# [SAMOA]

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version [30 March 2020]*

[reference to the provisions of the Budapest Convention]


**Chapter I – Use of terms**

Article 1 – "Computer system", "computer data", "service provider", "traffic data"

**Chapter II – Measures to be taken at the national level**

Section 1 – Substantive criminal law

Article 2 – Illegal access
Article 3 – Illegal interception
Article 4 – Data interference
Article 5 – System interference
Article 6 – Misuse of devices
Article 7 – Computer-related forgery
Article 8 – Computer-related fraud
Article 9 – Offences related to child pornography
Article 10 – Offences related to infringements of copyright and related rights
Article 11 – Attempt and aiding or abetting
Article 12 – Corporate liability
Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions
Article 15 – Conditions and safeguards
Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data
Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

**Chapter III – International co-operation**

Article 24 – Extradition
Article 25 – General principles relating to mutual assistance
Article 26 – Spontaneous information
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
Article 28 – Confidentiality and limitation on use
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 – Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance in the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network


*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; | **CA 205. Interpretation** "electronic system" includes the following and any part of the following:<br>(a) a device or a group of inter-connected or related devices 1 or more of which, pursuant to a program, performs automatic processing of data or any other function;<br>***(b) a computer;***<br>(c) two or more interconnected electronic systems;<br>(d) any communication links between electronic systems or to remote terminals or another device;<br>(e) two or more interconnected electronic systems combined with any communication links between computers or to remote terminals or any other device;<br><br>"device" **includes the following:**<br>(a) components of electronic systems such as computer, mobile phones, graphic cards, memory, chips;<br>(b) storage components such as hard drives, memory cards, compact discs, tapes;<br>(c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;<br>(d) output devices such as printer, screens; |
| 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; | **CA 205. Interpretation**<br>"electronic data" means any representation of facts, concepts, information (either texts, sounds or images), or machine readable code or instructions, in a form suitable for processing in an electronic system, including a program suitable to cause an electronic system to perform a function; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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; | **TA 2. Interpretation**<br>"service provider" means a person that provides a telecommunications service to the public or that owns or operates a telecommunications network used to provide telecommunications services to the public;<br><br>**12. Requirement to hold licence –**<br>(1) A person shall not:<br>(a) provide a telecommunications service to the public for direct or indirect compensation; or<br>(b) own or operate a telecommunications network used to provide a telecommunications service to the public for direct or indirect compensation, - except under a license or an exemption order. |
| 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 | |
| **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**<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 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. | **CA 205. Interpretation**<br>"access", in relation to an electronic system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the electronic system;<br><br>**CA 206. Accessing electronic system without authorisation –**<br>(1) A person is liable to imprisonment for a term not exceeding 7 years who intentionally accesses, **directly or indirectly**, an electronic system without **authorisation**, or being reckless as to whether the person is authorised to access the electronic system.<br>(2) This section does not apply if:<br>(a) a person who is authorised to access an electronic system accesses the electronic system for a purpose other than the one for which that person was given access; and |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (b) access to an electronic system is gained by a law enforcement agency—<br>(i) under a warrant; or<br>(ii) under the authority of any Act or rule of the common law.<br><br>**CA 207. Accessing electronic system for dishonest purpose –**<br>(1) A person is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly:<br>(a) accesses an electronic system and in so doing, dishonestly or by deception—<br>(i) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or<br>(ii) causes loss to any other person; or<br>(b) attempts to access an electronic system, dishonestly or by deception—<br>(i) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or<br>(ii) to cause loss to any other person.