[South Africa]

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [08 August 2022]

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention: 23/11/2001	
Ratification/accession: N/A	Invited to accede

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Cybercrimes Act 2021** **Chapter 1 DEFINITIONS AND INTERPRETATION** 1. (1) In this Act, unless the context indicates otherwise— **"article"** means any— (a) data; (b) computer program; (c) computer data storage medium; or (d) computer system, which— (i) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission; (ii) may afford evidence of the commission or suspected commission; or (iii) is intended to be used or is, on reasonable grounds believed to be intended to be used in the commission or intended commission, of— (aa) an offence in terms of Part I and Part II of Chapter 2; (bb) any other offence in terms of the law of the Republic; or (cc) an offence in a foreign State that is substantially similar to an offence contemplated in Part I or Part II of Chapter 2 or another offence recognised in the Republic; **"computer"** means any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	storage operations in accordance with set instructions and includes any data, computer program or computer data storage medium that are related to, connected with or used with such a device; **''computer data storage medium**'' means any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system; **''computer program''** means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; ''**computer system''** means— (a) one computer; or (b) two or more inter-connected or related computers, which allow these inter-connected or related computers to— (i) exchange data or any other function with each other; or (ii) exchange data or any other function with another computer or a computer system; **''computer system''** means— (a) one computer; or (b) two or more inter-connected or related computers, which allow these inter-connected or related computers to— (i) exchange data or any other function with each other; or (ii) exchange data or any other function with another computer or a computer system; (…) ''**electronic communications service provider''** means— (a) any person who provides an electronic communications service to the public, sections of the public, the State, or the subscribers to such service, under and in accordance with an electronic communications service licence issued to that person in terms of the Electronic Communications Act, 2005, or who is deemed to be licenced or exempted from being licenced as such in terms of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	that Act; and (b) a person who has lawful authority to control the operation or use of a private electronic communications network used primarily for providing electronic communications services for the owner's own use and which is exempted from being licensed in terms of the Electronic Communications Act, 2005; (…) "**traffic data''** means data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type, of the underlying service.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access 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.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 85 Definition** In this Chapter. unless the context indicates otherwise - **"access"** includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data" **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Unlawful access** 2. (1) Any person who unlawfully and intentionally performs an act in respect of— (a) a computer system; or (b) a computer data storage medium, which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3(1), 5(1) or 6(1), is guilty of an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) (a) Any person who unlawfully and intentionally accesses a computer system or a computer data storage medium, is guilty of an offence. (b) For purposes of paragraph (a)— (i) a person accesses a computer data storage medium, if the person— (aa) uses data or a computer program stored on a computer data storage medium; or (bb) stores data or a computer program on a computer data storage medium; and (ii) a person accesses a computer system, if the person— (aa) uses data or a computer program held in a computer system; (bb) stores data or a computer program on a computer data storage medium forming part of the computer system; or (cc) instructs, communicates with, or otherwise uses, the computer system. (c) For purposes of paragraph (b)— (i) a person uses a computer program, if the person— (aa) copies or moves the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; (bb) causes a computer program to perform any function; or (cc) obtains the output of a computer program; and (ii) a person uses data, if the person— (aa) copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or (bb) obtains the output of data.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 86 Unauthorised access to, interception of or interference with data** (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993). a person who intentionally accesses or intercepts any data without authority or permission to do so. is guilty of an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	(…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Unlawful interception of data** 3. (1) Any person who unlawfully and intentionally intercepts data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system, is guilty of an offence. (2) Any person who unlawfully and intentionally possesses data or the output of data, with the knowledge that such data was intercepted unlawfully as contemplated in subsection (1), is guilty of an offence. (3) Any person who is found in possession of data or the output of data, in regard to which there is a reasonable suspicion that such data was intercepted unlawfully as contemplated in subsection (1) and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. (4) For purposes of this section **''interception of data''** means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4(2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data, and includes the— (a) examination or inspection of the contents of the data; and (b) diversion of the data

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 86 Unauthorised access to, interception of or interference with data** (…) (2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence. (…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Unlawful interference with data or computer program** 5. (1) Any person who unlawfully and intentionally interferes with— (a) data; or (b) a computer program, is guilty of an offence. (2) For purposes of this section "**interfere with data or a computer program**" means to permanently or temporarily— (a) delete data or a computer program; (b) alter data or a computer program; (c) render vulnerable, damage or deteriorate data or a computer program; (d) render data or a computer program meaningless, useless or ineffective; (e) obstruct, interrupt or interfere with the lawful use of, data or a computer program; or (f) deny access to data or a computer program, held in a computer data storage medium or a computer system.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 86 Unauthorised access to, interception of or interference with data** (…) (5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence (…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Unlawful interference with data or computer program** 6. 1) Any person who unlawfully and intentionally interferes with a computer data storage medium or a computer system, is guilty of an offence. (2) For purposes of this section **''interfere with a computer data storage medium or a computer system''** means to permanently or temporarily— (a) alter any resource; or (b) interrupt or impair— (i) the functioning; (ii) the confidentiality; (iii) the integrity; or (iv) the availability, of a computer data storage medium or a computer system.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of:	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 86 Unauthorised access to, interception of or interference with data** (…) (3) A person who unlawfully produces, sells, offers to sell, procures for use,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence (…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device** 7. (1) Any person who unlawfully and intentionally— (a) acquires; (b) possesses; (c) provides to another person; or (d) uses, a password, an access code or similar data or device for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), is guilty of an offence. (2) Any person who is found in possession of a password, an access code or similar data or device in regard to which there is a reasonable suspicion that such password, access code or similar data or device— (a) was acquired; (b) is possessed; (c) is to be provided to another person; or (d) was used or may be used, for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence. (3) For purposes of this section **''password, access code or similar data or**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	device'' includes— (a) a secret code or pin; (b) an image; (c) a security token; (d) an access card; (e) any device; (f) biometric data; or (g) a word or a string of characters or numbers, used for financial transactions or user-authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 87 Computer-related extortion, fraud and forgery** (…) (1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence. (…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Cyber forgery and uttering** 9. (1) Any person who unlawfully and with the intention to defraud makes— (a) false data; or (b) a false computer program, to the actual or potential prejudice of another person, is guilty of the offence of cyber forgery. (2) Any person who unlawfully and with the intention to defraud, passes off—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) false data; or (b) a false computer program, to the actual or potential prejudice of another person, is guilty of the offence of cyber uttering.