CYBERCRIMES ACT
NO. 19 OF 2020

[ASSENTED TO 26 MAY, 2021]
[DATE OF COMMENCEMENT TO BE PROCLAIMED]

(Unless otherwise indicated)

(English text signed by the President)

This Act was published in *Government Gazette* 44651 dated 1 June, 2021.

ACT

To create offences which have a bearing on cybercrime; to criminalise the disclosure of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes; to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes; to delete and amend provisions of certain laws; and to provide for matters connected therewith.

ARRANGEMENT OF SECTIONS

Parliament of the Republic of South Africa enacts as follows:-

CHAPTER 1
DEFINITIONS AND INTERPRETATION

1. Definitions and interpretation.-(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 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;

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"Criminal Procedure Act, 1977" means the Criminal Procedure Act, 1977 (Act No. 51 of 1977);

"Customs and Excise Act, 1964" means the Customs and Excise Act, 1964 (Act No. 91 of 1964);

"Customs Control Act, 2014" means the Customs Control Act, 2014 (Act No. 31 of 2014);

"data" means electronic representations of information in any form;

"data message" means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form;

"designated judge" means a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002;

"designated Point of Contact" means the office established or designated in terms of section 52;

"Electronic Communications Act, 2005" means the Electronic Communications Act, 2005 (Act No. 36 of 2005);

"electronic communications network" means an electronic communications net-work as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;

"electronic communications service" means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;

"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 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;

"financial institution" means a financial institution as defined in section 1 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017);

"foreign State" means any State other than the Republic;

"Intelligence Services Oversight Act, 1994" means the Intelligence Services Oversight Act, 1994 (Act No. 40 of 1994);

"International Co-operation in Criminal Matters Act, 1996" means the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996);

"Justices of the Peace and Commissioners of Oaths Act, 1963" means the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963);

"magistrate" includes a regional court magistrate;

"Magistrates' Courts Act, 1944" means the Magistrates' Courts Act, 1944 (Act No. 32 of 1944);

"National Commissioner" means the National Commissioner of the South African Police Service, appointed by the President under section 207 (1) of the Constitution;

"National Director of Public Prosecutions" means the person contemplated in section 179 (1) (*a*) of the Constitution and appointed in terms of section 10 of the National Prosecuting Authority Act, 1998;

"National Head of the Directorate" means a person appointed in terms of section 17CA (1) of the South African Police Service Act, 1995;

"National Prosecuting Authority Act, 1998" means the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998);

"National Strategic Intelligence Act, 1994" means the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);

"output of a computer program" means any-

(*a*) data or output of the data;

(*b*) computer program; or

(*c*) instructions,

generated by a computer program;

"output of data" means by having data displayed or in any other manner;

"person" means a natural or a juristic person;

"police official" means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995;

"Prevention of Organised Crime Act, 1998" means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998);

"Protection from Harassment Act, 2011" means the Protection from Harassment Act, 2011 (Act No. 17 of 2011);

"Protection of Personal Information Act, 2013" means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013);

"publicly available data" means data which is accessible in the public domain without restriction;

"Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002" means the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002);

"responsible party" means a responsible party as defined in section 1 of the Protection of Personal Information Act, 2013;

"South African Police Service Act, 1995" means the South African Police Service Act, 1995 (Act No. 68 of 1995);

"South African Reserve Bank" means the South African Reserve Bank, referred to in section 223 of the Constitution, read with the South African Reserve Bank Act, 1989;

"South African Reserve Bank Act, 1989" means the South African Reserve Bank Act, 1989 (Act No. 90 of 1989);

"specifically designated police official" means a police official of the rank of captain or above referred to in section 33 of the South African Police Service Act, 1995, who has been designated in writing by the National Commissioner and the National Head of the Directorate, respectively, to-

(*a*) make oral applications for a search warrant or an amendment of a warrant contemplated in section 30;

(*b*) issue expedited preservation of data directions contemplated in section 41; or

(*c*) serve or execute an order of the designated judge as contemplated in section 48 (10);

"Superior Courts Act, 2013" means the Superior Courts Act, 2013 (Act No. 10 of 2013);

"Tax Administration Act, 2011" means the Tax Administration Act, 2011 (Act No. 28 of 2011); and

"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.

(2) For the purposes of section 2, 3 (2) or (3), or 7 (1) or (2) of this Act, any failure by a responsible party to comply with-

(*a*) the conditions for lawful processing of personal information referred to in Chapter 3;

(*b*) section 72; or

(*c*) the provisions of a code of conduct issued in terms of section 60,

of the Protection of Personal Information Act, 2013, must be dealt with in terms of Chapter 10 of that Act.

CHAPTER 2
CYBERCRIMES, MALICIOUS COMMUNICATIONS, SENTENCING AND ORDERS TO PROTECT COMPLAINANTS FROM THE HARMFUL EFFECT OF MALICIOUS COMMUNICATIONS

Part I
Cybercrimes

2. Unlawful access.-(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.

(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.

3. Unlawful interception of data.-(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 or any part thereof from its intended destination to any other destination.

4. Unlawful acts in respect of software or hardware tool.-(1) Any person who unlawfully and intentionally-

(*a*) uses; or

(*b*) possesses,

any software or hardware tool for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6 (1) or 7 (1) (*a*) or (*d*), is guilty of an offence.

(2) For purposes of this section **"software or hardware tool"** means any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof or a computer program, which is designated or adapted primarily for the purpose to-

(*a*) access as contemplated in section 2 (1) or (2);

(*b*) intercept data as contemplated in section 3 (1);

(*c*) interfere with data or a computer program as contemplated in section 5 (1);

(*d*) interfere with a computer data storage medium or a computer system as contemplated in section 6 (1); or

(*e*) acquire, make available or use a password, access code or similar data or device as defined in section 7 (3).

5. Unlawful interference with data or computer program.-(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.

6. Unlawful interference with computer data storage medium or computer system.-(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.

7. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device.-(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 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.

8. Cyber fraud.-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.

9. Cyber forgery and uttering.-(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-

(*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.

10. Cyber extortion.-Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in section 3 (1), 5 (1), 6 (1) or 7 (1) (*a*) or (*d*), for the purpose of-

(*a*) obtaining any advantage from another person; or

(*b*) compelling another person to perform or to abstain from performing any act,

is guilty of the offence of cyber extortion.

11. Aggravated offences.-(1) (*a*) Any person who commits an offence referred to in-

(i) section 3 (1), 5 (1) or 6 (1), in respect of; or

(ii) section 7 (1), in so far as the passwords, access codes or similar data and devices relate to,

a restricted computer system, and who knows or ought reasonably to have known or suspected that it is a restricted computer system, is guilty of an aggravated offence.

(*b*) For purposes of paragraph (*a*), a **"restricted computer system"** means any data, computer program, computer data storage medium or computer system-

(i) under the control of, or exclusively used by-

(*aa*) a financial institution; or

(*bb*) an organ of state as set out in section 239 of the Constitution, including a court; and

(ii) which is protected by security measures against unauthorised access or use.

(2) Any person who commits an offence referred to in section 5 (1), 6 (1) or 10, and who knows or ought reasonably to have known or suspected that the offence in question will-

(*a*) endanger the life or cause serious bodily injury to, or the death of, any person, or any number or group of persons;

(*b*) cause serious risk to the health or safety of the public or any segment of the public; or

(*c*) create a serious public emergency situation,

is guilty of an aggravated offence.

(3) The Director of Public Prosecutions having jurisdiction must authorise in writing a prosecution in terms of subsection (1) or (2).

12. Theft of incorporeal property.-The common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property.

Part II
Malicious Communications

13. Definitions.-In Part II, unless the context indicates otherwise-

"damage to property" means damage to any corporeal or incorporeal property;

"disclose" in respect of a data message referred to in sections 14, 15 and 16, means to-

(*a*) send the data message to a person who is the intended recipient of the electronic communication or any other person;

(*b*) store the data message on an electronic communications network, where the data message can be viewed, copied or downloaded; or

(*c*) send or otherwise make available to a person, a link to the data message that has been stored on an electronic communication network, where the data message can be viewed, copied or downloaded;

"group of persons" means characteristics that identify an individual as a member of a group, which characteristics include without limitation, race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth or nationality;

"related person" means any member of the family or household of a person or any other person in a close relationship with that person; and

"violence" means bodily harm.

14. Data message which incites damage to property or violence.-Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite-

(*a*) the causing of any damage to property belonging to; or

(*b*) violence against,

a person or a group of persons, is guilty of an offence.

15. Data message which threatens persons with damage to property or violence.-A person commits an offence if they, by means of an electronic communications service, unlawfully and intentionally discloses a data message, which-

(*a*) threatens a person with-

(i) damage to property belonging to that person or a related person; or

(ii) violence against that person or a related person; or

(*b*) threatens a group of persons or any person forming part of, or associated with, that group of persons with-

(i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or

(ii) violence against the group of persons or any person forming part of, or associated with, that group of persons,

and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph (*a*) or (*b*), respectively.

16. Disclosure of data message of intimate image.-(1) Any person (**"A"**) who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person (**"B"**), without the consent of B, is guilty of an offence.

(2) For purposes of subsection (1)-

(*a*) **"B"** means-

(i) the person who can be identified as being displayed in the data message;

(ii) any person who is described as being displayed in the data message, irrespective of the fact that the person cannot be identified as being displayed in the data message; or

(iii) any person who can be identified from other information as being displayed in the data message; and

(*b*) **"intimate image"** means a depiction of a person-

(i) real or simulated, and made by any means in which-

(*aa*) B is nude, or the genital organs or anal region of B is displayed, or if B is a female person, transgender person or intersex person, their breasts, are displayed; or

(*bb*) the covered genital or anal region of B, or if B is a female person, transgender person or intersex person, their covered breasts, are displayed; and

(ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made in a manner that-

(*aa*) violates or offends the sexual integrity or dignity of B; or

(*bb*) amounts to sexual exploitation.

