# Sierra Leone

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version [09 May 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.*



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

| State: | |
|---|---|
| **Signature of the Budapest Convention:** | No |
| **Ratification/accession:** | No |

| 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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART I - PRELIMINARY**<br>**Definitions**<br>**1.**<br>In this Act, unless the contrary intention appears -<br>"**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><br>"**computer data storage medium**" means any device, physical or virtual, containing or designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed form for use by a computer;<br><br>"**computer system**" means any physical or virtual device, or any set of associated physical or virtual devices; or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data at least one of which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system;<br>(…)<br>"**service provider**" means a public or private entity that provides to users of its services the means to communicate by use of a computer system including any other entity that processes or stores computer data on behalf of that entity or its users; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | "**subscriber information**" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established4 5<br>(a) the type of communication service used, the technical provisions taken thereto and the period of service;<br>(b) the subscriber's identity, postal, geographic, electronic mail address, telephone and other access number, billing and payment information available on the basis of a service agreement or arrangement; or<br>(c) any other information on the site of an installation of communication equipment available on the basis of a service agreement or arrangement;<br><br>"**traffic data"** means 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 the type of underlying service;<br>(…) |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Unauthorised access**<br>**33.**<br>(1) A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured other than to secure and protect the integrity of digital communications or for unlawful purposes, commits an offence and is liable upon conviction to fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (2) For the purposes of this section, a person secures access to computer data stored in a computer system if by causing a computer system to perform a function he -<br>(a) alters or erases computer data; or<br>(b) copies, transfers or moves computer data to<br>(i) a computer system or computer data storage medium other than that in which it is stored; or<br>(ii) a different location in the same computer system or computer data storage medium in which it is stored;<br>(c) has the computer data output from the computer system in which it is held, whether by having it displayed or in any other manner;<br>(d) uses the computer data.<br><br>(3) For the purposes of this section, "**unauthorised**" means access of any kind, to a computer system, program or data, by a person who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than those authorised, with intent to secure access to the whole or a part of a computer system or to enable such access to be secured.<br><br>(4) The absence of authority to secure access to the whole or any part of a computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.<br><br>(5) For the purposes of this section intention or recklessness needs not relate to-<br>(a) a particular computer system;<br>(b) a particular program or data; or<br>(c) a program or data of any particular kind.<br><br>(6) A person shall be deemed to have contravened subsection (1)-<br>(a) in the absence of proof that the accused has the requisite knowledge to access the computer, program or data;<br>(b) notwithstanding the fact that committing the offence is impossible;<br>(c) in the absence of a program or data of any particular kind. |
| **Article 3 – Illegal interception** | **The CYBER SECURITY AND CRIME ACT, 2021** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. | **PART VI - OFFENCES**<br>**Unauthorised data interception**<br>**35.** (1) A person, including a corporation, partnership, or association, who intentionally and without authorisation intercepts or causes to be intercepted non-public transmissions of data to or from a computer system whether directly or indirectly the transmission of which -<br>(a) results in a significant financial loss;<br>(b) threatens national security;<br>(c) causes physical injury or death to any person; or<br>(d) threatens public health or public safety,<br>commits an offence and is liable upon conviction to a fine not less than Le 100.000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.<br><br>(2) Where a person, including a corporation, partnership, or association, intentionally and without authorisation, intercepts or causes to be intercepted, the transmission of data to or from a computer system over a telecommunication under subsection (1), commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.<br><br>Itis immaterial whether -<br>(a) the unauthorised interception is not directed at -<br>(i) a telecommunications system;<br>(ii) a particular computer system;<br>(iii) a program or data of any kind; or<br>(iv) a program or data held in any particular computer system;<br>(b) an unauthorised interception or an intended effect of it is permanent or temporary. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Unauthorised data interference**<br>**36.** A person, including a corporation, partnership, or association, who intentionally or without authorisation does an act in relation to a computer system which -<br>(a) causes destruction, damage, deletion, erasure, deterioration, generation,<br>modification or alteration of a program or data or any aspect or attribute related to the program or data;<br>(b) renders a program or data meaningless, useless or ineffective;<br>(c) obstructs, interrupts or interferes with the use of any program or data or any aspect or attribute related to the program or data;<br>(d) causes denial, prevention, suppression or hindrance of access to a program or data or any aspect or attribute related to the program or data or to any person entitled to it;<br>(e) causes impairment to the operation of a program;<br>(f) causes impairment to the reliability of any data, aspect or attribute related to a program or data;<br>(g) causes impairment to the security of a program or data or any aspect, attribute related to a program or data; or<br>(h) enables any of the acts mentioned in paragraphs (a) to (g) to be done,<br>commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000. |