<br>(2) In this section, "deception" has the same meaning as in<br>section 172(2).<br>(3) This section does not apply if:<br>(a) a person who is authorised to access an electronic system accesses the electronic system for a purpose other than the one for which that person was given access; and<br>(b) access to an electronic system is gained by a law enforcement agency—<br>(i) under a warrant; or<br>(ii) under the authority of any Act or rule of the common law.<br><br>**CA 208. Illegal remaining in an electronic system –**<br>(1) A person is liable to imprisonment for a period not exceeding 7 years who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification:<br>(a) logs into and remains logged in an electronic system; or<br>(b) accesses and continues to remain in access to an electronic system.<br>(2) This section does not apply if:<br>(a) a person who is authorised to access an electronic system accesses the electronic system for a purpose other than the one for which that person was |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | given access; and<br>(b) access to an electronic system is gained by a law enforcement agency—<br>(i) under a warrant; or<br>(ii) under the authority of any Act or rule of the common law. |
| **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. | **CA 205. Interpretation**<br>"intercept" includes to acquire, **view** and capture any electronic data or communication **whether by wire, wireless, electronic, optical, magnetic, oral, or other means**, during transmission through the use of any **technical device**.<br><br>**CA 209. Illegal interception –** A person is liable to imprisonment for a term not exceeding 7 years who intentionally, **without right** and with dishonest or otherwise **unlawful intent**, intercept or attempt to intercept:<br>(a) a transmission **not intended for public reception** of electronic data to, from or within an electronic system; or<br>(b) electromagnetic emissions from an electronic system. |
| **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. | **CA 210. Damaging or interfering with electronic data –**<br>A person is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly and without **authorisation**, or being reckless as to whether or not he or she is authorised:<br>(a) damages or deteriorates electronic data; or<br>(b) deletes electronic data; or<br>(c) alters electronic data; or<br>(d) renders electronic data meaningless, useless or ineffective; or<br>**(e) obstructs, interrupts or interferes with the lawful use of electronic data; or**<br>**(f) obstructs, interrupts or interferes with any person in the lawful use of electronic data; or**<br>(g) denies access to electronic data to any person authorised to access it. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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 | **CA 205. Interpretation**<br>"hinder", in relation to an electronic system, includes the following:<br>**(a) cutting the electricity supply to an electronic system;**<br>**(b) causing electromagnetic interference to an electronic system;**<br>**(c) corrupting an electronic system by any means; and**<br>(d) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data;<br><br>**CA 212. Illegal system interference –**<br>(1) A person is liable to imprisonment for a term not exceeding 7 years who intentionally and **without authorisation** hinders or interferes:<br>(a) with the functioning of an electronic system if he or she knows or ought to know that **danger to life** is likely to result; or<br>(b) with a person who is lawfully using or operating an electronic system if he or she knows or ought to know that **danger to life** is likely to result; or<br>(c) with an electronic system that is **exclusively** for the use of **critical infrastructure operations**, or in the case in which such is not **exclusively** for the use of **critical infrastructure operations**, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure.<br>(2) In subsection (1)(c), "critical infrastructure" means electronic systems, devices, networks, electronic programs, and electronic data, that are so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters. |
| **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; | **CA 213. Illegal devices –**<br>A person is liable to imprisonment for a term not exceeding 7 years who intentionally and **without authorisation** produces, sells, procures for use, imports, distributes or otherwise makes available, or attempts to use, possess, produce, sell, procure for use, import, distribute or otherwise make available:<br>(a) a device, including an electronic program, that is designed or adapted for the purpose of committing an offence; or<br>(b) a password, access code or similar data by which the whole or any part of an electronic system is capable of being accessed |