Part III
Attempting, Conspiring, Aiding, Abetting, Inducing, Inciting, Instigating, Instructing, Commanding or Procuring to Commit Offence

17. Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence.-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.

Part IV
Competent Verdicts

18. Competent verdicts.-(1) If the evidence in criminal proceedings does not prove the commission of the offence charged but proves a contravention of section 17-

(*a*) in respect of the offence charged; or

(*b*) in respect of any other offence of which an accused may be convicted on the offence charged,

the accused may be found guilty of the offence so proved.

(2) If the evidence on a charge of a contravention of section 3 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of-

(*a*) section 2 (1) or (2);

(*b*) section 3 (2) or (3); or

(*c*) section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 3 (1),

the accused may be found guilty of the offence so proved.

(3) If the evidence on a charge of a contravention of section 5 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves-

(*a*) a contravention of section 2 (1) or (2);

(*b*) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 5 (1); or

(*c*) the offence of malicious injury to property,

the accused may be found guilty of the offence so proved.

(4) If the evidence on a charge of a contravention of section 6 (1), does not prove the offence or a contravention of section 17 in respect of that offence, but proves-

(*a*) a contravention of section 2 (1) or (2);

(*b*) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for purposes of contravening section 6 (1); or

(*c*) the offence of malicious injury to property,

the accused may be found guilty of the offence so proved.

(5) (*a*) If the evidence on a charge of a contravention of section 7 (1) (*a*) or (*d*) does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of-

(i) section 2 (1) or (2);

(ii) section 7 (1) (*b*) or (*c*) or (2); or

(iii) section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, to acquire or use a password, access code or similar data or device,

the accused may be found guilty of the offence so proved.

(*b*) If the evidence on a charge of a contravention of section 7 (1) (*b*) or (*c*) does not prove the offence or a contravention of section 17 in respect of that offence, but proves a contravention of section 7 (2), the accused may be found guilty of an offence so proved.

(6) If the evidence on a charge of a contravention of section 8, does not prove the offence or a contravention of section 17 in respect of the offence, but proves-

(*a*) a contravention of section 2 (1) or (2);

(*b*) a contravention of section 4 (1), in so far as it relates to the use or possession of a software or hardware tool, for the purposes of-

(i) interfering with data or a computer program as contemplated in section 5 (1); or

(ii) interfering with a computer data storage medium or a computer system as contemplated in section 6 (1);

(*c*) a contravention of section 7 (1) or (2), in so far as the password, access code or similar data or device was acquired, possessed, provided to another person or used for purposes of contravening the provisions of section 8;

(*d*) a contravention of section 9 (1) or (2);

(*e*) the common law offence of fraud or attempt to commit that offence;

(*f*) the common law offence of forgery or uttering or attempt to commit that offence; or

(*g*) the common law offence of theft or attempt to commit that offence,

the accused may be found guilty of the offence so proved.

(7) (*a*) If the evidence on a charge of a contravention of section 9 (1), does not prove the offence or a contravention of section 17 in respect of the offence, but proves-

(i) the common law offence of forgery;

(ii) a contravention of section 9 (2); or

(iii) the common law offence of uttering,

the accused may be found guilty of the offence so proved.

(*b*) If the evidence on a charge of a contravention of section 9 (2), does not prove the offence, but proves the common law offence of uttering, the accused may be found guilty of the offence so proved.

(8) If an accused is charged with a contravention of section 11 (1), and the evidence on the charge does not prove a contravention of section 11 (1) or a contravention of section 17 in respect of that offence, but proves a contravention of-

(*a*) section 2 (1) or (2);

(*b*) section 3 (1) or any competent verdict provided for in subsection (2);

(*c*) section 5 (1) or any competent verdict provided for in subsection (3);

(*d*) section 6 (1) or any competent verdict provided for in subsection (4); or

(*e*) section 7 (1) or any competent verdict provided for in subsection (5),

the accused may be found guilty of the offence so proved.

(9) If an accused is charged with a contravention of section 11 (2), and the evidence on the charge does not prove the offence or a contravention of section 17 in respect of the offence, but proves a contravention of-

(*a*) section 2 (1) or (2);

(*b*) section 5 (1) or any competent verdict provided for in subsection (3); or

(*c*) section 6 (1) or any competent verdict provided for in subsection (4),

the accused may be found guilty of the offence so proved.

(10) If the evidence on a charge for any offence referred to in the preceding subsections does not prove the commission of the offence so charged or any competent verdict in respect of the offence, but proves the commission of an offence which by reason of the essential elements of that offence is included in the offence so charged, the accused may be found guilty of the offence so proved.

(11) If an accused is charged with a contravention of section 14, 15 or 16, and the evidence on the charge does not prove the offence in question or a contravention of section 17 in respect of the offence, but proves the commission of an offence which by reason of the essential elements of that offence is included in the offence so charged, the accused may be found guilty of the offence so proved.

Part V
Sentencing

19. Sentencing.-(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.

(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.

Part VI
Orders to Protect Complainants from the Harmful Effect of Malicious Communications

20. Order to protect complainant pending finalisation of criminal proceedings.-(1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 14, 15 or 16 has allegedly been committed against them, may on an *ex parte* basis in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to-

(*a*) prohibit any person to disclose or further disclose the data message which relates to the charge; or

(*b*) order an electronic communications service provider whose electronic communications service is used to host or disclose the data message which relates to the charge, to remove or disable access to the data message.

(2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose, consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(3) If the court is satisfied that there-

(*a*) is *prima facie* evidence that an offence referred to in section 14, 15 or 16, has allegedly been committed against the applicant; and

(*b*) are reasonable grounds to believe that a person referred to in subsection (1) (*a*) disclosed the data message in question; or

(*c*) are reasonable grounds to believe that the electronic communications service of the electronic communications service provider referred to in subsection (1) (*b*), is used to host or was or is used to disclose the data message in question,

the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form.

(4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1) (*a*) or electronic communications service provider referred to in subsection (1) (*b*), in the prescribed manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1) (*a*) or electronic communications service provider referred to in subsection (1) (*b*).

(6) A person referred to in subsection (1) (*a*), other than the person who is accused of having committed the offence in question, or an electronic communications service provider referred to in subsection (1) (*b*), may, within 14 days after the order has been served on them in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3).

(7) (*a*) The court must as soon as reasonably possible consider an application submitted to it in terms of subsection (6) and may, for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(*b*) The court may, if good cause is shown for the variation or setting aside of the protection order, issue an order to this effect.

(8) The court may, for purposes of subsection (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(9) Any person referred to in subsection (1) (*a*) or an electronic communications service provider, referred to in subsection (1) (*b*), that fails to comply with an order referred to in subsection (3) or any variations thereof, is guilty of an offence.

(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to-

(*a*) attend or to remain in attendance;

(*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(*c*) remain in attendance at those proceedings as so adjourned; or

(*d*) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section.

(12) For purposes of this section and sections 21 and 22 **"to host a data message"** means to store the data message on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded.

21. Electronic communications service provider to furnish particulars to court.-(1) If an application for a protection order is made in terms of section 20 (1) and the court is satisfied in terms of section 20 (3) that a protection order must be issued and the particulars of the person referred to in section 20 (1) (*a*), who discloses the data message, or the electronic communications service provider referred to in section 20 (1) (*b*), whose service is used to host or was or is used to disclose the data message, is not known, the court may-

(*a*) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and

(*b*) issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with-

(i) the electronic communications identity number from where the data message originated;

(ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;

(iii) any information which indicates that the data message was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;

(iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 20 (1) (*a*) or the electronic communications service provider referred to in section 20 (1) (*b*), which provides a service to that person;

(v) any information that is available to an electronic communications service provider which-

(*aa*) confirms whether or not its electronic communications service is used to host or was or is used to disclose the data message in question; or

(*bb*) may be of assistance to the court to identify the electronic communications service provider whose service is used to host or was or is used to disclose the data message in questions; or

(vi) an assessment whether or not the electronic communications service provider is in a position to-

(*aa*) remove the data message or a link to such data message; or

(*bb*) disable access to the data message or a link to such data message.

(2) If the court issues a direction in terms of subsection (1) (*b*), the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(3) (*a*) The information referred to in subsection (1) (*b*) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.

(*b*) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for-

(i) an extension of the period of five ordinary court days referred to in paragraph (*a*) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or

(ii) the cancellation of the direction on the grounds that-

(*aa*) it does not provide an electronic communications service to the applicant or the person referred to in section 20 (1) (*a*);

(*bb*) the requested information is not available in the records of the electronic communications service provider; or

(*cc*) its service is not used to host or was or is not used to disclose the data message in question.

(4) After receipt of an application in terms of subsection (3) (*b*), the court-

(*a*) must consider the application;

(*b*) may, in the prescribed manner, request such additional evidence by way of an affidavit from the electronic communications service provider as it deems fit;

(*c*) must give a decision in respect thereof; and

(*d*) must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application.

(5) (*a*) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1) (*b*), consider the issuing of a protection order in terms of section 20 (3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned.

(*b*) Any information furnished to the court in terms of subsection (1) (*b*) forms part of the evidence that a court may consider in terms of section 20 (3).

(6) The Cabinet member responsible for the administration of justice may, by notice in the *Gazette*, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1) (*b*).

(7) Any electronic communications service provider or employee of an electronic communications service provider who-

(*a*) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3) (*a*) or such extended period allowed by the court in terms of subsection (3) (*b*); or

(*b*) makes a false statement in an affidavit referred to in subsection (1) (*b*) or (3) (*b*) in a material respect,

is guilty of an offence.