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 87 Computer-related extortion, fraud and forgery** (…) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence. (…) **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part I CYBERCRIMES** **Cyber fraud** 8. Any person who unlawfully and with the intention to defraud makes a misrepresentation— (a) by means of data or a computer program; or (b) through any interference with data or a computer program as contemplated in section 5(2)(a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(a), which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography	**SEXUAL OFFENCES AND RELATED MATTERS AMENDMENT ACT, 2007** **CHAPTER 1 DEFINITIONS AND OBJECTS** **Definitions and interpretation of Act**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	1. (…) **"child"** means— (a) a person under the age of 18 years; or (b) with reference to sections 15 and 16, a person 12 years or older but under the age of 16 years. **"child pornography"** means any image, however created, or any description or presentation of a person, real or simulated, who is, or who is depicted or described or presented as being, under the age of 18 years, of an explicit or sexual nature, whether such image or description or presentation is intended to stimulate erotic or 40 aesthetic feelings or not, including any such image or description of such person— (a) engaged in an act that constitutes a sexual offence; (b) engaged in an act of sexual penetration; (c) engaged in an act of sexual violation; (d) engaged in an act of self-masturbation; 45 (e) displaying the genital organs of such person in a state of arousal or stimulation; (f) unduly displaying the genital organs or anus of such person; (g) displaying any form of stimulation of a sexual nature of such person's breasts; (h) engaged in sexually suggestive or lewd acts; (i) engaged in or as the subject of sadistic or masochistic acts of a sexual nature; (j) engaged in any conduct or activity characteristically associated with sexual intercourse; or (k) showing or describing the body, or parts of the body, of that person in a manner or in circumstances which, within the context, violate or offend the sexual integrity or dignity of that person or any other person or is capable of 5 being used for the purposes of violating or offending the sexual integrity or dignity of that person or any other person;
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising	[The Copyright Act, 1978 (Act No. 98 of 1978) was originally drafted in 1978 and so does not adequately address the innovations of the 21st century and digital and electronic copyright]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 88 Attempt, and aiding and abetting** (…) (1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be. (2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be **Cybercrimes Act 2021**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS **Part III: ATTEMPTING, CONSPIRING, AIDING, ABETTING, INDUCING, INCITING, INSTIGATING, INSTRUCTING, COMMANDING OR PROCURING TO COMMIT OFFENCE** **Cyber fraud** **Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence** 17. Any person who unlawfully and intentionally— (a) attempts; (b) conspires with any other person; or (c) aids, abets, induces, incites, instigates, instructs, commands or procures another person, to commit an offence in terms of Part I or Part II of this Chapter, is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	N\A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIII CYBERCRIME** **Section 89 Penalties** (1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5). 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months. is liable to a fine or imprisonment for a period not exceeding five years. (2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years **Cybercrimes Act 2021** **Chapter 2 CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS** **Part V: SENTENCING** **Sentencing** 19. (1) Any person who contravenes the provisions of section 2(1) or (2), 3(3) or 7(2) is liable on conviction to a fine or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment. (2) Any person who contravenes the provisions of section 3(1) or (2), 4(1), 5(1), 6(1) or 7(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. (3) Any person who contravenes the provisions of section 11(1) is liable on conviction to a fine or to imprisonment for a period not exceeding 15 years or to both a fine and such imprisonment. (4) A court which convicts a person of an offence in terms of section 8, 9(1) or (2), 10 or 11(2) may, where a penalty is not prescribed in respect of that offence by any other law, impose a sentence, as provided for in section 276 of the Criminal Procedure Act, 1977, which that court considers appropriate and which is within that court's penal jurisdiction.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) A court which imposes any sentence in terms of this section, or where a person is convicted of the offence of theft that was committed or facilitated by electronic means, must, without excluding other relevant factors, consider as aggravating factors— (a) the fact that the offence was committed by electronic means; (b) the extent of the prejudice and loss suffered by the complainant or any other person as a result of the commission of such an offence; (c) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or (d) the fact that the offence was committed in concert with one or more persons. (6) (a) If a person is convicted of any offence provided for in section 2(1) or (2), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2), a court imposing any sentence in terms of those sections must, unless substantial and compelling circumstances justify the imposition of another sentence, impose a period of direct imprisonment, with or without a fine, if the offence was committed— (i) by the person; or (ii) with the collusion or assistance of another person, who as part of their duties, functions or lawful authority were in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed. (b) A sentence imposed in terms of paragraph (a) may not be suspended as contemplated in section 297(4) of the Criminal Procedure Act, 1977. (7) Any person who contravenes the provisions of section 14, 15 or 16 is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	N\A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the	N\A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE** **Expedited preservation of data direction** **41** (1) A specifically designated police official may— (a) if they believe on reasonable grounds that any person, an electronic communications service provider referred to in section 40(3), or a financial institution is— (i) in possession of; (ii) to receive; or (iii) in control of, data as contemplated in paragraph (a) of the definition of ''article''; and (b) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, issue an expedited preservation of data direction to such a person, electronic communications service provider or financial institution. (2) Subsection (1) also applies to— (a) archived communication-related information which an electronic communications service provider is no longer required to store due to the fact that the period contemplated in section 30(2)(a)(iii) of the Regulation of Interception of Communications and Provision of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Communication-related Information Act, 2002, is due to come to an end; or (b) any other data which— (i) must be stored for a certain period in terms of any other law and that period is due to come to an end; or (ii) is stored by an electronic communications service provider which is not real-time communication-related information or archived communication-related information as contemplated in section 1, read with section 30(2) and any directive issued in terms of that section, of the Regulation of Interception of Communications and Provision of Communication related Information Act, 2002. (3) An expedited preservation of data direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official. (4) An expedited preservation of data