| **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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Unauthorised system interference**<br>**37.** A person, including a corporation, partnership, or association, who intentionally or without authorisation does an unauthorised act in relation to a computer system which - |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (a) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the functioning of a computer system;<br>(b) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the communication between or with a computer system;<br>(c) interferes with or hinders access to a computer system;<br>(d) impairs the operation of a computer system;<br>(e) impairs the reliability of a computer system;<br>(f) impairs the security of a computer system; or<br>(g) enables any of the acts mentioned in paragraphs (a) to (f) to be done,<br>commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.<br><br>Provided that it shall not be an offence if interference with a computer system is undertaken in compliance and in accordance with the terms of a warrant issued under this Act or any law. |
| **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;<br>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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Misuse of device**<br>**38.** (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation manufactures, adapts, sells, procures for use, receives, possesses, imports, offers to supply, distributes or otherwise makes available -<br>(a) a device designed or adapted primarily for the purpose of committing an offence under this Act; or<br>(b) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, designed or adapted primarily for the purposes of a computer system.<br>(c) uses electronic communication equipment to bypass standard inter-connection path by illegal redirection of traffic.<br>commits an offence and is liable upon conviction to a fine not less than Le 500.000,000 and not more than Le 1,500,000,000 or to a term of imprisonment |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.<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. | not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 3,000,000,000 and not exceeding Le 6,000,000,000..<br><br>(2) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act under subsection (1), -<br>(a) for the purpose of training, testing or protection of a computer system; or<br>(b) in compliance of and in accordance with the terms of a judicial order issued or in exercise of a power under this Act or any law.<br><br>(3) For the purpose of subsection (1), possession of a program or a computer password, access code, or similar data includes having -<br>(a) possession of a computer system which contains the program or a computer password, access code, or similar data;<br>(b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or<br>(c) control of a program or a computer password, access code, or similar data that is in the possession of another person.<br><br>**Unauthorised disclosure of password**<br>**39.** A person, including a corporation, partnership, or association, who intentionally or without authorisation discloses to another person a password, access code or other means of gaining access to any program or data held in a computer system -<br>(a) for any wrongful gain;<br>(b) for any unlawful purpose; or<br>(c) to occasion any loss,<br>commits an offence and is liable upon conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 50,000,000 and not exceeding Le 100,000,000. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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 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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Computer-related fraud.**<br>**40.** (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes readable or intelligible, commits an offence and is liable upon conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 50,000,000 and not exceeding Le 100,000,000.<br><br>(2) A person, including a corporation, partnership, or association, who dishonestly or with similar intent -<br>(a) for wrongful gain;<br>(b) for wrongful loss to another person; or<br>(c) for any economic benefit for oneself or for another person,<br>intentionally or without authorisation inputs, alters, deletes or suppresses 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 of whether or not the data is directly readable or intelligible commits an offence and is liable on conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 year and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Computer fraud**<br>**41**. A person, including a corporation, partnership, or association, who intentionally causes loss of property, valuable security or consideration to another person by -<br>(a) inputting, alteration, modification, deletion, suppression or generation of a program or data;<br>(b) interference, hindrance, impairment or obstruction with the functioning of that computer system; or<br>(c) copying, transferring or moving data or program to another computer system, device or storage medium other than that in which it is held or to a different location in any other computer system, device or storage medium in which it is held;<br>(d) using any data or program; or<br>(e) having any data or program output from the computer system in which it is held, whether by having it displayed or in any other manner,<br>with fraudulent or dishonest intent of procuring, without right, an economic benefit for himself or for another person commits an offence and is liable upon conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100, 000,000 and not exceeding Le 250,000,000". |
| **Title 3 – Content-related offences** | |
| **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; | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - OFFENCES**<br>**Online child sexual abuse**<br>**47**. A person, including a corporation, partnership, or association, who, intentionally-<br>(a) distributes, produces, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, prints, photographs, copies, provides location, requests for, offers in any other way, or makes available in any |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | way child pornography through a computer system or storage data medium; or<br>(b) acquiesces a child's participation in pornography,<br>commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.<br><br>(2) A person, including a corporation, partnership, or association, who intentionally poses, grooms or solicits, through any computer system or network, to meet a child for the purpose of-<br>(a) engaging in sexual activity with the child;<br>(b) engaging in sexual activity with the child where-<br>(i) coercion, inducement, force or threat is used;<br>(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or<br>(iii) a child's mental or physical disability or situation of dependence is abused,<br>commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.<br><br>(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement.<br><br>(4) For purposes of this section -<br>**"child"** means a person under the age of 18 years;<br>**"child pornography**" includes data which, whether visual or audio, depicts -<br>(a) a child engaged in sexually explicit conduct;<br>(b) a person who appears to be a child engaged in sexually explicit conduct; or |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (c) realistic images representing a child engaged in sexually explicit conduct. |