(8) For purposes of this section **"electronic communications identity number"** means a technical identification label which represents the origin or destination of electronic communications traffic.

22. Orders on finalisation of criminal proceedings.-(1) Whenever a person is-

(*a*) convicted of an offence in terms of section 14, 15 or 16; or

(*b*) acquitted of an offence in terms of section 14, 15 or 16,

but evidence proves that the person engaged in, or attempted to engage in, harassment as contemplated in the Protection from Harassment Act, 2011, the trial court may, after holding an enquiry, issue a protection order contemplated in section 9 (4) of the Protection from Harassment Act, 2011, against the person, whereafter the provision of that Act must apply with the necessary changes as required by the context.

(2) The trial court which convicts a person of an offence contemplated in section 14, 15 or 16, must order-

(*a*) that person to refrain from further making available, disclosing or distributing the data message contemplated in section 14, 15 or 16, which relates to the charge on which that person is convicted;

(*b*) that person or any other person to destroy the data message in question, any copy of the data message or any output of the data message and to submit an affidavit in the prescribed form to the prosecutor identified in the order that the data message has been so destroyed; or

(*c*) an electronic communications service provider to remove or disable access to the data message in question.

(3) The order referred to in subsection (2) (*b*), in so far as it relates to a person other than the person who has been convicted of the offence, and subsection (2) (*c*), must be in the prescribed form and must be served on the person or electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(4) Any person contemplated in subsection (2) (*a*) or (*b*) or electronic communications service provider contemplated in subsection (2) (*c*), that fails to comply with an order referred to in subsection (2), is guilty of an offence.

(5) An electronic communications service provider that is ordered to remove or disable access to the data message may, within 14 days after the order has been served on it in terms of subsection (3), upon notice to the trial court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (2) (*c*).

(6) (*a*) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (5) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(*b*) The trial court may, if good cause has been shown for the variation or setting aside of the order, issue an order to this effect.

(7) The court may, for purposes of subsection (6) (*a*), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(8) Any person who is subpoenaed in terms of subsection (7) to attend proceedings and who fails to-

(*a*) attend or to remain in attendance;

(*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(*c*) remain in attendance at those proceedings as so adjourned; or

(*d*) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(9) For purposes of this section **"trial court"** means-

(*a*) a magistrate's court established under section 2 (1) (*f*) (i) of the Magistrates' Courts Act, 1944;

(*b*) a court for a regional division established under section 2 (1) (*g*) (i) of the Magistrates' Courts Act, 1944; or

(*c*) a High Court referred to in section 6 (1) of the Superior Courts Act, 2013.

(10) Whenever a person is convicted of an offence in terms of section 14, 15 or 16, the trial court must issue an order that the person must reimburse all expenses reasonably incurred by-

(*a*) a complainant as a result of any direction issued in terms of section 21 (1) (*b*); or

(*b*) an electronic communications service provider to remove or disable access to the data message in question,

whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.

23. Penalties.-Any person or electronic communications service provider that is convicted of an offence referred in section 20 (9) or (10), 21 (7) or 22 (4) or (8), is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

CHAPTER 3
JURISDICTION

24. Jurisdiction.-(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;

(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.

(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 4
POWERS TO INVESTIGATE, SEARCH, ACCESS OR SEIZE

25. Definitions.-In this Chapter, unless the context indicates otherwise-

"access" includes without limitation to make use of-

(*a*) a computer data storage medium, or a computer system, or their accessories and components or any part thereof or any ancillary device or component thereto; and

(*b*) data or a computer program held in a computer data storage medium or a computer system,

to the extent necessary to search for and seize an article;

"investigator" means any fit and proper person, who is not a member of the South African Police Service and who is-

(*a*) identified and authorised in terms of a search warrant as contemplated in section 29 (3); or

(*b*) requested by a police official in terms of section 31 (2), 32 (3) or 33 (4),

to, subject to the direction and control of a police official, assist the police official with the search for, access or

seizure of an article; and

"seize" includes to-

(*a*) remove a computer data storage medium or any part of a computer system;

(*b*) render inaccessible, data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence;

(*c*) make and retain a copy of data or a computer program; or

(*d*) make and retain a printout of the output of data or a computer program.

26. Standard Operating Procedures.-(1) The Cabinet member responsible for policing, in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice must, after following a process of public consultation, within 12 months of the commencement of this Chapter, issue Standard Operating Procedures which must be observed by-

(*a*) the South African Police Service; or

(*b*) any other person or agency who or which is authorised in terms of the provisions of any other law to investigate any offence in terms of any law,

in the investigation of any offence or suspected offence in terms of Part I or Part II of Chapter 2 or any other offence or suspected offence which may be committed by means of, or facilitated through the use of, an article.

(2) The Standard Operating Procedures referred to in subsection (1) and any amendment thereto must be published in the *Gazette*.

27. Application of Criminal Procedure Act, 1977.-The Criminal Procedure Act, 1977, applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter.

28. Search for, access to, or seizure of certain articles.-A police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic.

29. Article to be searched for, accessed or seized under search warrant.-(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;

(*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.

(*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).

30. Oral application for search warrant or amendment of warrant.-(1) An application referred to in section 29 (1) (*a*), or an application for the amendment of a warrant issued in terms of section 29 (1) (*a*), may be made orally by a specifically designated police official, if it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must-

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(3) A magistrate or judge of the High Court may, upon an oral application made to them in terms of subsection (1) and subject to subsection (4), issue a warrant or amend a warrant as contemplated in section 29 (1) (*a*).

(4) A warrant or any amendment to a warrant may only be issued under sub-section (3)-

(*a*) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that-

(i) there are reasonable grounds to believe that a warrant or any amendment to a warrant applied for could be issued;

(ii) a warrant or an amendment to a warrant is necessary immediately in order to search for, access or seize an article-

(*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; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant or to amend a warrant; and

(*b*) on condition that the police official concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the warrant or amended warrant under subsection (3).

(5) A warrant or any amendment to a warrant issued under subsection (3) must-

(*a*) be in writing;

(*b*) be transmitted electronically to the police official or be provided to the specifically designated police official; and

(*c*) contain a summary of the facts which were considered and the grounds upon which the warrant was issued.

(6) A magistrate or judge of the High Court who has issued a warrant or amended a warrant under subsection (3) or, if unavailable, any other magistrate or judge of the High Court must, upon receipt of a written application in terms of subsection (4) (*b*), reconsider that application whereupon they may confirm, amend or cancel that warrant.

(7) A magistrate or judge of the High Court contemplated in subsection (6), who amends or cancels the warrant, must make an order they deem fit on how any article which is affected by their decision is to be dealt with.

31. Search for, access to, or seizure of article without search warrant with consent of person who has lawful authority to consent.-(1) Any police official may, without a search warrant, execute the powers referred to in section 29 (2), subject to any other law, if the person who has the lawful authority to consent to the search for, access to, or seizure of the article in question, consents, in writing, to such search, access or seizure.

(2) A police official acting in terms of subsection (1), may, subject to the lawful consent, in writing, of the person who has the lawful authority to consent, in writing authorise an investigator to assist them with the search for, access to, or seizure of the article in question.

32. Search for, access to, or seizure of article involved in the commission of an offence without search warrant.-(1) A police official may without a search warrant referred to in section 29 (1) (*a*) search any person, container, premises, vehicle, facility, ship or aircraft for the purposes of performing the powers referred to in paragraphs (*a*) and (*b*) of the definition of "seize" in respect of a computer data storage medium or any part of a computer system referred to in paragraph (*c*) or (*d*) of the definition of "article", if the police official on reasonable grounds believes-

(*a*) that a search warrant will be issued to them under section 29 (1) (*a*) if they apply for such warrant; and

(*b*) that the delay in obtaining such warrant would defeat the object of the search and seizure.

(2) A police official may only access or perform the powers referred to in paragraphs (*c*) or (*d*) of the definition of "seize", in respect of the computer data storage medium or a computer system referred to in subsection (1), in accordance with a search warrant issued in terms of section 29 (1) (*a*): Provided that a police official may, if they on reasonable grounds believe-

(*a*) that a search warrant will be issued to them under section 29 (1) (*a*) if they apply for such warrant; and

(*b*) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant,

access and perform the powers referred to in paragraph (*c*) or (*d*) of the definition of "seize" without a search warrant.

(3) An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections (1) and (2) and to access the article as contemplated in subsection (2).

33. Search for, access to, or seizure of article on arrest of person.-(1) A police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person-

(*a*) who commits any offence in terms of Part I or Part II of Chapter 2 in their presence;

(*b*) whom they reasonably suspect of having committed any offence in terms of Part I and part II of Chapter 2; or

(*c*) who is concerned with or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that they have been concerned with 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, and for which they are, under any law relating to extradition or fugitive offenders, liable to be arrested or detained in custody in the Republic.

(2) On the arrest of a person contemplated in subsection (1) or in terms of section 40 or 43 of the Criminal Procedure Act, 1977, a police official may search for and perform the powers referred to in paragraphs (*a*) and (*b*) of

the definition of "seize" in respect of a computer data storage medium or any part of a computer system referred to in paragraph (*c*) or (*d*) of the definition of "article", which is found in the possession of or in the custody or under the control of the person.

(3) A police official may only access or perform the powers referred to in paragraphs (*c*) or (*d*) of the definition of "seize", in respect of a computer data storage medium or a computer system referred to in subsection (2), in accordance with a search warrant issued in terms of section 29 (1) (*a*): Provided that a police official may, if they on reasonable grounds believe-

(*a*) that a search warrant will be issued to them under section 29 (1) (*a*), if they apply for such warrant; and

(*b*) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant,

access and perform the powers referred to in paragraph (*c*) and (*d*) of the definition of "seize" without a search warrant.