direction must direct the person, electronic communications service provider or financial institution affected thereby, from the time of service of the direction, and for a period of 21 days— (a) to preserve the current status of; (b) not to deal in any manner with; or (c) to deal in a certain manner with, the data referred to in the direction in order to preserve the availability and integrity of the data. (5) No data may be disclosed to a police official on the strength of an expedited preservation of data direction, unless it is authorised in terms of section 44. (6) The 21 day period referred to in subsection (4), may only be extended by way of a preservation of evidence direction contemplated in section 42, once, for an additional period which may not exceed 90 days. (7) A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction, referred to in subsection (1), is addressed may, in writing in the prescribed form and manner, apply to a magistrate in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated, for an amendment or the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	cancellation of the direction concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the direction. (8) The magistrate to whom an application is made in terms of subsection (7) must, as soon as possible after receipt thereof— (a) consider the application and may for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application; (b) give a decision in respect of the application; and (c) inform the applicant and specifically designated police official referred to in subsection (1) of the outcome of the application. (9) A person, electronic communications service provider or financial institution referred to in subsection (1) who— (a) fails to comply with an expedited preservation of data direction or contravenes the provisions of subsection (5); or (b) makes a false statement in an application referred to in subsection (7), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE** **Disclosure of data direction and search for, access to and seizure of articles subject to preservation** **44** (1) (a) A police official may, where it is expedient, other than by way of a search and seizure in terms of a warrant contemplated in section 29(1), to obtain— (i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction; or (ii) data as contemplated in paragraph (a) of the definition of ''article'', which is— (aa) held in a computer system or computer storage medium; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(bb) available to a computer system, apply to a magistrate or judge of the High Court for the issuing of a disclosure of data direction. (b) An application referred to in paragraph (a)(i) must— (i) indicate the identity of the police official who applies for the disclosure of data direction; (ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed; (iii) be accompanied by a copy of the expedited preservation of data direction or preservation of evidence direction or any amendment thereof; (iv) contain a description of the data which must be provided and the format in which it must be provided; (v) specify the grounds for believing that the data is an article as contemplated in paragraph (a) of the definition of ''article''; and (vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8(3) of the Superior Courts Act, 2013. (c) An application referred to in paragraph (a)(ii) must— (i) indicate the identity of the policy official who applies for the disclosure of data direction; (ii) identify the person, electronic communications service provider or financial institution to whom the disclosure of data direction must be addressed; (iii) contain a description of the data which must be provided and the format in which it must be provided; (iv) specify the grounds for believing that the data is an article as contemplated in paragraph (a) of the definition of ''article''; (v) specify the grounds for believing that the data, in question, is held in a computer system or computer data storage medium or is available to a computer system that is under the control of the person, electronic communications service provider or financial institution, referred to in subparagraph (ii), within the area of jurisdiction of the court; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(vi) comply with any supplementary directives relating to applications for the disclosure of data, which may be issued by the Chief Justice in terms of section 8(3) of the Superior Courts Act, 2013. (2) A magistrate or judge of the High Court may, subject to the provisions of section 4(2) of the Customs and Excise Act, 1964, sections 69(2)(b) and 71 of the Tax Administration Act, 2011, and section 21(e) and (f) of the Customs Control Act, 2014, on the written application by a police official referred to in subsection (1), if it appears to the magistrate or judge from information on oath or by way of affirmation, as set out in the application that— (a) there are reasonable grounds for believing that— (i) data which is subject to preservation in terms of an expedited preservation of data direction or a preservation of evidence direction, is an article as contemplated in paragraph (a) of the definition of ''article''; or (ii) data, which is an article as contemplated in paragraph (a) of the definition of ''article'', is— (aa) held in a computer system or computer data storage medium; or (bb) available to a computer system, within their area of jurisdiction; and (b) it will be in the interests of justice if a disclosure of data direction is issued, issue the disclosure of data direction applied for. (3) A disclosure of data direction must be in the prescribed form and must be served on the person, electronic communications service provider or financial institution affected thereby, in the prescribed manner by a police official. (4) The disclosure of data direction— (a) must direct the person, electronic communications service provider or financial institution to provide the data identified in the direction to the extent set out in the direction to an identified police official; (b) must specify the format in which the data identified in paragraph (a) must be provided; (c) must set out the period within which the data identified in paragraph (a) must

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	be provided; and (d) may specify conditions or restrictions relating to the provision of data authorised therein. (5) A person, electronic communications service provider or financial institution on whom a disclosure of data direction referred to in subsection (3) is served may, in writing in the prescribed form and manner, apply to the magistrate or judge for an amendment or the cancellation of the direction concerned on the ground that they cannot timeously or in a reasonable fashion comply with the direction. (6) The magistrate or judge to whom an application is made in terms of subsection (5) must, as soon as possible after receipt thereof— (a) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application; (b) give a decision in respect of the application; and (c) if the application is successful, inform the police official and the applicant of the outcome of the application. (7) Any data made available in terms of a disclosure of data direction, must be— (a) provided to the police official identified in the direction; and (b) accompanied by an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or financial institution, verifying the authenticity, integrity and reliability of the data that is furnished. (8) A person, electronic communications service provider or a financial institution who— (a) fails to comply with a disclosure of data direction; (b) makes a false statement in an application referred to in subsection (5); or (c) fails to comply with subsection (7), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment. (9)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) Any article subject to a preservation of evidence direction that is not "data" must be seized in terms of a warrant referred to in section 29(1). (b) A police official may, at any time, apply for a search warrant in terms of section 29(1) to search for, access or seize an article (which includes "data") that is or was subject to an expedited preservation of data direction or a preservation of evidence direction.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE** **Obtaining and using publicly available data or receiving data from person who is in possession of data** **45** A police official may, without being specifically authorised thereto in terms of this Chapter, for the purposes of investigating any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article— (a) receive, obtain or use publicly available data regardless of where the data is located geographically; or (b) receive and use non-publicly available data, regardless of where the data is located geographically, if a person who is in control of, or possesses the data, voluntarily and on such conditions regarding confidentiality and limitation of use which they deem necessary, discloses the data to a police official.