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. | **with the intent that it be used by the person or another person for the purpose of committing an offence.**<br><br>**CA 214. Making, selling, distributing or possessing software for committing a crime –**<br>(1) A person is liable to imprisonment for a term not exceeding 7 years who does any of the following with the sole or principal use of which the person knows to be the commission of a crime, knowing or being reckless as to whether it will be used for the commission of a crime:<br>(a) invites another person to acquire from the person any software or other electronic information that would enable the other person to **access** an electronic system without authorisation;<br>(b) offers or exposes for sale or supply to another person any software or other electronic information that would enable the other person to **access** an electronic system without authorisation;<br>(c) agrees to sell or supply to another person any software or other electronic information that would enable the other person to **access** an electronic system without authorisation;<br>(d) sells or supplies to another person any software or other electronic information that would enable the other person to **access** an electronic system without authorisation;<br>(e) has in his or her possession for the purpose of sale or supply to another person any software or other electronic information that would enable the other person to **access** an electronic system without authorisation.<br>(2) A person is liable to imprisonment for a term not exceeding 7 years who:<br>(a) has in his or her possession any software or other electronic information that would enable him or her to **access** an electronic system without authorisation; and<br>(b) intends to use that software or other electronic information to commit a crime. |
| **Title 2 – Computer-related offences** | |
| **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 | **CA 216. Forgery of electronic data –**<br>A person is liable to imprisonment for a term not exceeding 7 years who intentionally and **without authorisation**, inputs, alters, deletes, or suppresses |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. | electronic data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. |
| **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. | **CA 215. Identity fraud –**<br>(1) A person commits an offence and is liable to imprisonment for a term not exceeding 5 years who knowingly obtains, transfers or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an offence that includes fraud, deceit, or falsehood as an element of the offence.<br>(2) A person commits an offence and is liable to imprisonment for a term not exceeding 10 years who dishonestly or fraudulently personates another person, living or dead:<br>(a) with intent to gain advantage for himself, herself or another person; or<br>(b) with intent to obtain any property or an interest in any property; or<br>(c) with intent to cause disadvantage to the person being personated or another person; or<br>(d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.<br>(3) A person is liable to imprisonment for a period not exceeding 7 years who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, by using an electronic system in any stage of the offence, transfers, possesses, or uses a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime.<br>(4) A person is liable to imprisonment for a term not exceeding 7 years who intentionally, without authorisation and with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, causes a loss of property to another person by:<br>(a) any input, alteration, deletion or suppression of electronic data; or<br>(b) any interference with the functioning of an electronic system. |
| **Title 3 – Content-related offences** | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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;<br>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. | **CA 82. Publication, distribution or exhibition of indecent material on child –**<br>(1) A person is liable to imprisonment for a term not exceeding 7 years who without lawful justification who does any of the following:<br>(a) sells, or delivers by way of hire, or has in his or her possession for sale or hire, or otherwise distributes in public any indecent material on a child;<br>(b) exhibits or presents in or within view of any place to which the public have or are permitted to have access any indecent material on a child;<br>(c) exhibits or presents in the presence of any person in consideration or expectation of any payment, or otherwise for gain, any indecent material on a child;<br>(d) prints or causes to be printed any indecent material on a child;<br>(e) knowingly has in possession or publishes any indecent material on a child;<br>(f) creates, draws, affixes, impresses, or exhibits, or causes to be created, drawn, affixed, impressed or exhibited, any indecent material on a child;<br>(g) communicate, exhibit, send, supply or transmit any indecent material on a child to another person, whether to a particular person or not;<br>(h) make an indecent material on a child available to access to any other person, whether by a particular person or not;<br>(i) produces indecent material for the purpose of its distribution through an electronic system;<br><br>(3) It is a defence to a charge of an offence under subsection (1)(i) to (n) if the person establishes that the indecent material was stored for a bona fide law enforcement purpose and if so, the indecent material must be deleted as soon as it is not legally required anymore.