(4) An investigator authorised in writing by a police official may assist the police official to seize an article as contemplated subsections (2) and (3) and to access the article as contemplated in subsection (3).

34. Assisting police official or investigator.-(1)An electronic communications service provider, financial institution or person, other than the person who is suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a search authorised in terms of section 29 (1) must, if required, provide-

(*a*) technical assistance; and

(*b*) such other assistance as may be reasonably necessary,

to a police official or investigator in order to search for, access or seize an article.

(2) An electronic communications service provider, financial institution or person who fails to comply with the provisions of subsection (1), 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.

35. Obstructing or hindering police official or investigator and authority to overcome resistance.-(1) Any person who unlawfully and intentionally obstructs or hinders a police official or an investigator in the exercise of their powers or the performance of their duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 29 (1), 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.

(2) (*a*) A police official who may lawfully execute any power conferred upon them in terms of section 29 (2), may use such force as may be-

(i) reasonably necessary; and

(ii) proportional to all the circumstances,

relating to the execution of such powers.

(*b*) No police official may enter upon or search any premises, vehicle, facility, ship or aircraft unless they have audibly demanded admission to the premises, vehicle, facility, ship or aircraft and have notified the purpose of their entry.

(*c*) The provisions of paragraph (*b*) do not apply where the police official is, on reasonable grounds, of the opinion that an article which is the subject of the search may be destroyed, disposed of or tampered with if the provisions of paragraph (*b*) are complied with.

36. Powers conferred upon police official or investigator to be conducted in decent and orderly manner with due regard to rights of other persons.-(1) The powers conferred upon a police official or an investigator in terms of section 29 (2), 31, 32 or 33, must be conducted-

(*a*) with strict regard to decency and order; and

(*b*) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

(2) If a female needs to be searched physically in terms of section 29 (2) (*a*), (*c*) or (*d*), 32 or 33, such search must be carried out by a police official who is also a female: Provided that if no female police official is available, the search must be carried out by any female designated for that purpose by a police official.

37. Wrongful search, access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access.-(1) A police official or an investigator who unlawfully and intentionally-

(*a*) acts contrary to the authority of-

(i) a search warrant issued under section 29 (1); or

(ii) consent granted in terms of section 31 (1); or

(*b*) without being authorised thereto under this Chapter or the provision of any other law which affords similar powers to a police official or an investigator-

(i) searches for, accesses or seizes data, a computer program, a computer data storage medium or any part of a computer system; or

(ii) obtains or uses any instrument, device, password, decryption key or other information that is necessary to access data, a computer program, a computer data storage medium or any part of a computer system,

is guilty of an offence.

(2) (*a*) A police official or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 29 (2) (*h*)-

(i) must use the instrument, device, equipment, password, decryption key, data or information only in respect of and to the extent specified in the warrant to gain access to or use data, a computer program, a computer data storage medium or any part of a computer system in the manner and for the purposes specified in the search warrant concerned; and

(ii) must destroy all passwords, decryption keys, data or other information if-

(*aa*) it is not required by a person who may lawfully possess the passwords, decryption keys, data or other information;

(*bb*) it will not be required for purposes of any criminal proceedings or civil proceedings contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, or for purposes of evidence or for purposes of an order of court; or

(*cc*) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, are to be instituted in connection with such information.

(*b*) A police official or an investigator who unlawfully and intentionally-

(i) uses any instrument, device, equipment, password, decryption key, data or information outside the authorisation of a warrant as contemplated in paragraph (*a*) (i); or

(ii) fails to destroy all passwords, decryption keys, data or other information as contemplated in paragraph (*a*) (ii),

is guilty of an offence.

(3) A police official or an investigator who contravenes or fails to comply with subsection (1) or (2), is liable on conviction to a fine or imprisonment for a period not exceeding 2 years or to both a fine and such imprisonment.

(4) Where a police official or an investigator is convicted of an offence referred to in subsection (1) or (2), the court convicting such a person may, upon application of any person who has suffered damage or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context to such award.

38. False information under oath or by way of affirmation.-(1) Any person who unlawfully or intentionally gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that-

(*a*) a search warrant is issued;

(*b*) a search contemplated in section 31 took place on the basis of such information;

(*c*) a person, container, premises, vehicle, facility, ship or aircraft is searched or a computer data storage medium or any part of a computer system is seized or accessed in terms of section 32;

(*d*) an expedited preservation of data direction contemplated in section 41 is issued;

(*e*) a preservation of evidence direction contemplated in section 42 is issued; or

(*f*) a disclosure of data direction contemplated in section 44 is issued,

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(2) Where a person is convicted of an offence referred to in subsection (1), the court convicting such a person may, upon application of any person who has suffered damage or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context to such award.

39. Prohibition on disclosure of information.-(1) No person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution may, subject to subsection (2), disclose any information which they have obtained in the exercise of their powers or the performance of their duties in terms of Chapters 4 or 5 of this Act, except-

(*a*) to any other person who of necessity requires it for the performance of their functions in terms of this Act;

(*b*) if they are a person who of necessity supplies such information in the performance of their duties or functions in terms of this Act;

(*c*) if it is information which is required in terms of any law or as evidence in any court of law;

(*d*) if it constitutes information-sharing between electronic communications service providers, financial institutions, the South African Police Service, competent authorities or any other person or entity which is aimed at preventing, detecting, investigating or mitigating cybercrime: Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings; or

(*e*) to any competent authority in a foreign State which requires it for the prevention, detection, or mitigation of cybercrime, or the institution of criminal proceedings or an investigation with a view to institute criminal proceedings.

(2) The prohibition on disclosure of information contemplated in subsection (1) does not apply where the disclosure-

(*a*) is authorised in terms of this Act or any other Act of Parliament; or

(*b*) reveals a criminal activity.

(3) A person, investigator, police official, electronic communications service provider, financial institution or an employee of an electronic communications service provider or financial institution who unlawfully and intentionally contravenes the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

40. Interception of indirect communication and obtaining of real-time communication-related information.-(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;

(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.

41. Expedited preservation of data direction.-(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 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 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.

42. Preservation of evidence direction.-(1) A magistrate or judge of the High Court, may-

(*a*) upon written application by a police official;

(*b*) if it appears to the magistrate or judge upon consideration of the information provided under oath or by way of affirmation, as set out in the application, that there are reasonable grounds to believe that any person, electronic communications service provider or financial institution-

(i) may receive;

(ii) is in possession of; or

(iii) is in control of,

an article; and

(*c*) with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question,

issue a preservation of evidence direction.

(2) A preservation of evidence 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.

(3) The preservation of evidence direction must direct the person, electronic communications service provider or financial institution, from the time of service of the direction, and for the time period specified in the direction, which may not exceed 90 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,

an article in order to preserve the availability or integrity of the article.

(4) Any person, electronic communications service provider or financial institution who fails to comply with a preservation of evidence direction is guilty of an offence and 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.

(5) A person, electronic communications service provider or financial institution to whom a preservation of evidence direction referred to in subsection (1) is addressed may, in writing in the prescribed form and manner, apply to a magistrate or judge of the High Court in whose area of jurisdiction the person, electronic communications service provider or financial institution is situated 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 of the High Court 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*) inform the applicant and police official of the outcome of the application.

43. Oral application for preservation of evidence direction.-(1) A police official may orally make an application referred to in section 42 (1), if they are of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must-

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the police official, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications which may be issued by the Chief Justice in terms of section 8 (3) of the Superior Courts Act, 2013.

(3) A magistrate or judge of the High Court may, upon receipt of an oral application made to them in terms of subsection (1), issue the preservation of evidence direction applied for.

(4) A preservation of evidence direction may only be issued under subsection (3)-

(*a*) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that-

(i) there are reasonable grounds to believe that a preservation of evidence direction applied for could be issued;

(ii) a preservation of evidence direction is necessary immediately in order to ensure the availability or integrity, of the article; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of the preservation of evidence direction applied for; and

(*b*) on condition that the police official concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the preservation of evidence direction under subsection (3).

(5) A preservation of evidence direction issued under subsection (3) must be in writing and must be transmitted electronically to the police official or be provided to a specifically designated police official.

(6) A magistrate or judge of the High Court who issued a direction under subsection (3) or, if they are not available, any other magistrate or judge of the High Court must, upon receipt of a written application in terms of subsection (4) (*b*), reconsider that application whereupon they may confirm, amend or cancel that preservation of evidence direction.

44. Disclosure of data direction and search for, access to, and seizure of articles subject to preservation.-(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

(*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

(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 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) (*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.

45. Obtaining and using publicly available data or receiving data from person who is in possession of data.-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.

CHAPTER 5
MUTUAL ASSISTANCE

46. Application of provisions of Chapter.-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,

pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.

47. Spontaneous information.-(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,

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.

48. Foreign requests for assistance and cooperation.-(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 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.

(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;

(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-

(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.

49. Complying with order of designated judge.-(1) A person, electronic communications service provider or financial institution must comply with an order of the designated judge issued in terms of section 48 (6).

(2) A person, electronic communications service provider or financial institution to whom an order referred to in section 48 (6) is addressed may, in writing, apply to the designated judge for an amendment or the cancellation of the order concerned on the ground that they cannot timeously or in a reasonable fashion, comply with the order.

(3) The designated judge to whom an application is made in terms of subsection (2) 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 National Director of Public Prosecutions of the outcome of the application.

(4) A person, electronic communications service provider or financial institution who-

(*a*) fails to comply with an order referred to in section 48 (6); or

(*b*) makes a false statement in an application referred to in subsection (2),

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.

50. Informing foreign State of outcome of request for mutual assistance and expedited disclosure of traffic data.-(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 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.

51. Issuing of direction requesting assistance from foreign State.-(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-

(*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.

CHAPTER 6
DESIGNATED POINT OF CONTACT

52. Establishment and functions of designated Point of Contact.-(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

(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.