Article 19 – Search and seizure of stored computer data	**Electronic Communications and Transactions Act, 2002** **CHAPTER XII CYBER INSPECTORS**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 82 Power to inspect, search and seize** A cyber inspector may, in the performance of his or her functions, at any reasonable time, without prior notice and on the authority of a warrant issued in terms of section 83(1), enter any premises or access an information system that has a bearing on an investigation and— (a) search those premises or that information system; (b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation; (c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation; (d) demand the production of and inspect relevant licences and registration certificates as provided for in any law; (e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation; (f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence; (g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system; (h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter; or (i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with. (2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) The Criminal Procedure Act, 1977 (Act n°51 of 1977), applies with the necessary changes to searches and seizures in terms of this Act. (4) For purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages. **Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE** **Articles to be searched for, accesses or seized under search warrant** **29** (1) Subject to the provisions of sections 31, 32, 33 and 40(1) and (2) of this Act, section 4(3) of the Customs and Excise Act, 1964, sections 69(2)(b) and 71 of the Tax Administration Act, 2011, and section 21(e) and (f) of the Customs Control Act, 2014, an article can only be searched for, accessed or seized by virtue of a search warrant issued— (a) by a magistrate or judge of the High Court, on written application by a police official, if it appears to the magistrate or judge, from information on oath or by way of affirmation, as set out in the application, that there are reasonable grounds for believing that an article— (i) is within their area of jurisdiction; or (ii) is being used or is involved or has been used or was involved in the commission of an offence— (aa) within their area of jurisdiction; or (bb) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved or has been used or was involved in the commission of an offence; or (b) by a magistrate or judge of the High Court presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings. (2) A search warrant issued under subsection (1) must require a police official identified in the warrant to search for, access or seize the article in question and, to that end, must authorise the police official to— (a) search any person identified in the warrant;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant; (c) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found near such container, on or at such premises, vehicle, facility, ship or aircraft; (d) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who— (i) is nearby; (ii) uses; or (iii) is in possession or in direct control of, any data, computer program, computer data storage medium or computer system identified in the warrant to the extent set out in the warrant; (e) search for any article identified in the warrant to the extent set out in the warrant; (f) access an article identified in the warrant to the extent set out in the warrant; (g) seize an article identified in the warrant to the extent set out in the warrant; or (h) use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent set out in the warrant. (3) A search warrant issued under subsection (1) may require an investigator or other person identified in the warrant to assist the police official identified in the warrant, with the search for, access or seizure of the article in question, to the extent set out in the warrant. (4) (a) A search warrant may be executed at any time, unless the person issuing the warrant in writing specifies otherwise.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) A search warrant may be issued on any day and is of force until it is executed or is cancelled by the person who issued it or, if such person is not available, by a person with like authority. (5) A police official who executes a warrant under this section must hand to any person whose rights in respect of any search, or article accessed or seized under the warrant have been affected, a copy of the warrant and the written application of the police official contemplated in subsection (1)(a). (6) The provisions of subsections (1) to (5) apply with the changes required by the context to an amendment of a warrant issued in terms of subsection (1).
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE** **Interception of indirect communication and obtaining of real-time communication-related information** **40.** (1) The interception of an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication related Information Act, 2002, must take place in terms of a direction issued in terms of section 16(4) or 18(3) of that Act and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (2) The obtaining of real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, on an ongoing basis, as it becomes available, must take place in terms of a direction issued in terms of section 17(3) or 18(3) of that Act, and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (3) An electronic communications service provider who is— (a) in terms of section 30(1)(b) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, required to provide an electronic communications service which has the capability to store communication-related information; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) not required to store communication-related information in terms of a directive issued in terms of section 30(2) of that Act, must, in addition to any other obligation imposed by any law, comply with— (i) a real-time communication-related direction contemplated in subsection (2), in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available; (ii) an expedited preservation of data direction contemplated in section 41, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer; (iii) a preservation of evidence direction contemplated in section 42, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer; (iv) a disclosure of data direction contemplated in section 44, in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provider; or (v) any order of the designated judge in terms of section 48(6), in terms of which the electronic communications service provider is ordered to— (aa) obtain and preserve any real-time communication-related information; or (bb) obtain and furnish traffic data. (4) Any indirect communication which is to be intercepted or any real-time communication-related information or traffic data which is to be obtained, at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must further be dealt with in the manner provided for in an order referred to in section 48(6), which is issued by the designated judge
Article 21 – Interception of content data	**Cybercrimes Act 2021** **CHAPTER 4: POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE**