<br><br>(4) A person shall not be prosecuted for an offence against this section without the leave in writing of the Director of Public Prosecutions, who before giving leave may make such inquiries as the Director of Public Prosecutions thinks fit.<br><br>(5) It is no defence that the person charged under this section did not know that the document to which the charge relates was indecent, unless that person satisfies the Court:<br>(a) that the person had no reasonable opportunity of knowing it; and<br>(b) that in the circumstances the person's ignorance was excusable.<br>(6) This section does not apply to any document or matter to which the Indecent Publications Ordinance 1960 relates, whether the document or matter is indecent within the meaning of that Ordinance or not. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | **CA 205. Interpretation**<br>"child pornography":<br>(a) means pornographic material that depicts, presents or represents—<br>(i) a child engaged in sexually explicit conduct; or<br>(ii) a person appearing to be a child engaged in sexually explicit conduct; or<br>(iii) images representing a child engaged in sexually explicit conduct; and<br>(b) includes any audio, visual or text pornographic material;<br><br>"child" means a person 16 years and under;<br><br>"indecent material" means any book, newspaper, picture, film, photograph, child pornography, print, or writing, and any paper or other thing of any description whatsoever, which has printed or impressed upon it, or otherwise attached thereto, or appearing, shown, or exhibited in any manner whatsoever thereon, any indecent picture, illustration, or representation, or which unduly emphasises matters of sex, horror, crime, cruelty, or violence; |
| **Title 4 – Offences related to infringements of copyright and related rights** | |
| **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 | **CRA 2. Interpretation**<br>"**Computer**" means an electronic or similar device having information-processing capabilities; and a "computer program" is a set of instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a medium that the computer can read, or causing a computer to perform or achieve a particular task or result:<br>**3. Works protected**<br>(1) Literary and artistic works (herein-after referred to as "works") are original intellectual creations in the literary and artistic domain, including in particular -<br>(1) Literary and artistic works (herein-after referred to as "works") are original intellectual creations in the literary and artistic domain, including in particular -<br>(a) Books, pamphlets, articles, **computer programs** and other writings;<br>**13. Reproduction and adaptation of computer programs** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (1) Notwithstanding section 6(1)(a) and (c), the reproduction, in a single copy, or the adaptation of a computer program by the lawful owner of a copy of that computer program shall be permitted without the authorization of the author or other owner of copyright, provided that the copy or adaptation is necessary -<br>(a) For use of the computer program with a computer for the purpose and extent for which the computer program has been obtained;<br>(b) For archival purposes and for the replacement of the lawfully owned copy of the computer program in the event that the said copy of the computer program is lost, destroyed or rendered unusable.<br><br>27. Criminal sanctions<br>(1) Any infringement of a right protected under this Act, if committed wilfully or by gross negligence and for profit-making purposes, shall be punished by a maximum fine of not exceeding 250 penalty units where the offence involves the breach of a copyright relating to a computer or computer program, and in every other case, or to imprisonment for a term not exceeding five years or both. The amount of the fine shall be fixed by the court, taking into particular account the defendant's profits attributable to the infringement. |
| **Title 5 – Ancillary liability and sanctions** | |
| **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. | **CA 33. Parties to offences –**<br>(1) A person is a party to and guilty of an offence who:<br>(a) actually commits the offence; or<br>(b) does or omits an act for the purpose of aiding any person to commit the offence; or<br>(c) abets any person in the commission of the offence; or<br>(d) incites, counsels, or procures any person to commit the offence.<br>(2) Where 2 or more persons form a common intention tocarry into effect any unlawful purpose and to assist each other in that object, each of them is a party to every offence committed by any one of them in carrying into effect that unlawful purpose if the commission of that offence was or ought to have been known to be a probable consequence of carrying into effect that common purpose. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) Nothing in this section prevents the charging of a person as a party to any offence under both subsections (1) and (2) or in the alternative. |
| **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. | |
| ***Section 2 – Procedural law*** | |
| **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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 | |