CHAPTER 7
EVIDENCE

53. Proof of certain facts by affidavit.-(1) Whenever any fact established by any examination or process requiring any skill in-

(*a*) the interpretation of data;

(*b*) the design or functioning of data, a computer program, a computer data storage medium or a computer system;

(*c*) computer science;

(*d*) electronic communications networks and technology;

(*e*) software engineering; or

(*f*) computer programming,

is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, a document purporting to be an affidavit or a solemn or attested declaration made by a person who, in that document, states that they-

(i) (*aa*) fall within a category of persons within the Republic; or

(*bb*) are in the service of a body in the Republic or a foreign State,

designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*;

(ii) possess relevant qualifications, expertise and experience which makes them competent to make the affidavit; and

(iii) have established such fact by means of an examination or process that is documented in the document,

is, upon its mere production at such proceedings, *prima facie* proof of such fact.

(2) Any person who makes an affidavit or a solemn or attested declaration under subsection (1) and who in

such affidavit or solemn or attested declaration wilfully states anything which is false, 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.

(3) The court before which an affidavit or solemn or attested declaration is produced as *prima facie* proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit or solemn or attested declaration to be subpoenaed to give oral evidence in the proceedings in question or may cause written interrogatories to be submitted to such person for reply and such interrogatories and any reply thereto purporting to be a reply from such person are likewise admissible in evidence at such proceedings.

(4) No provision of this section affects any other law under which any certificate or other document is admissible in evidence and the provisions of this section are deemed to be additional to and not in substitution of any such law.

(5) (*a*) For the purposes of subsection (1), a document purporting to be an affidavit or a solemn or attested declaration made by a person who in that affidavit alleges that they are in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the *Gazette*, has no effect unless it is-

(i) obtained in terms of an order of a competent court or on the authority of a government institution of the foreign State concerned, as the case may be; and

(ii) authenticated-

(*aa*) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(*bb*) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963.

(*b*) The admissibility and evidentiary value of an affidavit contemplated in paragraph (*a*) are not affected by the fact that the form of the oath, confirmation or attestation thereof differs from the form of the oath, confirmation or attestation prescribed in the Republic.

(*c*) A court before which an affidavit or a solemn or attested declaration contemplated in paragraph (*a*) is placed may, in order to clarify any obscurities in the said affidavit, order that a supplementary affidavit or a solemn or attested declaration be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.

CHAPTER 8
REPORTING OBLIGATIONS AND CAPACITY BUILDING

54. Obligations of electronic communications service providers and financial institutions.-(1) An electronic communications service provider or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must-

(*a*) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and

(*b*) preserve any information which may be of assistance to the South African Police Service in investigating the offence.

(2) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must by notice in the *Gazette*, prescribe-

(*a*) the category or class of offences which must be reported to the South African Police Service in terms of subsection (1); and

(*b*) the form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service.

(3) An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000.

(4) Subject to any other law or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic service provider or financial institution to-

(*a*) monitor the data which the electronic communications service provider or financial institution transmits or stores; or

(*b*) actively seek facts or circumstances indicating any unlawful activity.

(5) This section does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

55. Capacity to detect, prevent and investigate cybercrimes.-(1) The Cabinet member responsible for policing must-

(*a*) establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes;

(*b*) ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes; and

(*c*) in co-operation with any institution of higher learning, in the Republic or elsewhere, develop and implement accredited training programmes for members of the South African Police Service primarily involved with the detection, prevention and investigation of cybercrimes.

(2) The Cabinet member responsible for policing may make regulations to further regulate any aspect referred to in subsection (1).

(3) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Parliament regarding-

(*a*) progress made with the implementation of this section;

(*b*) the number of-

(i) offences provided for in Part I or Part II of Chapter 2, which were reported to the South African Police Service;

(ii) cases which were, in terms of subparagraph (i), reported to the South African Police Service which resulted in criminal prosecutions; and

(iii) cases where no criminal prosecutions were instituted after a period of 18 months after a case was, in terms of subparagraph (i), reported to the South African Police Service; and

(*c*) the number of members of the South African Police Service who received training as contemplated in subsection (1) (*b*) and (*c*).

56. National Director of Public Prosecutions must keep statistics of prosecutions.-(1) The National Director of Public Prosecutions must keep statistics of the number of prosecutions instituted for offences in terms of Part I or Part II of Chapter 2, the outcome of such prosecutions and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice.

(2) The statistics or information contemplated in subsection (1) must be included in the report of the National Director of Public Prosecutions referred to in section 22 (4) (*g*) of the National Prosecuting Authority Act, 1998.

CHAPTER 9
GENERAL PROVISIONS

57. National Executive may enter into agreements.-(1) The National Executive may enter into any agreement with any foreign State regarding-

(*a*) the provision of mutual assistance and cooperation relating to the investigation and prosecution 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 that foreign State;

(*b*) the implementation of cybercrime response activities;

(*c*) training, research, information and technology-sharing and the exchange of information on the detection, prevention, mitigation and investigation of cybercrimes;

(*d*) the establishment or designation of points of contact to facilitate the provision of mutual assistance and cooperation as contemplated in paragraph (*a*);

(*e*) the implementation of emergency cross-border response mechanisms to mitigate the effect of cybercrimes; and

(*f*) the reciprocal implementation of measures to curb cybercrime.

(2) A member of the National Executive must, as soon as practicable after Parliament has agreed to the ratification of, accession to, amendment of, or revocation of, an agreement referred to in subsection (1), give notice thereof in the *Gazette*.

58. Repeal or amendment of laws.-The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

59. Regulations.-(1) The Cabinet member responsible for the administration of justice-

(*a*) must make regulations to prescribe the-

(i) form and manner of the application as contemplated in section 20 (1);

(ii) form of the order as contemplated in section 20 (3);

(iii) manner of serving the order as contemplated in section 20 (4);

(iv) form and manner of the application as contemplated in section 20 (6);

(v) form and manner in which the court may subpoena a person as contemplated in section 20 (8);

(vi) form of the direction and affidavit and manner to furnish information to a court as contemplated in section 21 (1) (*b*);

(vii) manner of serving a direction as contemplated in section 21 (2);

(viii) manner and the form of the affidavit to apply for an extension of the time period or cancellation of the direction as contemplated in section 21 (3) (*b*);

(ix) manner for requesting additional information as contemplated in section 21 (4) (*b*);

(x) form and manner of informing an electronic communications service provider of the outcome of application as contemplated in section 21 (4) (*d*);

(xi) tariffs of compensation payable to an electronic communications service provider as contemplated in section 21 (6);

(xii) form of the order and manner of service of the order as contemplated in section 22 (3);

(xiii) form and manner of the application as contemplated in section 22 (5);

(xiv) form and manner in which the court may subpoena a person as contemplated in section 22 (7);

(xv) the form of the expedited preservation of data direction and manner of service as contemplated in section 41 (3);

(xvi) form and manner for the making of an application as contemplated in section 41 (7);

(xvii) form of the preservation of evidence direction and manner of service as contemplated in section 42 (2);

(xviii) form and manner of an application to set aside a preservation of evidence direction as contemplated in section 42 (5);

(xix) form of the disclosure of data direction and manner of service as contemplated in section 44 (3);

(xx) form and manner of an application for the amendment or setting aside of a disclosure of data direction as contemplated in section 44 (5);

(xxi) form of the affidavit as contemplated in section 44 (7) (*b*);

(xxii) manner in which traffic data must be provided to the designated Point of Contact as contemplated in section 50 (2);

(xxiii) form of the affidavit as contemplated in section 50 (2) (*b*) (ii); and

(xxiv) form of the direction as contemplated in section 51 (1); and

(*b*) may make regulations which are not inconsistent with this Act or any other law to prescribe any matter which in terms of this Act may be prescribed or which may be necessary or expedient to prescribe in order to achieve or promote the objects of this Act.

(2) (*a*) The Cabinet member responsible for policing must make regulations in terms of section 54 (2), prescribing the-

(i) category or class of offences which must be reported to the South African Police Service in terms of

section 54 (2) (*a*); and

(ii) form and manner in which an electronic communications service provider or financial institution must report offences to the South African Police Service as contemplated in section 54 (2) (*b*).

(*b*) The Cabinet member responsible for policing may make regulations to further regulate aspects contemplated in section 52 (4) and 55 (2).

60. Short title and commencement.-(1) This Act is called the Cybercrimes Act, 2020, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act.

SCHEDULE
LAWS REPEALED OR AMENDED

[Section 58.]