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Interception of indirect communication and obtaining of real-time communication-related information** **40.** (1) The interception of an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication related Information Act, 2002, must take place in terms of a direction issued in terms of section 16(4) or 18(3) of that Act and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (2) The obtaining of real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, on an ongoing basis, as it becomes available, must take place in terms of a direction issued in terms of section 17(3) or 18(3) of that Act, and must, subject to subsection (4), be dealt with further in the manner provided for in that Act. (3) An electronic communications service provider who is— (a) in terms of section 30(1)(b) of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, required to provide an electronic communications service which has the capability to store communication-related information; and (b) not required to store communication-related information in terms of a directive issued in terms of section 30(2) of that Act, must, in addition to any other obligation imposed by any law, comply with— (i) a real-time communication-related direction contemplated in subsection (2), in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available; (ii) an expedited preservation of data direction contemplated in section 41, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer; (iii) a preservation of evidence direction contemplated in section 42, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iv) a disclosure of data direction contemplated in section 44, in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provider; or (v) any order of the designated judge in terms of section 48(6), in terms of which the electronic communications service provider is ordered to— (aa) obtain and preserve any real-time communication-related information; or (bb) obtain and furnish traffic data. (4) Any indirect communication which is to be intercepted or any real-time communication-related information or traffic data which is to be obtained, at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must further be dealt with in the manner provided for in an order referred to in section 48(6), which is issued by the designated judge.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and	**Electronic Communications and Transactions Act, 2002** **CHAPTER XIV GENERAL PROVISIONS** **Section 90 Jurisdiction of courts** A court in the Republic trying an offence in terms of this Act has jurisdiction where- (a) the offence was committed in the Republic; (b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic; (c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or (d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**Cybercrimes Act 2021** **CHAPTER III JURISDICTION** **Jurisdiction** **24** (1) A court in the Republic has jurisdiction to try any offence referred to in Part I or Part II of Chapter 2, if— (a) the accused was arrested in the territory of the Republic, on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in the Republic; (b) the person to be charged is— (i) a citizen of the Republic or ordinary resident in the Republic; (ii) a company, incorporated or registered as such under any law, in the Republic; or (iii) any body of persons, corporate or unincorporated, in the Republic; (c) the offence was committed— (i) in the territory of the Republic; or (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time that the offence was committed; (d) any act in preparation of the offence or any action necessary to commit the offence or any part of the offence took place— (i) in the territory of the Republic; or (ii) on board a vessel, a ship, an off-shore installation or fixed platform, or an aircraft registered or required to be registered in the Republic at the time when the act, action or part of the offence took place; (e) the offence affects any person, a restricted computer system contemplated in section 11(1)(b), a public body or any business, in the Republic; (f) the offence was committed outside of the Republic against— (i) any person who is a citizen of the Republic or ordinarily resident in the Republic; (ii) a restricted computer system contemplated in section 11(1)(b); (iii) a company, incorporated or registered as such under any law, in the Republic;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iv) any body of persons, corporate or unincorporated, in the Republic; or (v) a government facility of the Republic, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or (g) the evidence reveals any other basis recognised by law in terms of which the court may assert jurisdiction to try the offence. (2) Any act alleged to constitute an offence referred to in Part I or Part II of Chapter 2 and which is committed outside the Republic by a person other than a person contemplated in subsection (1), must, regardless of whether or not the act constitutes an offence at the place of its commission, be deemed to have been committed in the Republic if— (a) that person is extradited to the Republic; or (b) that person— (i) is found to be in the Republic; and (ii) is for one or other reason not extradited by the Republic or if there is no application to extradite the person. (3) Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person so acted. (4) (a) A prosecution of an offence referred to in Part I or Part II of Chapter 2, which was committed outside the Republic— (i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and (ii) must commence before a court designated by the National Director of Public Prosecutions. (b) The accused must be served with a copy of the written permission and designation and the original thereof must be handed in at the court in which the proceedings are to commence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) The National Commissioner and the National Head of the Directorate, in consultation with the National Director of Public Prosecutions, must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act, regarding the investigation of offences that were committed outside the Republic.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 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.	**Act to provide for the extradition of persons accused or convicted of certain offences and for other indidental matters (1962 and amended in 1996)** **Extradition agreements** **2.** (1) The [State] President may, on such conditions as he or she may deem fit, but subject to the provisions of this Act- ~ (a) enter into an agreement with any foreign State, other than a designated State, providing for the surrender on a reciprocal basis of persons accused or convicted of the commission within the jurisdiction of the Republic or such State or any territory under the sovereignty or protection of such State of an extraditable offence or offences specified in such agreement and may likewise agree to any amendment or revocation of such agreement; and (b) designate any foreign State for purposes of section 3(3), and may at any time amend the conditions to which such designation was subjected to or revoke such designation (2) [amended] (3) No such agreement or designation or any amendment thereof, or revocation of the designation, shall be of any force or effect (a) until the ratification of, or accession to, or amendment or revocation of such agreement or designation has been agreed to by Parliament; (b) [amended] (c) unless provision is made by the law of the foreign State or by the agreement, that no person surrendered to such State shall, until he has been returned or had an opportunity of returning to the Republic, be detained or tried in the foreign State for any offence committed prior to his surrender other than the offence in respect of which extradition was sought.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	(3) ter The Minister shall as soon as practicable after Parliament has 35 agreed to the ratification of, or accession to, or amendment or revocation of an agreement or the designation of a foreign State, give notice thereof in the Gazette. (4) Any arrangement made with any foreign State which, by virtue of the provisions of the Extradition Acts, 1870 to 1906 of the Parliament of the United Kingdom as applied in the Republic, was in force in respect of the Republic immediately prior to the date of commencement of this Act, shall be deemed to be an agreement entered into and published on the said date by the State President under this section.