| **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 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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Infringement of copyright and related rights**<br>**46.** A person, including a corporation, partnership, or association, who, through input, alteration, modification, deletion, suppression or generation of a program or data or through use of a computer, computer system or electronic device willfully infringes any right protected under the **Copyright Act, 2011 (Act No. 8 of 2011)** or any law in force for protection of copyrights and related rights, commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000 without prejudice to civil remedies that may be available**.** |
| **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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Attempting and aiding and abetting** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | **49.** (1) A person, including a corporation, partnership, or association, who intentionally abets the commission of, aids to commit, attempts to commit or does any act preparatory to or in furtherance of the commission of an offence under this Act commits an offence and is liable upon conviction to the same penalty as that prescribed in respect of the substantive offence under this Act.<br><br>(2) An offence may be deemed to have been committed under subsection (1), notwithstanding where the act in question took place. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART VI - OFFENCES**<br>**Corporate liability**<br>**56.** A natural person, who exercises management or supervisory authority, based on -<br>(a) power of representation of a legal person;<br>(a) authority to take decisions on behalf of a legal person;<br>(c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person,<br>and fails to exercise reasonable and proper control over such legal person commits an offence under this Act, and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000.<br><br>(2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act. |
| **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. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - POWERS AND PROCEDURES**<br>**Scope of powers and procedures**<br>**9.** (1) Powers and procedures under this Act shall be applicable to and may be exercised with respect to -<br>(a) criminal offences under this Act;<br>(b) criminal offences committed by means of a computer system, including mobile phones and other electronic equipment, under any other law; and<br>(c) the collection of evidence in electronic form of a criminal offence under this Act or any other law.<br><br>(2) In a trial of an offence under any law, the fact that evidence has been generated, transmitted or seized from or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted provided that the evidence has been properly obtained and preserved.<br><br>(3) The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under the Criminal Procedure Act, when exercised lawfully by any other law enforcement agency or service or any regulatory authority that by itself does not investigate or prosecute an offence. |

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. | 1991 Constitution of Sierra Leone, subsequently amended, provides in Chapter III for the recognition and protection of fundamental human rights and freedoms of the individual: fundamental human rights and freedoms of the individual, protection of right to life, protection from arbitrary arrest or detention, protection from inhuman treatment, protection from deprivation of property, protection for privacy of home and other property, protection of freedom of expression and the press.<br><br>Cyber Security and Cyber Crime Act 2021 provides specific safeguards and conditions related to procedural powers, such as judicial oversight and recognition of legal privileges and gives effect to principles of necessity and proportionality. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - POWERS AND PROCEDURES**<br>**Expedited preservation and partial disclosure of traffic data**<br>**13.** (1) An enforcement officer or other authorised person may, where he is satisfied that-<br>(a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and<br>(b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed, or rendered inaccessible,<br>by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expeditious preservation of the computer data.<br><br>(2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify-<br>(a) the service providers; and |

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 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.<br><br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | (b) the path through which the communication was transmitted.<br><br>(3) The period of preservation of data required under subsection (1) shall not exceed 30 days.<br><br>(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by an enforcement officer or other authorised person, where such extension is reasonably required for the purposes of -<br>(a) an investigation or prosecution;<br>(b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or<br>(c) averting overly burdensome cost of such preservation on the person in control of the computer system.<br><br>(5) A person to whom a notice under subsection (1) is given shall-<br>(a) be responsible to preserve the data for -<br>(i) a period not exceeding 30 days as specified in subsection (3); or<br>(ii) any extended period permitted by a Judge of the High Court under subsection (4).<br>(b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests, and<br>(c) disclose as soon as practicable, a sufficient amount of the non-content data to enable an enforcement officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2020**<br>**PART IV - POWERS AND PROCEDURES**<br>**Expedited preservation and partial disclosure of traffic data**<br>**13.