Number and year of law	*Short title*	*Extent of repeal or amendment*
Act No. 51 of 1977	Criminal Procedure Act, 1977	The addition of the following items to Schedule 5- "A contravention of section 8, 9 or 10 of the Cybercrimes Act, 2020- (*a*) involving amounts of more than R500 000,00; (*b*) involving amounts of more than R100 000,00, if it is proven that the offence was committed- (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed; or (*c*) if it is proven that the offence was committed by any law enforcement officer- (i) involving amounts of more than R10 000; or (ii) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (iii) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed. A contravention of section 11 (2) of the Cybercrimes Act, 2020.".
Act No. 68 of 1995	South African Police Service Act, 1995	The deletion of section 71.
Act No. 65 of 1996	Films and Publications Act, 1996	The deletion of section 24B.
Act No. 105 of 1997	Criminal Law Amendment Act, 1997	The addition of the following item to Part II of Schedule 2: "A contravention of section 8, 9 or 10 of the Cybercrimes Act, 2020- (*a*) involving amounts of more than R500 000,00;

		(*b*) involving amounts of more than R100 000,00, if it is proven that the offence was committed- (i) by a person, group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (ii) by a person or with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed; or (*c*) if it is proven that the offence was committed by any law enforcement officer- (i) involving amounts of more than R10 000; or (ii) as a member of a group of persons, syndicate or any enterprise acting in the execution or furtherance of a common purpose or conspiracy; or (iii) with the collusion or assistance of another person, who as part of his or her duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person in respect of which the offence in question was committed.".
Act No. 32 of 1998	National Prosecuting Authority Act, 1998	The deletion of sections 40A and 41 (4).
Act No. 111 of 1998	Correctional Services Act, 1998	The deletion of section 128.
Act No. 38 of 2001	Financial Intelligence Centre Act, 2001	The deletion of sections 65, 66 and 67.
Act No. 25 of 2002	Electronic Communications and Transactions Act, 2002	(*a*) The deletion of sections 85, 86, 87 and 88. (*b*) The substitution for section 89 of the following section- "**Penalties** **89.** A person convicted of an offence referred to in sections 37 (3), 40 (2), 58 (2), 80 (5) or 82 (2) is liable to a fine or imprisonment for a period not exceeding 12 months. ".
Act No. 70 of 2002	Regulation of Interception of Communications and Provision of Communication related Information Act, 2002	(*a*) The amendment of section 1 by the substitution for paragraph (*a*) of the definition of "serious offence" of the following paragraph: "(*a*) offence mentioned in Schedule 1; or". (*b*) The amendment of section 4 by the addition of the following subsection: "(3) Notwithstanding subsection (2), a law enforcement officer or a person who is authorised in terms of the Criminal Procedure Act, 1977, the Cybercrimes Act, 2020, or any other law to engage or to apprehend a suspect or to enter premises in respect of the commission or suspected commission of any offence, may during the apprehension of the suspect or during the time that he or she is lawfully on the premises, record what he or she observes or hears if- (*a*) the recording relates directly to the purpose for which the suspect was apprehended or the law enforcement officer or person entered the premises; and (*b*) the law enforcement officer or person has- (i) identified himself or herself as such; and

(ii) verbally informed any person concerned that his or her direct communications are to be recorded,

before such recording is made.".

(*c*) The substitution for subsection (4) of section 17 of the following subsection:

"(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

(*a*) a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed;

(*b*) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(*c*) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(*d*) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime, an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-

(i) accordance with an international mutual assistance agreement; or

(ii) the interests of the Republic's international relations or obligations; or

(*e*) the gathering of information concerning an offence mentioned in Schedule II, or property which is or could probably be an instrumentality of a serious offence, or is or could probably be the proceeds of unlawful activities, is necessary,

and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.".

(*d*) The substitution for subsection (4) of section 19 of the following subsection:

"(4) An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

(*a*) a serious offence or an offence mentioned in Schedule II has been or is being or will probably be committed;

(*b*) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(*c*) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(*d*) the making of a request for the provision, or the provision to the competent authorities of a

		country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime, an offence mentioned in Schedule II or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in- (i) accordance with an international mutual assistance agreement; or (ii) the interests of the Republic's international relations or obligations; or (*e*) the gathering of information concerning an offence mentioned in Schedule II, or property which is or could probably be an instrumentality of a serious offence, or is or could probably be the proceeds of unlawful activities, is necessary, and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.". (*e*) The renaming of the Schedule to the Act as "Schedule I" and the addition of the following items: "**15.** Any offence contemplated in section 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act No. 32 of 2007). **16**. Any offence contemplated in- (*a*) section 8, 9 (1) or (2) or 10, which involves an amount of R200 000, 00 or more; or (*b*) section 11 (1) or (2) or 17 (in so far as the section relates to the offences referred to in section 11 (1) or (2)), of the Cybercrimes Act, 2020).". (*f*) The addition of the following Schedule after Schedule I: "**SCHEDULE II** **1.** Any offence referred to in- (*a*) sections 3 (1), 5, 6, 7 (1), 8, 9 (1) or (2), or 10; or (*b*) section 17 (in so far as the section relates to the offences referred to in paragraph (*a*)), of the Cybercrimes Act, 2020, which involves an amount of R50 000, 00 or more. **2.** Any offence which is substantially similar to an offence referred to in item 1 which is or was committed in a foreign State, which involves an amount of R50 000, 00 or more.".
Act No. 32 of 2007	Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007	(*a*) The Index to the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, is hereby amended by- (i) the insertion of the following Part and items after item 11: "PART 3A ***Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography*** **11A.** Harmful disclosure of pornography **11B.** Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings **11C.** Electronic communications service provider to furnish particulars to court **11D.** Orders on finalisation of criminal proceedings";

(ii) the substitution for the heading to Part 2 of Chapter 3 of the following heading:

"Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, child pornography and using children for pornographic purposes or benefiting from child pornography"; and

(iii) the insertion after item 19 of the following item:

"**19A.** Offences relating to child pornography".

(*b*) The amendment of section 1-

(i) by the insertion, after the definition of "Director of Public Prosecutions", of the following definitions:

" '**disclose**' and **'disclosure',** in relation to the harmful disclosure of pornography contemplated in section 11A, includes-

(*a*) to send the pornography to a person who is the intended recipient of the electronic communication or any other person;

(*b*) to store the pornography on an electronic communications network, where the pornography can be viewed, copied or downloaded; or

(*c*) to send or otherwise make available to a person, a link to the pornography that has been stored on an electronic communication network, where the pornography can be viewed, copied or downloaded;

'Electronic Communications Act' means the Electronic Communications Act, 2005 (Act No. 36 of 2005);

'electronic communications identity number' means a technical identification label which represents the origin or destination of electronic communications traffic;

'electronic communications network' means an 'electronic communications network' as defined in section 1 of the Electronic Communications Act, 2005, and includes a computer system;

'**electronic communications service'** means any service which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services as defined in section 1 of the Electronic Communications Act, 2005;

'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 licensed or exempted from being licensed as such in terms of 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;"; and

(ii) by the insertion, after the definition of "genital organs" of the following definitions:

" **'host'** means to store information on an electronic communications network that is used to provide an electronic communications service, where it can be viewed, copied or downloaded;

'live performance involving child pornography' means an event where a child is used to create, make or produce child pornography;".

(*c*) The following Part and sections are hereby inserted in Chapter 2 after section 11:

"PART 3A

Persons 18 years or older: Harmful disclosure of pornography and orders to protect complainant against the harmful effects of disclosure of pornography

Harmful disclosure of pornography

11A. (1) A person ("A") who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person ("B") appears or is described and such disclosure-

(*a*) takes place without the consent of B; and

(*b*) causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B,

is guilty of the offence of harmful disclosure of pornography.

(2) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1) (*b*), is guilty of the offence of threatening to disclose pornography that will cause harm.

(3) A person ("A") who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.

Orders to protect complainant against harmful disclosure of pornography pending finalisation of criminal proceedings

11B. (1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 11A (1), (2) or (3) has allegedly been committed against him or her, may on an *ex parte basis* in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to-

(*a*) prohibit any person to disclose, or cause the disclosure or threaten the applicant with the disclosure or

causing the disclosure of pornography which relates to the charge; or

(*b*) order an electronic communications service provider whose electronic communications service is used to host or disclose the pornography which relates to the charge, to remove or disable access to such pornography.

(2) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (1) and may, for that purpose consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(3) If the court is satisfied that there-

(*a*) is *prima facie* evidence that an offence referred to in section 11A (1), (2) or (3), has allegedly been committed against the applicant; and

(*b*) are reasonable grounds to believe that a person referred to in subsection (1) (*a*), disclosed or caused the disclosure or threatened the applicant with the disclosure or causing the disclosure of such pornography; or

(*c*) are reasonable grounds to believe that the electronic communications service of the electronic communications service provider referred to in subsection (1) (*b*), is used to host or disclose such pornography,

the court may, subject to such conditions as the court may deem fit, issue the order referred to in subsection (1), in the prescribed form.

(4) The order, referred to in subsection (3), must be served on the person referred to in subsection (1) (*a*) or electronic communications service provider referred to in subsection (1) (*b*), in the prescribed manner: Provided, that if the court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(5) An order referred to in subsection (3) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1) (*a*) or electronic communications service provider referred to in subsection (1) (*b*).

(6) A person referred to in subsection (1) (*a*), other than the person who is accused of having committed the offence in question, or an electronic communications service provider, referred to in subsection (1) (*b*) may, within 14 days after the order has been served on him, her or it in terms of subsection (4) or within such further period as the court may allow, upon notice to the magistrate's court concerned, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (3).

(7) (*a*) The court must as soon as is reasonably possible consider an application

submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(*b*) The court may if good cause has been shown for the variation or setting aside of the protection order, issue an order to this effect.

(8) The court may, for purposes of subsections (2) and (7), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(9) A person referred to in subsection (1) (*a*) or electronic communications service provider referred to in subsection (1) (*b*), that fails to comply with an order referred to in subsection (3) or any variation thereof, is guilty of an offence.

(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to-

(*a*) attend or to remain in attendance;

(*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(*c*) remain in attendance at those proceedings as so adjourned; or

(*d*) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(11) The provisions in respect of appeal and review as provided for in the Magistrates' Courts Act, 1944, and the Superior Courts Act, 2013, apply to proceedings in terms of this section.

(12) Sections 8 and 9 (3) of the Protection from Harassment Act, 2011 (Act No. 17 of 2011), apply with the necessary changes required by the context to proceedings contemplated in subsections (2) and (7).

