authority prescribed by law for the determination of the existence or extent of any civil right or obligation shall be established by law and shall be independent and impartial; and where proceedings for such a determination are instituted by any persons before such a court or other authority, the case shall be given a fair hearing within a reasonable time.<br>(9) Except with the agreement of all that parties thereto, all proceedings of every court and proceedings for the determination of the existence or extent of any civil right or obligation before any other authority, including the announcement of the decision of the court or other authority, shall be held in public.<br>(10) Nothing in subsection (9) of this section shall prevent the court or other authority from excluding from the proceedings persons other than the parties thereto and the legal practitioners representing them to such an extent as the court or other authority –<br>(a) may by law be empowered to do and may consider necessary or expedient in circumstances where publicity would prejudice the interests of justice or in interlocutory proceedings or in the interests of public morality, the welfare of persons under the age of eighteen years or the protection of the private lives of persons concerned in the proceedings; or<br>(b) may by law be empowered or required to do in the interests of defence, public safety, public order or public morality.<br>(11) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of –<br>(a) subsection (2) (a) of this section, to the extent that the law in question imposes upon any person charged with a criminal offence the burden of proving particular facts;<br>(b) subsection (2) (e) if this section, to the extent that the law in question imposes reasonable conditions that must be satisfied if witnesses called |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | to testify on behalf of an accused person are to be paid their expenses out of public funds; or<br>(c) subsection (5) of this section, to the extent that the law in question authorises a court to try a member of a disciplined force for a criminal offence notwithstanding any trial and conviction or acquittal of that member under the disciplinary law of that force so however, that any court so trying such a member and convicting him shall in sentencing him to any punishment take into account any punishment awarded him under that disciplinary law.<br>(12) In the case of any person who is held in lawful detention, the provisions of subsection (1), paragraphs (d) and (e) of subsection (2), and subsection (3) of this section shall not apply in relation to his trial for a criminal offence under the law regulating the discipline of persons held in such detention.<br>(13) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of subsection (2) of this section to the extent that it authorises the trial of a defendant by a magistrate for a summary offence to take place in the defendant's absence. |
| **Article 16 – Expedited preservation of stored computer data**<br>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.<br><br>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.<br><br>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 | **Electronic Crimes Act (2013)**<br><br>**Part III. Investigations and Procedures**<br>**Section 16 (Preservation order)**<br>(1) A police officer may apply to a Magistrate/Judge in Chambers for an Order for the expeditious preservation of data that has been stored or processed by means of an electronic system, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence.<br>(2) For the purposes of subsection (1), data includes traffic data and subscriber information.<br>(3) An Order made under subsection (1) remains in force–<br>(a) until such time as may be reasonably be required for the investigation of an offence;<br>(b) where prosecution is instituted, until the fi nal determination of the case; or<br>(c) until such time as the Magistrate/Judge in Chambers determines necessary. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.<br><br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 17 – Expedited preservation and partial disclosure of traffic data**<br>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:<br>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<br>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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | **Electronic Crimes Act (2013)**<br><br>**Part III. Investigations and Procedures**<br>**Section 17 (Disclosure of preserved data order)**<br>A police officer may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a Magistrate/Judge in Chambers for an Order for the disclosure of–<br>(a) any preserved data, irrespective of whether one or more service providers were involved in the transmission of the data;<br>(b) sufficient data to identify the service providers and the path through which the data was transmitted; or<br>(c) the electronic key enabling access to or the interpretation of data. |
| **Article 18 – Production order**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:<br>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<br>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.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.<br>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: | **Electronic Crimes Act (2013)**<br><br>**Part III. Investigations and Procedures**<br>**Section 18 (Production order)**<br>(1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer may apply to a Magistrate/Judge in Chambers for an Order compelling–<br>(2) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer shall make a request of–<br>(a) a person to submit specified data in that person's possession or control, which is stored in an electronic system;<br>(b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control.<br>(3) Where any material to which an investigation relates consists of data stored in an electronic system, disc, cassette, or on microfilm or preserved by any mechanical or electronic device, the request shall be deemed to require the person |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a the type of communication service used, the technical provisions taken thereto and the period of service;<br>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;<br>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | to produce or give access to it in a form in which it can be taken away and in which it is visible, audible or legible.<br>(4) A person or service provider who refuses to produce the information under subsection (1) commits an offence and is liable on summary conviction to a fi ne<br><br>**Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 9 (Amendment of section 18 – Production order)**<br>Section 18 of the principal Act is amended –<br>(a) in subsection (1) –<br>(i) by repealing the words "may apply" and replacing these with the words "shall apply"; and<br>(ii) by inserting immediately after the words "compelling -" the following –<br>"(a) a person to submit specified data in that person's possession or control, which is stored in an electronic system;<br>(b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control."<br>(b) by repealing subsection (2) in its entirety; and<br>(c) by renumbering subsection (3) as subsection (2), and subsection (4) as subsection (3). |