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	**Cybercrimes Act** **CHAPTER 5 MUTUAL ASSISTANCE** **Application of provisions of Chapter** **46.** The provisions of sections 48 to 51 apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996, and relate, unless specified otherwise, to the preservation of an article or other evidence in electronic format regarding the commission or suspected commission of— (a) an offence in terms of Part I or Part II of Chapter 2; (b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (c) an offence— (i) similar to those contemplated in Part I or Part II of Chapter 2; or (ii) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in a foreign State,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996. **International Co-operation in Criminal Matters Act (1996)** **CHAPTER 2 Mutual provision of evidence** **Issuing of letter of request** **2.** (1) If it appears to a court or to the officer presiding at proceedings that the examination at such proceedings of a person who is in a foreign State, is necessary in the interests of justice and that the attendance of such person cannot be obtained without undue delay, expense or inconvenience, the court or such presiding officer may issue a letter of request in which assistance from that foreign State is sought to obtain such evidence as is stated in the letter of request for use at such proceedings. (2) A judge in chambers or a magistrate may on application made to him or her issue 10 a letter of request in which assistance from a foreign State is sought to obtain such information as is stated in the letter of request for use in an investigation related to an alleged offence if he or she is satisfied - (a) that there are reasonable grounds for believing that an offence has been committed in the Republic or that it is necessary to determine whether an 15 offence has been committed; (b) that an investigation in respect thereof is being conducted; and (c) that for purposes of the investigation it is necessary in the interests of justice that information be obtained from a person or authority in a foreign State. (3) Subject to subsection (4), a letter of request shall be sent to the Director General 20 for transmission- (a) to the court or tribunal specified in the letter of request; or (b) to the appropriate government body in the requested State. (4) (a) In a case of urgency a letter of request may be sent directly to the court or tribunal referred to in subsection (3)(a), exercising jurisdiction in the place where the 25 evidence is to be obtained, or to the appropriate government body referred to in subsection (3)(b).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) The Director-General shall as soon as practicable be notified that a letter of request was sent in the manner referred to in paragraph (a) and he or she shall be furnished with a copy of such a letter of request.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Spontaneous information** **47.** (1) The National Commissioner or the National Head of the Directorate, may, on such conditions regarding confidentiality and limitation of use as they may determine, furnish any information obtained during any investigation, to a law enforcement agency of a foreign State when the National Commissioner or the National Head of the Directorate is of the opinion that the disclosure of such information may— (a) assist the foreign State in the initiation or carrying out of investigations; or (b) lead to further cooperation with a foreign State to carry out an investigation, regarding the commission or suspected commission of— (i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic; (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (iii) an offence— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in that foreign State. (2) The South African Police Service may receive any information from a foreign State, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which may— (a) assist the South African Police Service in the initiation or carrying out of investigations; or (b) lead to further cooperation with a foreign State to carry out an investigation,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	regarding the commission or suspected commission of— (i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic; (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (iii) an offence— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in that foreign State.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Foreign requests for assistance and cooperation** **48.** (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the— (a) preservation of data or other article; (b) seizure of data or other article; (c) expedited disclosure of traffic data; (d) obtaining of real-time communication-related information or archived communication-related information; or (e) interception of indirect communications, must, subject to subsection (9), be submitted to the designated Point of Contact. (2) The designated Point of Contact must submit the request to the National Director of Public Prosecutions for consideration. (3) (a) Upon receipt of a request referred to in subsection (2), the National Director of Public Prosecutions must satisfy himself or herself that— (i) proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or (ii) there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent	to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and (iii) the offence in question is— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article; and (iv) the foreign State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, 1996, for obtaining the data, information, a communication or an article in the Republic for use in such proceedings or investigation in the foreign State. (b) For purposes of paragraph (a), the National Director of Public Prosecutions may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in subsection (3)(a). (4) (a) The National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the Cabinet member responsible for the administration of justice, for the Cabinet member's approval. (b) Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1) to the designated judge for consideration. (5) Where the request relates to the expedited disclosure of traffic data, subsections (3)(a)(iv) and (4) do not apply, and the National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the designated judge.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	(6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order they deem appropriate to ensure that the requested— (a) data or other article is preserved in accordance with section 42; (b) data or other article is seized on an expedited basis in accordance with section 29 and preserved; (c) traffic data is disclosed on an expedited basis in terms of a disclosure of data direction in accordance with section 44; (d) real-time communication-related information or archived communication related information, is obtained and preserved; or (e) indirect communications are intercepted and preserved, as is specified in the request**.** (7) The designated judge may only issue an order contemplated in subsection (6), if— (a) on the facts alleged in the request, there are reasonable grounds to believe that— (i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been, is being, or will probably be committed; or (ii) any other offence substantially similar to an offence recognised in the Republic, has been, is being, or will probably be committed by means of, or facilitated through the use of, an article; and (iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6); (b) the request clearly identifies— (i) the person, electronic communications service provider or financial institution— (aa) who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or (bb) from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted; (ii) the data or other article which must be preserved;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii) the data or other article which must be seized on an expedited basis and be preserved; (iv) the traffic data which must be disclosed on an expedited basis; (v) the real-time communication-related information or archived communication-related information, which is to be obtained; or (vi) the indirect communications, which are to be intercepted; (c) the request is, where applicable, in accordance with— (i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or (ii) any agreement with any foreign State entered into in terms of section 57; and (d) the order contemplated in subsection (6) is in accordance with any applicable law of the Republic. (8) The designated judge may, where a request relates to the expedited disclosure of traffic data— (a) specify conditions or restrictions relating to the disclosure of traffic data as they deem appropriate; or (b) refuse to issue an order referred to in subsection (6)(c), if the disclosure of the traffic data may prejudice the sovereignty, security, public safety or other essential interests of the Republic. (9) (a) In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State referred to in subsection (1), may be submitted directly to the designated judge. (b) Upon receipt of a request in terms of paragraph (a), the designated judge may issue any order referred to in subsection (6). (10) (a) A specifically designated police official must serve or execute an order contemplated in subsection (6). (b) The specifically designated police official referred to in paragraph (a), must inform—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) the designated judge; and (ii) the National Director of Public Prosecutions, in writing, of the fact that an order has been served or executed. (11) The National Director of Public Prosecutions must, in writing, inform the applicable authority in a foreign State of the fact that an order was issued and executed or not issued**.**