Electronic communications service provider to furnish particulars to court

11C. (1) If an application for a protection order is made in terms of section 11B (1) and the court is satisfied in terms of section 11B (3) that a protection order must be issued and the particulars of the person referred to in section 11B (1) (*a*), or the electronic communications service provider referred to in section 11B (1) (*b*), whose service is used to host or disclose such pornography, is not known, the court may-

(*a*) adjourn the proceedings to any time and date on the terms and conditions which the court deems appropriate; and

(*b*) issue a direction in the prescribed form, directing an electronic communications service provider, that is believed to be able to furnish such particulars, to furnish the court in the prescribed manner by means of an affidavit in the prescribed form with-

(i) the electronic communications identity number from where such

pornography originated;

(ii) the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned;

(iii) any information which indicates that such pornography was or was not sent from the electronic communications identity number of the person to the electronic communications identity number of the applicant;

(iv) any information that is available to an electronic communications service provider that may be of assistance to the court to identify the person referred to in section 11B (1) (*a*) or the electronic communications service provider referred to in section 11B (1) (*b*), which provides a service to that person;

(v) any information that is available to an electronic communications service provider which-

(*aa*) confirms whether or not its electronic communications service is used to host or was or is used to disclose such pornography; or

(*bb*) may be of assistance to the court to identify the electronic communications service provider whose service is used to host or was or is used disclose such pornography; and

(vi) an assessment whether or not the electronic communications service provider is in a position to-

(*aa*) remove such pornography or a link to such pornography; or

(*bb*) disable access to such pornography or a link to such pornography.

(2) If the court issues a direction in terms of subsection (1) (*b*) the court must direct that the direction be served on the electronic communications service provider in the prescribed manner: Provided, that if the court is satisfied that the direction cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(3) (*a*) The information referred to in subsection (1) (*b*) must be provided to the court within five ordinary court days from the time that the direction is served on an electronic communications service provider.

(*b*) An electronic communications service provider on which a direction is served, may in the prescribed manner by means of an affidavit in the prescribed form apply to the court for-

(i) an extension of the period of five ordinary court days referred to in

paragraph (*a*) for a further period of five ordinary court days on the grounds that the information cannot be provided timeously; or

(ii) the cancellation of the direction on the grounds that-

(*aa*) it does not provide an electronic communications service to the applicant or the person referred to in section 11B (1) (*a*);

(*bb*) the requested information is not available in the records of the electronic communications service provider; or

(*cc*) its service is not used to host or was or is not used to disclose such pornography.

(4) After receipt of an application in terms of subsection (3) (*b*), the court-

(*a*) must consider the application;

(*b*) may, in the prescribed manner, request such additional evidence by way of affidavit from the electronic communications service provider as it deems fit;

(*c*) must give a decision in respect thereof; and

(*d*) must inform the electronic communications service provider in the prescribed form and manner of the outcome of the application.

(5) (*a*) The court may, on receipt of an affidavit from an electronic communications service provider which contains the information referred to in subsection (1) (*b*), consider the issuing of a protection order in terms of section 11B (3) against the person or electronic communications service provider on the date to which the proceedings have been adjourned.

(*b*) Any information furnished to the court in terms of subsection (1) (*b*) forms part of the evidence that a court may consider in terms of section 11B (3).

(6) The Cabinet member responsible for the administration of justice may, by notice in the *Gazette*, prescribe reasonable tariffs of compensation payable to electronic communications service providers for providing the information referred to in subsection (1) (*b*).

(7) Any electronic communications service provider or employee of an electronic communications service provider who-

(*a*) fails to furnish the required information within five ordinary court days from the time that the direction is served on such electronic communications service provider to a court in terms of subsection (3) (*a*) or such extended period allowed by the court in terms of subsection (3) (*b*); or

(*b*) makes a false statement in an affidavit referred to in subsection (1) (*b*) or (3) (*b*) in a material respect,

is guilty of an offence.

Orders on finalisation of criminal proceedings

11D. (1) The trial court, on convicting a

person of any offence referred to in section 11A (1), (2) or (3), must order-

(*a*) that person to destroy the pornography and to submit an affidavit in the prescribed form to the prosecutor identified in the order, that the pornography has been so destroyed; or

(*b*) an electronic communications service provider whose service is used to host or disclose such pornography to remove or disable access to such pornography.

(2) The order referred to in subsection (1) (*b*), must be in the prescribed form and must be served on the electronic communications service provider in the prescribed manner: Provided, that if the trial court is satisfied that the order cannot be served in the prescribed manner, the court may make an order allowing service to be effected in the form or manner specified in that order.

(3) Any person or electronic communications service provider who fails to comply with an order referred to in subsection (1) is guilty of an offence.

(4) An electronic communications service provider may, within 14 days after the order referred to in subsection (1) (*b*) has been served on it in terms of subsection (2), upon notice to the trial court concerned, in the prescribed form and manner, apply to the trial court for the setting aside or amendment of the order.

(5) (*a*) The trial court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (4) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings.

(*b*) The trial court may if good cause has been shown for the variation or setting aside of the order, issue an order to this effect.

(6) The trial court may, for purposes of subsections (5) (*a*), in the prescribed form and manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just decision of the case.

(7) Any person who is subpoenaed in terms of subsection (6) to attend proceedings and who fails to-

(*a*) attend or to remain in attendance;

(*b*) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(*c*) remain in attendance at those proceedings as so adjourned; or

(*d*) produce any book, document or object specified in the subpoena,

is guilty of an offence.

(8) For purposes of this section **"trial court"** means-

(*a*) a magistrate's court established under section 2 (1) (*f*) (i) of the Magistrates'

Courts Act, 1944;

(*b*) a court for a regional division established under section 2 (1) (*g*) (i) of the Magistrates' Courts Act, 1944; or

(*c*) a High Court referred to in section 6 (1) of the Superior Courts Act, 2013.

(9) Whenever a person is convicted of an offence referred to in section 11A (1), (2) or (3), the trial court must issue an order that the person so convicted must reimburse all expenses reasonably incurred by-

(*a*) a complainant as a result of any direction issued in terms of section 11C (1) (*b*); or

(*b*) an electronic communications service provider to remove or disable access to such pornography,

whereupon the provisions of section 300 of the Criminal Procedure Act, 1977, shall apply with the necessary changes required by the context, to such order.".

(*d*) Chapter 3 is hereby amended-

(i) by the substitution for the heading to Part 2 of Chapter 3 of the following heading:

"***Sexual exploitation and sexual grooming of children, exposure or display of or causing exposure or display of child pornography or pornography to children, offences relating to child pornography and using children for pornographic purposes or benefiting from child pornography***";

(ii) by the addition to section 17 of the following subsection:

"(7) Any person who unlawfully and intentionally in any manner advocates, advertises, encourages or promotes the sexual exploitation of a child, is guilty of an offence.".

(iii) by the insertion of the following section after section 19:

" **Offences relating to child pornography**

19A. (1) Any person who unlawfully and intentionally creates, makes or produces child pornography in any manner, other than by using a child for child pornography as contemplated in section 20 (1), is guilty of an offence.

(2) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the creation, making or production of child pornography, is guilty of an offence.

(3) Any person who unlawfully and intentionally possesses child pornography, is guilty of an offence.

(4) Any person who unlawfully and intentionally, in any manner-

(*a*) distributes;

(*b*) makes available;

(*c*) transmits;

(*d*) offers for sale;

(*e*) sells;

(*f*) offers to procure;

(*g*) procures;

(*h*) accesses;

(*i*) downloads; or

(*j*) views,

child pornography, is guilty of an offence.

(5) Any person who unlawfully and intentionally, in any manner assists in, or facilitates the-

(*a*) distribution;

(*b*) making available;

(*c*) transmission;

(*d*) offering for sale;

(*e*) selling;

(*f*) offering to procure;

(*g*) procuring;

(*h*) accessing;

(*i*) downloading; or

(*j*) viewing,

of child pornography, is guilty of an offence.

(6) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate a contravention of subsections (1) to (5), is guilty of an offence."; and

(iv) by the addition to section 20 of the following subsections:

"(3) Any person who unlawfully and intentionally-

(*a*) attends;

(*b*) views; or

(*c*) participates in,

a live performance involving child pornography, is guilty of the offence of attending, viewing or participating in, a performance involving child pornography.

(4) Any person ("A") who unlawfully and intentionally recruits a child complainant ("B"), with or without the consent of B, whether for financial or other reward, favour or compensation to B or a third person ("C") or not, for purposes of-

(*a*) creating, making or producing of child pornography, is guilty of the offence of recruiting a child for child pornography; or

(*b*) participating in a live performance involving child pornography, as contemplated in subsection (3), is guilty of the offence of recruiting a child for participating in a live performance involving child pornography.".

(*e*) Section 54 of the Act is amended by the addition of the following subsections:

"(3) Any person who, having knowledge of the commission of any offence referred to in section 19A, or having reason to suspect that such an offence has been or is being or will probably be committed and unlawfully and intentionally fails to-

(*a*) report such knowledge or suspicion as soon as possible to the South African Police Service; or

(*b*) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,

is guilty of an offence.

(4) An electronic communications service provider that is aware or becomes aware that

its electronic communications service or electronic communications network is used or involved in the commission of any offence provided for in section 19A, must-

(*a*) immediately report the offence to the South African Police Service;

(*b*) preserve any information which may be of assistance to the South African Police Service in investigating the offence; and

(*c*) take all reasonable steps to prevent access to the child pornography by any person.".

(*f*) Section 56A of the Act is amended by the addition of the following subsections:

"(3) (*a*) Any person who contravenes the provisions of section 11A (1) or (2), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(*b*) Any person who contravenes the provisions of section 11A (3), is liable, on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(*c*) Any person or electronic communications service provider that is convicted of an offence referred to in section 11B (9) or (10), is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*d*) Any person or electronic communications service provider that is convicted of an offence referred to in section 11C (7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*e*) Any electronic communications service provider or person that is convicted of an offence referred to in section 11D (3) or (7), is liable, on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(4) Any person who contravenes the provisions of section 19A (3), (4) (*f*), (*g*), (*h*), (*i*) or (*j*), or (5) (*f*), (*g*), (*h*), (*i*) or (*j*) is liable-

(*a*) in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment;

(*b*) in the case of a second conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or

(*c*) in the case of a third or subsequent conviction, to a fine or to imprisonment for a period not exceeding 15 years or to both such fine and imprisonment.