| **Article 19 – Search and seizure of stored computer data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:<br>a a computer system or part of it and computer data stored therein; and<br>b a computer-data storage medium in which computer data may be stored<br>in its territory.<br>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. | **Electronic Crimes Act (2013)**<br><br>**Part III. Investigations and Procedures**<br>**Section 19 (Powers of access, search and seizure for the purpose of investigation)**<br>(1) Where a police officer has reason to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a Magistrate/Judge in Chambers for the issue of a warrant to enter any premises to access, search and seize that data.<br>(2) In the execution of a warrant under subsection (1), the powers of the police officer shall include the power to–<br>(a) access, inspect and check the operation of an electronic system;<br>(b) use or cause to be used an electronic system to search any data contained in or available to the electronic system;<br>(c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or available to |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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:<br>a seize or similarly secure a computer system or part of it or a computer-data storage medium;<br>b make and retain a copy of those computer data;<br>c maintain the integrity of the relevant stored computer data;<br>d render inaccessible or remove those computer data in the accessed computer system.<br>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.<br>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | an electronic system into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section;<br>(d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for required for the purpose of investigating the offence;<br>(e) seize or secure an electronic system.<br>(3) A person shall not intentionally, without lawful excuse or justification –<br>(a) obstruct a police officer in the exercise of the police officer's powers under this section; or<br>(b) fail to comply with a request made by a police officer under this section.<br>(4) A person who contravenes subsection (3) commits a summary offence and is liable on conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding twelve months, or both.<br>(5) For the purposes of this section–<br>"decryption information" means information or technology that enables a person to readily re-transform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;<br>"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable and incomprehensible format, regardless of the technique utilized for transformation or scrambling, and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; and<br>"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.<br><br>**Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 10 (Amendment of section 19(1) and 20 of the principal Act)**<br>The principal Act is amended in sections 19(1) and section 20 by repealing the words "may apply" and replacing these with the words "shall apply". |
| **Article 20 – Real-time collection of traffic data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:<br>a collect or record through the application of technical means on the territory of that Party, and | **Electronic Crimes Act (2013)**<br><br>**Part III. Investigations and Procedures**<br>**Section 20 (Real time collection of traffic data)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party; or<br>ii to co-operate and assist the competent authorities in the collection or recording of,<br>traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.<br>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.<br>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.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | Where a police officer has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence under this Act, the police officer may apply to a Magistrate/Judge in Chambers for an Order–<br>(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of an electronic system; or<br>(b) compelling a service provider, within its technical capabilities to effect such collection and recording referred to in paragraph (a) or assist the police officer to effect such collection and recording.<br><br>**Electronic Crimes (Amendment) Act (2018)**<br><br>**Section 10 (Amendment of section 19(1) and 20 of the principal Act)**<br>The principal Act is amended in sections 19(1) and section 20 by repealing the words "may apply" and replacing these with the words "shall apply". |
| **Article 21 – Interception of content data**<br>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:<br>a collect or record through the application of technical means on the territory of that Party, and<br>b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party, or<br>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.<br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| collection or recording of content data on specified communications in its territory through the application of technical means on that territory.<br>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.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| | |
| **Article 22 – Jurisdiction**<br>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:<br>a in its territory; or<br>b on board a ship flying the flag of that Party; or<br>c on board an aircraft registered under the laws of that Party; or<br>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.<br>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.<br>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.<br>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.<br>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. | |
| | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 24 – Extradition**<br>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.<br><br>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.<br>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.<br>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.<br>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.<br>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.<br>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. | **Electronic Crimes Act (2013)**<br><br>**Part IV Miscellaneous**<br>**28. Extraditable offences**<br>An offence pursuant to Part II shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act 1993. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.<br><br>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**<br>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.<br><br>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.<br><br>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.<br><br>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.<br><br>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 | **Mutual Assistance in Criminal Matters Act (1993) (only for Commonwealth countries)**<br><br>**Part II. Request by Antigua and Barbuda to Commonwealth countries for Assistance, Division 1. – General Assistance**<br>**Section 7 (Assistance in obtaining evidence, etc.)