** (1) An enforcement officer or other authorised person may, where he is satisfied that-<br>(a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and<br>(b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed, or rendered inaccessible,<br>by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expeditious preservation of the computer data. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | (2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify-<br>(a) the service providers; and<br>(b) the path through which the communication was transmitted.<br><br>(3) The period of preservation of data required under subsection (1) shall not exceed 30 days.<br><br>(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by an enforcement officer or other authorised person, where such extension is reasonably required for the purposes of -<br>(a) an investigation or prosecution;<br>(b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or<br>(c) averting overly burdensome cost of such preservation on the person in control of the computer system.<br><br>(5) A person to whom a notice under subsection (1) is given shall-<br>(a) be responsible to preserve the data for -<br>(i) a period not exceeding 30 days as specified in subsection (3); or<br>(ii) any extended period permitted by a Judge of the High Court under subsection (4).<br>(b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests, and<br>(c) disclose as soon as practicable, a sufficient amount of the non-content data to enable an enforcement officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2020**<br>**PART III - POWERS AND PROCEDURES**<br>**Production order.**<br>**12.** (1) Where it is necessary or desirable for the purposes of an investigation under this Act, a Judge of the High Court may upon an application by an enforcement officer or other authorised person, order-<br>(a) a person in possession or control of specified data stored in a computer system or a computer data storage medium; or<br>(b) a service provider in possession or control of specified subscriber information relating to services offered -<br>(i) in Sierra Leone; or |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.<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;<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. | (ii) based outside Sierra Leone but, offering its services in Sierra Leone;<br>to submit information in his possession or control.<br><br>(2) A Judge of the High Court may, by order, require a person-<br>(a) to whom an order is made under subsection (1), or<br>(b) in control of a computer system, to whom a warrant is issued under subsection (1) of section 10;<br>to keep such order or warrant confidential.<br><br>(3) A person who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 5,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 6 months and not more than 3 years or to both such fine and imprisonment and for a corporation partnership or association not less than Le100, 000,000 and not more than Le250, 000,000.<br><br>(4) An enforcement officer or other authorised person who uses the powers granted under subsection (1) for a purpose other than that stated in section 10 commits an offence and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not more than 5 years or to both such fine and imprisonment.<br><br>(5) An application under subsection (1) shall state the reasons explaining why it is believed that-<br>(a) a specified computer data sought is likely to be available with a person mentioned in subparagraph (a) or (b) of subsection (1);<br>(b) an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;<br>(c) the type of evidence suspected is likely to be produced by a person mentioned in subparagraph (a) or (b) of subsection (1);<br>(d) subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data;<br>(e) an identified offence is an offence in respect of which the order is sought; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (f) measures taken shall prepare and ensure that the specified computer data will be produced-<br>(i) whilst maintaining the privacy of other users, customers and third parties; and<br>(ii) without the disclosure of data of any party who is not part of the investigation; and<br>(g) measures taken shall prepare and ensure that the production of the specified computer data is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.<br><br>(6) Notwithstanding the provision of sub-section (1) above, a service provider or a person in possession or control of relevant specified data shall have the right to apply to the Judge of the High Court to challenge the issuance of a production order issued under this section on the ground of relevance, privilege, capacity to implement provisions of the order or otherwise protected from disclosure by law, or non-satisfaction of the requirements in subsection (5) of this Section. |
| **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: | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - POWERS AND PROCEDURES**<br>**Search and seizure of stored computer data.**<br>**10.** (1) Upon an application by an enforcement officer or other authorised person to a Judge of the High Court that there is reasonable grounds to believe that there may be in a specified computer system, program, data, computer data storage medium material specifying the basis of the belief and the scope of the warrant required which-<br>(a) may be reasonably required as evidence in proving a specifically identified offence in a criminal investigation or criminal proceedings;<br>(b) has been acquired by a person as a result of the commission of an offence,<br>the Judge may issue a warrant which shall authorise the enforcement officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.<br><br>(2) A warrant issued under subsection (1) shall authorize an enforcement officer or other authorised person to- |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (a) enter and search any premises or place if within those premises or place-<br>(i) an offence under this Act is being committed; or<br>(ii) there is evidence of the commission of an offence under this Act; or<br>(iii) there is an urgent need to prevent the commission of an offence under this Act<br>(b) search any person found on any premises or place which such authorised officers who are empowered to enter and search under paragraph (a) of subsection 1;<br>(c) stop, board and search where there is evidence of the commission of an offence under this Act;<br>(d) seize or secure a computer system or part of it or a computer-data storage medium;<br>(e) make and retain a copy of computer data;<br>(f) maintain the integrity of stored computer data;<br>(g) render inaccessible or remove computer data in the accessed computer system;<br>(h) have access to, inspect and check the operation of a computer system to which the warrant applies;<br>(i) have access to any information, obtained from the encrypted data contained or available to a computer system into an intelligible format for the purposes of the warrant;<br>(j) require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer<br>data therein, to provide the necessary computer data or information, to enable an enforcement officer or other authorised person in conducting an activity authorised under this section;<br>(k) have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.