| **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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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 computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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:<br>a the type of communication service used, the technical provisions taken thereto and the period of service; | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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.<br>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, | **CPA 33. Search and seize warrants –**<br>(1) This section applies whether or not any information has been laid.<br>(2) A Judge or Registrar may issue a search and seize warrant, or a restraining order, in the prescribed form, if he or she is satisfied on the oath of any person that there is reasonable ground or good cause for believing that there is in any building, aircraft, ship, vehicle, box, receptacle, premises, or place, or on any person:<br>(a) anything upon or for which an offence punishable by imprisonment has been or is suspected of having been committed; or<br>(b) anything which, there is reasonable ground to believe, will be evidence for the offence; or<br>(c) anything which there is reasonable ground to believe is intended to be used for the purposes of committing the offence.<br>(3) A restraining order may prohibit the defendant or any other person from disposing of, or otherwise dealing with, the property or part of or interest in it, as is specified in the order, either absolutely or except in any manner specified in the order.<br>(4) In this section, "Registrar" does not include a Deputy Registrar. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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<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,<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. | |
| **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 | **PPA 3. Application for a surveillance warrant–**<br>(1) An application may be made in accordance with this section to a Judge for a warrant for any member of the police to:<br>(a) intercept a private communication by means of an interception device; or<br>(2) An application under subsection (1) shall be in writing and on oath, and set |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | out the following particulars:<br>(a) the facts relied upon to show that there are reasonable grounds for suspecting that a person is planning, participating in, or committing, or has planned, participated in, or committed a serious offence; and<br>(b) a description of the manner in which it is proposed to intercept private communications or record or observe activities; and<br>(c) the name and address, if known, of the person whose private communications or a record or observations of whose activities there are reasonable grounds for suspecting will assist the police investigation of the case or if the name and address of the suspect are not known, a general description of the premises, place, thing, or type of facility in respect of which it is proposed to intercept private communications or record or observe activities; and<br>(d) the period for which a warrant is requested.<br><br>**11. Assistance to police executing a warrant or a permit –** It is a condition of a licence issued under Part 3 of the Telecommunications Act 2005 that the licensee provides such assistance to police executing a warrant granted under section 4or a permit granted under section 7 in respect of an interception device as is required by the police. |
| ***Section 3 – Jurisdiction*** | |
| **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 | **CA 4. Application –** (1) This Act applies to all offences for which the offender may be proceeded against and tried in Samoa.<br>(2) This Act applies to all acts done or omitted in Samoa.<br>(3) Subject to subsection (4), no act done or omitted outside of Samoa is an offence unless it is an offence by virtue of any provision of this Act or of any other enactment.<br>(4) For the purpose of jurisdiction, where any act or omission forming part of any offence, or any event necessary to the completion of any offence, occurs in Samoa, the offence shall be deemed to be committed in Samoa, whether the person charged with the offence was in Samoa or not at the time of the act, omission, or event.<br>(5) The Court of Appeal, the Supreme Court and the District Court shall have |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | jurisdiction to hear and determine any matter for which this Act or any other law provides such court with jurisdiction irrespective of whether any act or omission or event occurs in Samoa or any other place.<br><br>**7. Jurisdiction in respect of crimes on ships or aircraft beyond Samoa –**<br>(1) This section applies to any act done or omitted beyond Samoa by any person:<br>(a) on board any Samoan registered ship; or<br>(b) on board any Samoan aircraft; or<br>(c) on board any ship or aircraft, if that person arrives in Samoa on that ship or aircraft in the course or at the end of a journey during which the act was done or omitted; or<br>(d) being a citizen of Samoa, on board any foreign ship (not being a ship to which he or she belongs) on the high seas; or<br>(e) being a Samoan citizen or a person ordinarily resident in Samoa, on board any aircraft provided that paragraph (c) does not apply where the act was done or omitted by a person, not being a citizen of Samoa, on any ship or aircraft for the time being used as a ship or aircraft of any of the armed forces of any country; or<br>(f) being a Samoan citizen or a person ordinarily resident in Samoa, on board any ship or aircraft as a servant or an officer of the Government of Samoa.<br>(2) Where any person does or omits any act to which this section applies, and that act or omission would, if it occurred within Samoa, be a crime under this Act or under any other enactment (whether that enactment was passed before or after the commencement of this Act), then, subject to the provisions of this Act and of that other enactment, the person is liable on conviction as if the act or omission had occurred in Samoa:<br>PROVIDED THAT where any proceedings are taken by virtue of the jurisdiction conferred by this section it shall be a defence to prove that the act or omission would not have been an offence under the law of the country of which the person charged was a national or citizen at the time of the act or omission, if it had occurred in that country.