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Spontaneous information** **47.** (1) The National Commissioner or the National Head of the Directorate, may, on such conditions regarding confidentiality and limitation of use as they may determine, furnish any information obtained during any investigation, to a law enforcement agency of a foreign State when the National Commissioner or the National Head of the Directorate is of the opinion that the disclosure of such information may— (a) assist the foreign State in the initiation or carrying out of investigations; or (b) lead to further cooperation with a foreign State to carry out an investigation, regarding the commission or suspected commission of— (i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic; (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (iii) an offence— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in that foreign State. (2) The South African Police Service may receive any information from a foreign State, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which may—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) assist the South African Police Service in the initiation or carrying out of investigations; or (b) lead to further cooperation with a foreign State to carry out an investigation, regarding the commission or suspected commission of— (i) an offence contemplated in Part I or Part II of Chapter 2, in the Republic; (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (iii) an offence— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in that foreign State.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data** **50.** (1) The National Director of Public Prosecutions must inform— (a) the designated judge; and (b) the applicable authority in a foreign State, of the outcome of the request for assistance and cooperation. (2) Any traffic data made available in terms of an order referred to in section 48(6)(c), must be— (a) provided to the designated Point of Contact, in the prescribed manner, for submission to the applicable authority in a foreign State; and (b) accompanied by— (i) a copy of the order referred to in section 48(6); and (ii) an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	financial institution, verifying the authenticity, integrity and reliability of the information that is furnished. (3) The traffic data together with the copy of the order and affidavit referred to in subsection (2), must be provided to the applicable authority in a foreign State which requested the assistance in terms of section 48(1). (4) A person, electronic communications service provider or financial institution who— (a) fails to comply with subsection (2) or any regulations contemplated in section 59(1)(a)(xxii); or (b) makes a false statement in an affidavit referred to in subsection (2)(b)(ii), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment. **Issuing of direction requesting assistance from foreign State** **51.** (1) If it appears to a magistrate from information on oath or by way of affirmation that there are reasonable grounds for believing that— (a) an offence contemplated in Part I or Part II of Chapter 2; or (b) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article, has been committed or that it is necessary to determine whether the offence has been so committed and that it is necessary— (i) pending the issuing of a letter of request in terms of section 2(2) of the International Co-operation in Criminal Matters Act, 1996, to— (aa) preserve data or other articles; (bb) seize data or other articles on an expedited basis; (cc) obtain real-time communication-related information or archived communication-related information; or (dd) intercept indirect communications; or (ii) to obtain traffic data, within the area of jurisdiction of a foreign State, the magistrate may issue a direction in the prescribed form in which assistance from that foreign State is sought as is stated in the direction. (2) A direction contemplated in subsection (1) must specify that—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) there are reasonable grounds for believing that an offence contemplated in subsection (1)(a) or (b) has been committed in the Republic or that it is necessary to determine whether such an offence has been committed; (b) an investigation in respect thereof is being conducted; and (c) for purposes of the investigation it is necessary, in the interests of justice, that— (i) data or other articles specified in the direction, be preserved; (ii) data or any other article specified in the direction is to be seized on an expedited basis and be preserved; (iii) traffic data specified in the direction, be disclosed on an expedited basis; (iv) real-time communication-related information or archived communication-related information specified in the direction, be obtained and be preserved; or (v) indirect communications, specified in the direction, be intercepted and be preserved, within the area of jurisdiction of a foreign State. (3) The direction must be sent to the National Director of Public Prosecutions for transmission to— (a) the appropriate authority in the foreign State; or (b) a designated point of contact in the foreign State, which is requested to provide assistance and cooperation.
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Foreign requests for assistance and cooperation** **48.** (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the— (a) preservation of data or other article; (b) seizure of data or other article; (c) expedited disclosure of traffic data; (d) obtaining of real-time communication-related information or archived communication-related information; or (e) interception of indirect communications, must, subject to subsection (9), be submitted to the designated Point of Contact.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	(2) The designated Point of Contact must submit the request to the National Director of Public Prosecutions for consideration. (3) (a) Upon receipt of a request referred to in subsection (2), the National Director of Public Prosecutions must satisfy himself or herself that— (i) proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or (ii) there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and (iii) the offence in question is— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article; and (iv) the foreign State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, 1996, for obtaining the data, information, a communication or an article in the Republic for use in such proceedings or investigation in the foreign State. (b) For purposes of paragraph (a), the National Director of Public Prosecutions may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in subsection (3)(a). (4) (a) The National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the Cabinet member responsible for the administration of justice, for the Cabinet member's approval.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1) to the designated judge for consideration. (5) Where the request relates to the expedited disclosure of traffic data, subsections (3)(a)(iv) and (4) do not apply, and the National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the designated judge. (6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order they deem appropriate to ensure that the requested— (a) data or other article is preserved in accordance with section 42; (b) data or other article is seized on an expedited basis in accordance with section 29 and preserved; (c) traffic data is disclosed on an expedited basis in terms of a disclosure of data direction in accordance with section 44; (d) real-time communication-related information or archived communication related information, is obtained and preserved; or (e) indirect communications are intercepted and preserved, as is specified in the request**.** (7) The designated judge may only issue an order contemplated in subsection (6), if— (a) on the facts alleged in the request, there are reasonable grounds to believe that— (i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been, is being, or will probably be committed; or (ii) any other offence substantially similar to an offence recognised in the Republic, has been, is being, or will probably be committed by means of, or facilitated through the use of, an article; and (iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6); (b) the request clearly identifies—

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(i) the person, electronic communications service provider or financial institution— (aa) who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or (bb) from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted; (ii) the data or other article which must be preserved; (iii) the data or other article which must be seized on an expedited basis and be preserved; (iv) the traffic data which must be disclosed on an expedited basis; (v) the real-time communication-related information or archived communication-related information, which is to be obtained; or (vi) the indirect communications, which are to be intercepted; (c) the request is, where applicable, in accordance with— (i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or (ii) any agreement with any foreign State entered into in terms of section 57; and (d) the order contemplated in subsection (6) is in accordance with any applicable law of the Republic. (8) The designated judge may, where a request relates to the expedited disclosure of traffic data— (a) specify conditions or restrictions relating to the disclosure of traffic data as they deem appropriate; or (b) refuse to issue an order referred to in subsection (6)(c), if the disclosure of the traffic data may prejudice the sovereignty, security, public safety or other essential interests of the Republic. (9)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State referred to in subsection (1), may be submitted directly to the designated judge. (b) Upon receipt of a request in terms of paragraph (a), the designated judge may issue any order referred to in subsection (6). (10) (a) A specifically designated police official must serve or execute an order contemplated in subsection (6). (b) The specifically designated police official referred to in paragraph (a), must inform— (i) the designated judge; and (ii) the National Director of Public Prosecutions, in writing, of the fact that an order has been served or executed. (11) The National Director of Public Prosecutions must, in writing, inform the applicable authority in a foreign State of the fact that an order was issued and executed or not issued**.**