<br>(l) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.<br><br>(3) An application under subsection (1) shall provide reasons explaining why it is believed that- |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| | (a) the material sought will be found on the premises to be searched; or<br>(b) the purpose of an investigation search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.<br><br>(4) The court may issue a warrant under subsection (2) of this section where it is satisfied that-<br>(a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or<br>(b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or<br>(c) there are reasons for believing that the person or material on the premises may be relevant to the cyber crime or computer related offences under investigation; or<br>(d) there are reasons to believe that the person named in the warrant is preparing to commit an offence under this Act.<br><br>Provided that any such warrant is issued access shall be without prejudice to the rights to privacy of persons and may be rescinded upon an application by a person affected to a Judge of the High Court.<br><br>(5) Where an enforcement officer or other authorised person (s) authorised to search or access a specific computer system or part of it has reasonable grounds to believe that the data sought is stored in another cloud computer system and there is reasonable grounds to believe that such data is accessible from or available to the initial system, the enforcement officer or other authorised person may extend the search or accessing to such other system or systems.<br><br>(6) Computer data seized under subsection (2) shall only be lawfully used for the purpose for which it was originally obtained.<br><br>(7) An enforcement officer or other authorised person<br>shall- |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (a) only seize a computer system under subsection (2) when it is-<br>(i) not practical to secure the computer data; or<br>(ii) necessary to ensure that data will not be destroyed, altered or otherwise interfered with;<br>(b) exercise reasonable care while the computer system or computer data storage medium is retained.<br><br>(8) An enforcement officer or other authorised person who intentionally, recklessly or negligently misuses the powers granted under this section commits an offence and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not more than 5 years or to both such fine and imprisonment.<br><br>(9) A person who willfully obstructs an enforcement officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to a fine not less than Le5,000,000 and not more than Le30,000,000 or to a term of imprisonment not less than 6 months and not more than 3 years or to both such fine and imprisonment and in the case of a corporation, partnership or association to a fine not less than Le 50,000,000 and not more than Le100,000,000. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - POWERS AND PROCEDURES**<br>**Real-time collection of traffic data.**<br>**14.** (1) Where there are reasonable grounds to believe that traffic data associated with specified communications is reasonably required for the purposes of a specific criminal investigation, a Judge of the High Court may, on an application by an enforcement officer or other authorised person, order a service provider with the capacity to monitor, collect and record to-<br>(a) collect or record traffic data in real-time; and<br>(b) provide specified traffic data to the enforcement officer or other authorised person.<br><br>(2) An Order for the real-time collection or recording of traffic data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event not for more than 30 days. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (3) A period of real-time collection or recording of traffic data under subsection (2) may be extended by a Judge of the High Court for a further reasonable specified period of time the same to be for an additional period of 30 days, on an application by an enforcement officer or other authorised person, where the extension is reasonably required for the purposes of-<br>(a) an investigation or prosecution;<br>(b) further real-time collection or recording of traffic data necessary to achieve the purpose for which the Order under sub-section (1) was made;<br>(c) ensuring that the real-time collection or recording of traffic data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;<br>(d) preventing the investigation of being frustrated or seriously prejudiced; and<br>(e) averting overly burdensome cost of such extension on the person in control of the computer system.<br><br>(4) An application under subsection (1) shall state reasons explaining why it is believed that-<br>(a) a traffic data sought will be available with the person in control of the computer system;<br>(b) a type of traffic data suspected will be found on that computer system;<br>(c) the subject of an investigation or prosecution may be found on that computer system;<br>(d) an identified offence is an offence in respect of which the order is sought;<br>(e) measures shall be taken to maintain the privacy of other users, customers and third parties; and<br>(f) there will be no disclosure of data of any party not part of the investigation.<br><br>(5) A Judge of the High Court may also require a service provider to keep confidential, an Order under subsection (1) and a warrant issued under subsection (1) of section 10. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (6) A service provider who without reasonable excuse fails to comply with an Order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 5,000,000,000. |