**<br>Where there are reasonable grounds to believe that evidence Assistance in or information relevant to any criminal matter may be obtained in if, in a Commonwealth country -<br>(a) evidence is taken from any person;<br>(b) information is provided;<br>(i) person;<br>(ii) sample, specimen or other item from, or provided by, a person; or<br>(iii) remains which are, or may be, human, is or are subjected to any examination or test;<br>(d) judicial records or official records are produced, copied or examined;<br>(e) any record or article is produced, copied or examined;<br>(f) samples of any matter or thing are taken, examined or tested; or<br>(g) any building, place or thing is viewed or photographed,<br>a request may be transmitted requesting that assistance be given by the country in so obtaining the evidence or information.<br><br>**Part III. Requests by Commonwealth countries to Antigua and Barbuda for assistance, Division 1. – Form and acceptance or refusal of requests**<br>**Section 19 (Acceptance or refusal of requests, etc.)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. | (1) Subject to this section, a request for assistance under Acceptance or this Act duly made by a Commonwealth country shall be accepted.<br><br>**Mutual Assistance in Criminal Matters (Amendment) Act (2020)**<br><br>**Part IV. Application of acts to countries other than Commonwealth countries**<br>**Section 30B (Request for assistance)**<br>(1) A request by Antigua and Barbuda for assistance under this Part shall be made by the Attorney General.<br>(2) Every request to Antigua and Barbuda for assistance in criminal matters under this Part shall be made by the appropriate authority of a foreign country to the Attorney General or to a person authorised by the Attorney General in writing to receive the request.<br>(3) If a foreign country requests assistance under this Part, the Attorney General must consider the following matters before deciding whether the request must be dealt with under this Part:<br>(a) any assurance given by that country that it will entertain a similar request by Antigua and Barbuda for assistance in criminal matters;<br>(b) the seriousness of the offence to which the request relates;<br>(4) In addition to the matters referred to in subsection (3), the Attorney General must also consider whether the request is in relation to assistance concerning the following matter—<br>(a) the identification and location of persons charged with offences, or suspected on reasonable grounds, to have committed such offences;<br>(b) the obtaining of evidence, documents, or other articles;<br>(b) the production of documents and articles;<br>(d) the making of arrangements for persons to give evidence or assist in investigation;<br>(e) the service of documents<br>(f) the execution of a request for search and seizure; and<br>(g) the forfeiture of-<br>(i) tainted property; and<br>(ii) property of persons who have unlawfully benefited from criminal activity and<br>(iii) instrument of crime, and |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (iv) property that will satisfy all or part of a foreign pecuniary penalty order,<br>(h) the location of property that may be forfeited;<br>(i) the recovery of property to satisfy foreign pecuniary penalty orders,<br>(j) the restraining of dealing with property or the freezing of assets, that may be forfeited" |
| **Article 26 – Spontaneous information**<br>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.<br><br>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. | |
| **Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**<br>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.<br>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.<br>b The central authorities shall communicate directly with each other; | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| 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;<br>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.<br>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.<br>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.<br>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.<br>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.<br>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.<br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).<br>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.<br>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.<br>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**<br>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.<br>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:<br>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or<br>b not used for investigations or proceedings other than those stated in the request.<br>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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **Article 29 – Expedited preservation of stored computer data**<br>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.<br>2 A request for preservation made under paragraph 1 shall specify:<br>a the authority seeking the preservation;<br>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;<br>c the stored computer data to be preserved and its relationship to the offence;<br>d any available information identifying the custodian of the stored computer data or the location of the computer system;<br>e the necessity of the preservation; and<br>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.<br>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.<br>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.<br>5 In addition, a request for preservation may only be refused if: | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>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.<br>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**<br>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.<br>2 Disclosure of traffic data under paragraph 1 may only be withheld if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or<br>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**<br>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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.<br>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.<br>3 The request shall be responded to on an expedited basis where:<br>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or<br>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation. | |
| **Article 32 – Trans-border access to stored computer data with consent or where publicly available**<br>A Party may, without the authorisation of another Party:<br>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or<br>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. | |
| **Article 33 – Mutual assistance in the real-time collection of traffic data**<br>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.<br>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**<br>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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 35 – 24/7 Network**<br>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:<br>a the provision of technical advice;<br>b the preservation of data pursuant to Articles 29 and 30;<br>c the collection of evidence, the provision of legal information, and locating of suspects.<br>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.<br><br>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.<br><br>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network. | |
| **Article 42 – Reservations**<br>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