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Cybercrimes Act 2021** **CHAPTER 5 MUTUAL ASSISTANCE** **Foreign requests for assistance and cooperation** **48.** (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for the— (a) preservation of data or other article; (b) seizure of data or other article; (c) expedited disclosure of traffic data; (d) obtaining of real-time communication-related information or archived communication-related information; or (e) interception of indirect communications, must, subject to subsection (9), be submitted to the designated Point of Contact. (2) The designated Point of Contact must submit the request to the National Director of Public Prosecutions for consideration.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) (a) Upon receipt of a request referred to in subsection (2), the National Director of Public Prosecutions must satisfy himself or herself that— (i) proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or (ii) there are reasonable grounds for believing that an offence has been committed in the requesting foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State; and (iii) the offence in question is— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article; and (iv) the foreign State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, 1996, for obtaining the data, information, a communication or an article in the Republic for use in such proceedings or investigation in the foreign State. (b) For purposes of paragraph (a), the National Director of Public Prosecutions may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in subsection (3)(a). (4) (a) The National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the Cabinet member responsible for the administration of justice, for the Cabinet member's approval. (b) Upon being notified of the Cabinet member's approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1) to the designated judge for consideration.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) Where the request relates to the expedited disclosure of traffic data, subsections (3)(a)(iv) and (4) do not apply, and the National Director of Public Prosecutions must submit the request for assistance, together with their recommendations, to the designated judge. (6) Subject to subsections (7) and (8), the designated judge may on receipt of a request referred to in subsection (4) or (5), issue any order they deem appropriate to ensure that the requested— (a) data or other article is preserved in accordance with section 42; (b) data or other article is seized on an expedited basis in accordance with section 29 and preserved; (c) traffic data is disclosed on an expedited basis in terms of a disclosure of data direction in accordance with section 44; (d) real-time communication-related information or archived communication related information, is obtained and preserved; or (e) indirect communications are intercepted and preserved, as is specified in the request**.** (7) The designated judge may only issue an order contemplated in subsection (6), if— (a) on the facts alleged in the request, there are reasonable grounds to believe that— (i) an offence substantially similar to the offences contemplated in Part I or Part II of Chapter 2 has been, is being, or will probably be committed; or (ii) any other offence substantially similar to an offence recognised in the Republic, has been, is being, or will probably be committed by means of, or facilitated through the use of, an article; and (iii) for purposes of the investigation it is necessary, in the interests of justice, to give an order contemplated in subsection (6); (b) the request clearly identifies— (i) the person, electronic communications service provider or financial institution— (aa) who or which will receive, is in possession of, or is in control of, the data or other article that must be preserved; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(bb) from whose facilities the data, real-time communication-related information, archived communication-related information, indirect communications or traffic data must be obtained or intercepted; (ii) the data or other article which must be preserved; (iii) the data or other article which must be seized on an expedited basis and be preserved; (iv) the traffic data which must be disclosed on an expedited basis; (v) the real-time communication-related information or archived communication-related information, which is to be obtained; or (vi) the indirect communications, which are to be intercepted; (c) the request is, where applicable, in accordance with— (i) any treaty, convention or other agreement to which that foreign State and the Republic are parties or which can be used as a basis for mutual assistance; or (ii) any agreement with any foreign State entered into in terms of section 57; and (d) the order contemplated in subsection (6) is in accordance with any applicable law of the Republic. (8) The designated judge may, where a request relates to the expedited disclosure of traffic data— (a) specify conditions or restrictions relating to the disclosure of traffic data as they deem appropriate; or (b) refuse to issue an order referred to in subsection (6)(c), if the disclosure of the traffic data may prejudice the sovereignty, security, public safety or other essential interests of the Republic. (9) (a) In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State referred to in subsection (1), may be submitted directly to the designated judge. (b) Upon receipt of a request in terms of paragraph (a), the designated judge may issue any order referred to in subsection (6).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(10) (a) A specifically designated police official must serve or execute an order contemplated in subsection (6). (b) The specifically designated police official referred to in paragraph (a), must inform— (i) the designated judge; and (ii) the National Director of Public Prosecutions, in writing, of the fact that an order has been served or executed. (11) The National Director of Public Prosecutions must, in writing, inform the applicable authority in a foreign State of the fact that an order was issued and executed or not issued**.**
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	N\A
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	N\A
Article 34 – Mutual assistance regarding the interception of content data	N\A

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Cybercrimes Act 2021** **CHAPTER 6 DESGINATED POINT OF CONTACT** **Establishment and functions of designated Point of Contact** **52.** (1) The National Commissioner must— (a) establish or designate an office within existing structures of the South African Police Service to be known as the designated Point of Contact for the Republic; and (b) equip, operate and maintain the designated Point of Contact. (2) The National Commissioner exercises final responsibility over the administration and functioning of the designated Point of Contact. (3) (a) The designated Point of Contact must ensure the provision of immediate assistance for the purpose of proceedings or investigations regarding the commission or intended commission of— (i) an offence under Part I or Part II of Chapter 2; (ii) any other offence in terms of the laws of the Republic, which may be committed by means of, or facilitated through the use of, an article; or (iii) an offence— (aa) similar to those contemplated in Part I or Part II of Chapter 2; or (bb) substantially similar to an offence recognised in the Republic, which may be committed by means of, or facilitated through the use of, an article, in a foreign State. (b) The assistance contemplated in subsection (3)(a), includes— (i) the provision of technical advice and assistance; (ii) the facilitation or provision of assistance regarding anything which is authorised under Chapters 4 and 5; (iii) the provision of legal assistance; (iv) the identification and location of an article; (v) the identification and location of a suspect; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(vi) cooperation with appropriate authorities of a foreign State. (4) The Cabinet member responsible for policing may make regulations to further— (a) regulate any aspect provided for in subsection (3); (b) impose additional duties on the designated Point of Contact; and (c) regulate any aspect which is necessary or expedient for the proper implementation of this section. (5) The National Director of Public Prosecutions must make available members of the National Prosecuting Authority— (a) who have particular knowledge and skills in respect of any aspect dealt with in this Act; and (b) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the National Director of Public Prosecutions, to provide legal assistance to the designated Point of Contact as may be necessary or expedient for the effective operation of the designated Point of Contact. (6) (a) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Oversight Act, 1994, on the functions and activities of the designated Point of Contact. (b) The report contemplated in paragraph (a) must include— (i) the number of matters in which assistance was provided in terms of subsection (3)(a); and (ii) the number of matters in which assistance was received from a foreign State.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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