| **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 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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - POWERS AND PROCEDURES**<br>**Interception of content data**<br>**15.** (1) Where there are reasonable grounds to believe that the content of a specifically identified electronic communications is reasonably required for the purposes of a specific investigation in respect of a felonious offence, a Judge of the High Court may, on an application by an enforcement officer or other authorised person, order a service provider to-<br>(a) collect or record; or<br>(b) co-operate and assist a competent authority in the collection or recording of,<br>content data of specified communication within the jurisdiction transmitted by means of a computer system, in real-time.<br><br>(2) An Order for the real-time collection or recording of content data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event not more than 30 days.<br><br>(3) An application under subsection (1) shall state reasons explaining why it is believed that -<br>(a) the content data sought will be available with the person in control of the computer system;<br>(b) the type of content data suspected will be found on a computer system;<br>(c) an identified offence is the offence for which the warrant is sought;<br>(d) further disclosures are needed to achieve the purpose for which the warrant is to be issued, where authority to seek real-time collection or recording on more than one occasion is needed;<br>(e) measures taken shall be guided by regulations made pursuant to this Act which shall ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| | (f) the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted;<br>(g) to achieve the purpose for which the warrant is being applied, real time collection or recording by a person in control of a computer system is necessary; and<br>(h) adequate provision is made to ensure the safe storage and protection of the content data obtained and be used solely for matters relating to investigations.<br><br>(4) A period of real-time collection or recording of content data under subsection (3) may be extended by a Judge of the High Court for a further reasonable specified period of time the same to be for an additional period not more than 30 days, on an application by an enforcement officer or other authorised person, where the extension is reasonably required for the purposes of-<br>(a) an investigation or prosecution;<br>(b) achieving the objective for which the warrant is to be issued;<br>(c) ensuring that the real-time collection or recording of content data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;<br>(d) preventing an investigation from being frustrated or seriously prejudiced; and<br>(e) averting overly burdensome cost of such realtime recording and collection on the person in control of the computer system.<br><br>(5) A Judge of the High Court may also require a service provider to keep confidential, an order made under subsection (1) and a warrant issued under subsection (1) of section 10.<br><br>(6) The service provider shall have express right to challenge an order regarding the collection of real time content data where there is non-compliance with the provisions of the Act by filling an application to a Judge of the High Court.<br><br>(7) A service provider who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le5,000,000,000. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| ***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 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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART III - POWERS AND PROCEDURES**<br>**Territorial jurisdiction.**<br>**17.** (1) The High Court shall have jurisdiction over any violation of this Act, including any violation committed by a Sierra Leone national regardless of the place of commission.<br><br>(2) The Jurisdiction of the High Court under subsection (1), shall lie if an offence under this Act was committed -<br>(a) within Sierra Leone;<br>(b) with the use of a computer system wholly or partly situated in Sierra Leone; or<br>(c) when by such commission, damage is caused to a natural or juridical person who, at the time the offence was committed, was in Sierra Leone. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Extradition.**<br>**24.** (1) This Act complements the **Extradition Act, 1974 ( Act No. 11 of 1974)** which makes provision for the extradition of persons accused or convicted of an offence in another country.<br><br>(2) Extradition shall not be requested for an offence unless it is an offence in both the foreign state and in Sierra Leone. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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.<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. | (3) An offence under this Act shall be extraditable if the penalty imposed is imprisonment for a term of not less than one year or a fine equivalent to the penalty of one year imprisonment.<br><br>(4) Extradition will be subject to the conditions provided for by the law of the foreign state or applicable extradition treaties, including the grounds on which the foreign state may refuse extradition.<br><br>(5) In line with the extradite or prosecute principle, where extradition is refused on the sole basis of-<br>(a) the nationality of the person sought to be extradited; or<br>(b) Sierra Leone having jurisdiction over the offence,<br>the investigation or prosecution shall be conducted and the matter reported to the foreign state. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Authority to make and act on mutual assistance requests.**<br>**23.** 1) The Attorney-General may make requests on behalf of Sierra Leone to a foreign state for mutual assistance in an investigation commenced or prosecution instituted in Sierra Leone, relating to a computer related offence or collection of electronic evidence.<br><br>(2) The Attorney-General may, in respect of a request from a foreign state for mutual assistance in an investigation commenced or prosecution instituted in that state –<br>(a) grant the request, in whole or in part, on such terms and conditions as may be deemed necessary;<br>(b) refuse the request on such conditions as he deems necessary; or<br>(c) postpone a request, in whole or in part, after consulting with the appropriate authority of the foreign state, on the ground that granting the request would be likely to prejudice the conduct of an investigation or prosecution in Sierra Leone.<br><br>(3) Mutual assistance requests under this section shall be effectuated-<br>(a) in accordance with the procedures specified by a foreign state, except where it is incompatible with the laws of Sierra Leone; or<br>(b) where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.<br>(4) The Attorney-General shall, where appropriate, before refusing or postponing assistance, after having consulted with the foreign state, consider whether the request may be granted partially or subject to such conditions, as he deems necessary.