<br>(3) Where at any place beyond Samoa any person who belongs, or within 3 months previously has belonged, to any Samoan registered ship does or omits any act, whether on shore or afloat, not being an act, or omission to which |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | subsection (1) applies, and that act or omission would, if it occurred within Samoa, be a crime, then this section shall apply in respect of that act or omission in the same manner in all respects as if it had occurred on board a Samoan registered ship.<br>(4) This section shall be read subject to the provisions of section 221.<br><br>**8. Extraterritorial jurisdiction for offences with transnational aspects** –<br>(1) Even if the acts or omissions alleged to constitute the offence occurred wholly outside Samoa, proceedings may be brought for any offence against this Act committed in the course of committing any offence against the Counter Terrorism Act 2014, or an offence against sections 146 to 152 and 154 to 157 of this Act, if the person to be charged:<br>(a) is a Samoan citizen; or<br>(b) is ordinarily resident in Samoa; or<br>(c) has been found in Samoa and has not been extradited; or<br>(d) is a body corporate, or a corporation sole, incorporated under the law of Samoa.<br>(2) Even if the acts or omissions alleged to constitute the offence occurred wholly outside Samoa, proceedings may be brought for any offence against this Act, if the person to be charged:<br>(a) is a Samoan citizen or an ordinary resident of Samoa; and<br>(b) is outside of Samoa as an ambassador, diplomat, representative, envoy, attaché or employee or officer of the Government of Samoa. |
| **Chapter III – International co-operation** | |
| **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 | **EA 2. Interpretation-**<br>"Extradition offence" in relation to an extradition country, means:<br>(a) An offence (including an offence of a purely fiscal character) against the law of that extradition country that:<br>(i) Is an offence for which the maximum penalty is death or imprisonment, or other deprivation of liberty, for a period of not less than 12 months; and |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>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** | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | |
| **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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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;<br>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 | **MACMA 7. Requests to be made by Attorney-General –**<br>A request by Samoa for assistance under this Part shall be made by or through the Attorney-General.<br><br>**22. Requests to be made to Attorney-General-**<br>(1) Every request by a foreign State for assistance in a criminal matter pursuant to this Part shall be made:<br>(a) to the Attorney-General; or<br>(b) to a person authorised by the Attorney-General to receive requests by foreign States under this Part.<br>(2) Where a request by a foreign State is made to a person authorised under paragraph ( 1 )(b ), the request shall be taken, for the purposes of this Act, to have been made to the AttomeyGeneral.<br><br>**24. Refusal of assistance -** A request by a foreign State for assistance under this Act may be:<br>(a) refused in whole or in part if, in the opinion the Attorney-General, the request would be likely to prejudice the sovereignty, security or other essential public interest of Samoa or would be against the interest of justice; and/or<br>(b) postponed in whole or in part, if, after consulting with the Competent Authority of the foreign State, the Attorney-General is of the opinion that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Samoa. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| 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 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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<br>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. | **MACMA 23. Form of request –**<br>(1) A request for assistance shall:<br>(f) include a statement setting out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes; |
| **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; | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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:<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.<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, | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | **MACMA 39. Assistance in obtaining article or thing by search-**<br>(1) A foreign State may request the Attorney-General to assist in obtaining an article or thing by search and seizure.<br>(2) Where the Attorney-General is satisfied that:<br>(a) the request relates to a criminal matter in respect of a foreign serious offence; and<br>(b) there are reasonable grounds for believing that an article or thing relevant to the proceedings is located in Samoa,<br>the Attorney-General may direct an authorised officer to apply to a Judge or the Registrar of the Court for a search warrant in accordance with section 40. |
| **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, | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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 | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |

**SAMOA LEGISLATION :**
**- CRIMES ACT – "CA",**
**- TELECOMMUNICATIONS ACT – "TA"**
**- CRIMINAL PROCEDURE ACT - "CPA"**
**- COPYRIGHT ACT "CRA"**
**- POLICE POWERS ACT – "PPA"**
**- "MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT – "MACMA"**

Back to the Table of Contents