<br><br>(5) The Attorney-General shall promptly inform a foreign state of-<br>(a) the outcome of the execution of a request for mutual assistance;<br>(b) any reason that renders impossible, the execution of a request for mutual assistance or is likely to delay it significantly; or |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (c) any reason for refusal or postponement of a request for mutual assistance.<br><br>(6) A foreign state may request that Sierra Leone keeps confidential the fact of any request for mutual assistance, except to the extent necessary for its execution and if Sierra Leone cannot comply with the request for confidentiality, it shall promptly inform the foreign state, which shall then determine whether the request should nevertheless be executed. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Spontaneous information**<br>**21.** (1) The Attorney-General may, subject to this Act and without prior request, forward to a foreign state, information obtained under this Act, where he considers that the disclosure of such information may-<br>(a) assist the foreign state in initiating or carrying out an investigation or prosecution; or<br>(b) lead to a request for co-operation by a foreign state.<br><br>(2) Information provided under subsection (1), may be subject to such conditions including confidentiality, as the Attorney General may require.<br><br>(3) Where a foreign state cannot comply with conditions required under subsection (2), it shall notify the Attorney-General, who shall determine whether the information should nevertheless be provided and where the foreign state 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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Confidentiality and limitation of use**<br>**25.** Where there is no mutual assistance treaty or arrangement in force between a foreign state and Sierra Leone, Sierra Leone shall make the supply of information in response to a request on condition that it is-<br>(a) kept confidential; or<br>(b) used only for investigations or prosecutions stated in the request. |

Back to the Table of Contents

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

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Confidentiality and limitation of use**<br>**25.** Where there is no mutual assistance treaty or arrangement in force between a foreign state and Sierra Leone, Sierra Leone shall make the supply of information in response to a request on condition that it is-<br>(a) kept confidential; or<br>(b) used only for investigations or prosecutions stated in the request. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | |
| **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: | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Expedited preservation of stored computer data.**<br>**26.** (1) A foreign state may request or obtain the expeditious preservation of data stored by means of a computer system, located within Sierra Leone, in respect of which it intends to submit a request for mutual assistance, for the search, access, seizure, security or disclosure of the data.<br><br>(2) A request for preservation of data submitted under subsection (1) shall specify the-<br>(a) authority seeking the preservation of data;<br>(b) offence that is the subject of an investigation or prosecution, including a brief summary of the related facts;<br>(c) stored computer data to be preserved and its relationship to the offence;<br>(d) available information identifying the custodian of the stored computer data or the location of the computer system;<br>(e) necessity of the preservation of data; and<br>(f) intention to submit a request for mutual assistance for the search, access, seizure, security, or disclosure of the stored computer data.<br><br>(3) Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to expeditiously preserve the specified data in accordance with the procedures and powers under this Act.<br><br>(4) A request under subsection (1) shall be effected where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.<br><br>(5) A preservation of data effected in response to a request under subsection (1) shall be for a period not less than 90 days, in order to enable the foreign state, to submit a request for the search, access, seizure, security or disclosure of the |

| 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. | data and following the receipt of such a request, the data shall continue to be preserved until a final decision is taken on that pending request. |
| **Article 30 – Expedited disclosure of preserved traffic data**<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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Expedited disclosure of preserved traffic data.**<br>**27.** (1) Where during the course of executing a request undersection 26, with respect to a specified communication, it is discovered that a service provider in another state was involved in the transmission of the communication, the Attorney-General shall expeditiously disclose to the foreign state, sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.<br><br>(2) Expedited disclosure of preserved traffic data under subsection (1) may only be withheld where the –<br>(a) request concerns a political offence or an offence related to a political offence; or<br>(b) Attorney-General considers that the execution of the request is likely to prejudice the sovereignty of Sierra Leone, security or public interest. |
| **Article 31 – Mutual assistance regarding accessing of stored computer data** | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION** |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | **Mutual assistance regarding accessing of stored-computer data.**<br>**28.** (1) A foreign state may request the search, access, secure or disclosure of data stored by means of a computer system located within Sierra Leone, including data that has been preserved under section 26.<br><br>(2) When making a request under subsection (1), the foreign state shall provide adequate information on the following-<br>(a) the name of the authority conducting the investigation or prosecution to which the request relates;<br>(b) a description of the nature of the criminal offence and a statement setting out a summary of the relevant facts and laws;<br>(c) a description of the purpose of the request and of the nature of the assistance being sought;<br>(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in Sierra Leone, details of the offence in question, particulars of any investigation or prosecution commenced in respect of the offence, including a copy of any relevant restraining or confiscation order;<br>(e) details of any procedure that the foreign state wishes to be followed by Sierra Leone in giving effect to the request, particularly in the case of a request to take evidence;<br>(f) a statement setting out any wishes of the foreign state concerning confidentiality relating to the request and the reasons for those wishes;<br>(g) details of the period within which the foreign state wishes the request to be complied with;<br>(h) where applicable, details of the property, computer, computer system or device to be traced, restrained, seized or confiscated and of the grounds for believing that the property is believed to be in Sierra Leone;<br>(i) details of the stored computer data, data or program to be seized and its relationship to the offence;<br>(j) information identifying the custodian of the stored computer data or the location of the computer, computer system or device;<br>(k) an agreement on the question of the payment of the damages or costs of fulfilling the request;<br>(l) details to the effect that warrant in regard the matter under investigation has already been obtained to extend the investigations overseas; and<br>(m) any other information that may assist in giving effect to the request. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute in accordance with the procedures and powers under this Act or any other law.<br><br>(4) Upon obtaining necessary authorisation under subsection (3), including a warrant to execute, the Attorney-General may seek the support and cooperation of the foreign state during such search and seizure.<br><br>(5) Upon conducting the search and seizure under subsection (4), the Attorney-General shall provide the results of such search and seizure, as well as the evidence seized, to the foreign state. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Trans-border access to stored computer data.**<br>**29.** Subject to this Act, a police officer or other authorised person may, without authorisation-<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 Sierra Leone, stored computer data located in a foreign state, if such enforcement officer or other authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.<br><br>Provided that any such access shall be without prejudice to the right to privacy of persons and may be rescinded upon an application by a person affected to a Judge of the High Court. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Mutual assistance in real time collection of traffic data.**<br>**30.** (1) A foreign state may request the Attorney-General to provide assistance in real time collection of traffic data associated with specified communications in Sierra Leone transmitted by means of a computer system. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (2) A request for assistance under subsection (1) shall specify-<br>(a) the authority making the request;<br>(b) the offence that is the subject of a criminal investigation or prosecution and a brief summary of the related facts;<br>(c) the name of the authority with access to the relevant traffic data;<br>(d) the location at which the traffic data may be held;<br>(e) the intended purpose for the required traffic data;<br>(f) sufficient information to identify the traffic data;<br>(g) further details of relevant traffic data;<br>(h) the necessity for use of powers under this section; and<br>(i) the terms for the use and disclosure of the traffic data to third parties.<br><br>(3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute upon the request in accordance with the procedures and powers under this Act or any other law.<br><br>(4) Upon obtaining necessary authorisation including a warrant to execute a request under subsection (1), the Attorney- General may seek the support and cooperation of the foreign state during the search and seizure.<br><br>(5) Upon conducting the measures under this section, the Attorney-General shall provide the results of such measures as well as real-time collection of traffic data associated with specified communication to the foreign state. |
| **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. | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART IV - INTERNATIONAL COOPERATION**<br>**Mutual assistance regarding interception of content data.**<br>**31.** (1) A foreign state may, in relation to a serious offence in that state, request or provide assistance in the real time collection or recording of content data of specified communication transmitted by means of a computer system in Sierra Leone.<br><br>(2) A request for assistance under subsection (1) shall specify-<br>(a) the authority making the request;<br>(b) the offence that is the subject of a criminal investigation or prosecution and a brief summary of the facts; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (c) the name of the authority with access to the relevant communication;<br>(d) the location at which or nature of the communication;<br>(e) the intended purpose for the required communication;<br>(f) sufficient information to identify the communication;<br>(g) details of the data of the relevant interception;<br>(h) the recipient of the communication;<br>(i) the intended duration for the use of the communication;<br>(j) the necessity for use of powers under this section; and<br>(k) the terms for the use and disclosure of the communication to third parties.<br><br>(3) Upon receiving a request under subsection (1), the Attorney- General shall take appropriate action to execute the request in accordance with the procedures and powers under this Act.<br><br>(4) The Attorney-General shall, on executing the request under subsection (3), provide the results of such action as well as real time collection or recording of content data of specified communication to the foreign state. |
| **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 | **The CYBER SECURITY AND CRIME ACT, 2021**<br>**PART V - INTERNATIONAL COOPERATION**<br>**Point of contact.**<br>**32.** (1) The National Cybersecurity Coordinator or his authorized representative shall designate a point of contact available on a 24-hour, 7-days-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigation or prosecution of offences related to computer systems and data, or for the collection of evidence in electronic form.<br><br>(2) Immediate assistance to be provided under subsection (1) shall include -<br>(a) the provision of technical advice;<br>(b) the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; and<br>(c) the collection of evidence, the provision of legal information, and locating of suspects.<br><br>(3) A point of contact under subsection (1), shall - |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (a) be resourced with and possess the requisite capacity to securely and efficiently carry out communication with other points of contact in other states, on an expedited basis;<br>(b) have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis. |
| **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