(5) Any person who contravenes the provisions of section 17 (7), 19A (1), (2), (4) (*a*), (*b*), (*c*), (*d*), or (*e*), (5) (*a*), (*b*), (*c*), (*d*) or (*e*) or 20 (3) or (4), is liable-

(*a*) in the case of a first conviction, to a fine or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment; or

(*b*) in the case of a second and subsequent conviction, to a fine or to imprisonment for a period not

		exceeding 15 years or to both such fine and imprisonment. (6) Any person who contravenes the provisions of section 19A (6), is liable- (*a*) in the case of a first conviction, to a fine of R1 000 000 or to imprisonment for a period not exceeding 5 years, or to both such fine and imprisonment; or (*b*) in the case of a second or subsequent conviction, to a fine of R 2 000 000 or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment. (7) Any person who contravenes the provisions of section 54 (3), is liable, on conviction to a fine or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment. (8) Any electronic communications service provider who contravenes the provisions of section 54 (4), is liable, on conviction to a fine not exceeding R1 000 000 or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.".
Act No. 75 of 2008	Child Justice Act, 2008	(*a*) The addition of the following item to Schedule 2: **"26.** Any offence contemplated in- (*a*) section 2, 3 or 4 of the Cybercrimes Act, 2020; (*b*) section 5, 6, 7 or 11 (1) of the Cybercrimes Act, 2020, where the damage caused does not exceed an amount of R5000; (*c*) section 14, 15 or 16 of the Cybercrimes Act, 2020; or (*d*) section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved does not exceed R1500. **27.** An offence contemplated in section 11A (1) and (2) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007.". (*b*) The addition of the following item to Schedule 3: **"23.** Any offence contemplated in- (*a*) section 5, 6, 7 or 11 (1) of the Cybercrimes Act, 2020, where the damage caused exceeds an amount of R5000; (*b*) section 8, 9 or 10 of the Cybercrimes Act, 2020, where the amount involved exceeds R1500; or (*c*) section 11 (2) of the Cybercrimes Act, 2020. **24.** An offence contemplated in section 11A (3) of Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007."

GNR.1311 of 5 November 1999: Regulations under the Domestic Violence Act, 1998 (Act No. 116 of 1998)

DEPARTMENT OF JUSTICE

The Minister of Justice has under section 19 of the Domestic Violence Act, 1998 (Act No. 116 of 1998), made the regulations in the Schedule.

SCHEDULE

ARRANGEMENT OF REGULATIONS

1. Definitions.-In these regulations any word or expression to which a meaning has been assigned in the Act shall have that meaning and, unless the context otherwise indicates**-**

"the Act" means the Domestic Violence Act, 1998 (Act No. 116 of 1998).

2. Notice containing information.-The notice contemplated in section 2 (*b*) of the Act must contain the information provided for in Form 1 of the Annexure.

3. Explanation of notice.-For purposes of section 2 (*c*) of the Act a member of the South African Police Service must-

(*a*) explain to the complainant-

(i) that a member of the South African Police Service will render such assistance as circumstances may require, including assisting or making arrangements to find a suitable shelter and to obtain medical treatment;

(ii) his or her right to apply for a protection order to prohibit the respondent from committing further acts of domestic violence, even if no criminal complaint has been lodged, so as to ensure his or her safety, health and well-being;

(iii) his or her right to lodge a criminal complaint; and

(iv) the purpose of the notice;

(*b*) if the complainant is unable to read the notice, read the notice referred to in regulation 2 to the complainant, or take such reasonable steps as may be necessary to have the notice read to the complainant;

(*c*) inquire from the complainant whether he or she-

(i) understands the contents of the notice; and

(ii) requires further information regarding his or her remedies in terms of the Act and the right to lodge a criminal complaint;

(*d*) explain, to the best of his or her ability, to the complainant on request-

(i) any part of the notice which the complainant does not understand; and

(ii) his or her remedies in terms of the Act and the right to lodge a criminal complaint; and

(*e*) inform the complainant to obtain further information from the clerk of the magistrate's court should questions of the complainant remain unanswered.

4. Manner of application for protection order.-(1) A complainant may apply to the court for a protection order in a form substantially corresponding to Form 2 of the Annexure.

(2) The application referred to in subregulation (1) must be made by way of an affidavit in which must be stated-

(*a*) the facts on which the application is based;

(*b*) the nature of the order applied for; and

(*c*) the name of the police station where the complainant is likely to report any breach of the protection order applied for.

(3) Where the application is brought on behalf of a complainant by another person, the affidavit referred to in subregulation (2) must also set out or contain-

(*a*) the grounds on which such person has a material interest in the wellbeing of the complainant;

(*b*) the occupation of such person and capacity in which such person brings the application; and

(*c*) except in cases excluded by the provisions of paragraphs (*a*) to (*b*) of section 4 (3) of the Act, the written consent of the complainant.

5. Information to be given by clerk of the court.-(1) For purposes of section 4 (2) of the Act, the clerk of the court must, if the complainant is not represented by a legal representative-

(*a*) hand to the complainant a written notice which contains the information provided for in Form 3 of the Annexure, which must, if reasonably possible, be in the official language of the complainant's choice;

(*b*) read the notice or cause the notice to be read to the complainant, if the complainant is unable to read the notice;

(*c*) inquire from the complainant whether he or she-

(i) understands the contents of the notice; and

(ii) requires further information concerning the relief available in terms of the Act and the right to lodge a criminal complaint; and

(*d*) on request of the complainant, further explain, to the best of his or her ability

(i) any part of the notice which the complainant does not understand; and

(ii) the relief available in terms of the Act and the right to lodge a criminal complaint.

6. Issuing of interim protection order.-An interim protection order contemplated in section 5 (2) of the Act must be in the form of Form 4 of the Annexure.

7. Notice to show cause.-The notice calling on the respondent to show cause on the specified return date why a protection order should not be issued, contemplated in section 5 (4) of the Act, must be in the form of Form 5 of the Annexure.

8. Issuing of protection order.-A protection order contemplated in section 6 (1) of the Act must be-

(*a*) in the event that an interim protection order was issued, in the form of Form 6 of the Annexure; or

(*b*) in the event that an interim protection order was not issued, in the form of Form 7 of the Annexure.

9. Issuing of warrant of arrest.-The warrant of arrest contemplated in section 8 (1) (*a*) of the Act must be authorised and issued in the form of Form 8 of the Annexure.

10. Affidavit for further warrant of arrest.-An affidavit contemplated in section 8 (3) of the Act for purposes of obtaining a second or further warrant of arrest must be in a form substantially corresponding to Form 9 of the Annexure.

11. Affidavit regarding contravention of protection order.-An affidavit contemplated in section 8 (4) (*a*) of the Act in which it is stated that the respondent has contravened any prohibition, condition, obligation or order contained in a protection order must be in a form substantially corresponding to Form 10 of the Annexure.

12. Written notice to respondent to appear before court.-(1) The written notice contemplated in section 8 (4) (*c*) of the Act calling on the respondent to appear before a court on a charge of committing the offence referred to in section 17 (*a*) of the Act must be in a form substantially corresponding to Form 11 of the Annexure.

(2) Any respondent who is called upon to appear before the court in accordance with a written notice referred to in subregulation (1) and who fails to-

(*a*) appear at the place and on the date and time specified in that notice; or

(*b*) remain in attendance at the proceedings, shall be guilty of an offence and liable to the punishment prescribed under subregulation (3) (*b*).

(3) (*a*) The court may if satisfied from the duplicate original of the notice referred to in section 8 (4) (*d*) of the Act that the notice was handed to the respondent and that the respondent has failed to appear at the place and on the date and time specified in the notice, or if satisfied that the respondent has failed to remain in attendance at the proceedings concerned, issue a warrant for the respondent's arrest.

(*b*) The court may when the respondent is brought before it, in a summary manner enquire into his or her failure so to appear or to remain in attendance and unless the respondent satisfies the court that his or her failure was not due to any fault on his or her part, convict him or her of the offence referred to in subregulation (2) and sentence him or her to a fine or to imprisonment for a period not exceeding six months.

13. Application for variation or setting aside of protection order.-An application for the variation or setting aside of a protection order, contemplated in section 10 (1) of the Act, must be made in a form substantially corresponding to Form 12 of the Annexure.

14. Notice of variation or setting aside of protection order.-(1) The notice of the variation or setting aside of a protection order, contemplated in section 10 (3) of the Act, must be in the form of Form 13 of the Annexure.

(2) The notice referred to in subregulation (1) must be forwarded by the clerk of the court to the complainant and respondent by handing it to them personally or sending it to them by registered mail.

15. Service of documents.-(1) Service of any document in terms of the Act or these regulations, except where the Act or regulations provide otherwise, must without delay be effected by-

(*a*) the clerk of the court by handing or presenting for handing over a certified copy of the document to the person on whom the document is to be served or sending a certified copy of the document to that person by registered mail and endorsing the original document to this effect;

(*b*) the sheriff in terms of the provisions of the Magistrate's Courts Act, 1944 (Act No. 32 of 1944), and Rules published in terms of section 6 of the Rules Board for Courts of Law Act, 1985 (Act No. 107 of 1985); or

(*c*) a peace officer in terms of the provisions of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), relating to the service of subpoenas.

(2) The clerk of the court sending a copy of the document in terms of subregulation (1) (*a*) to the person on whom the document is to be served, must require that proof of receipt thereof be returned to him or her by the relevant postal authority.

(3) A person authorised to effect service in terms of subregulation (1), who is not a member of the South African Police Service, may, in any case where resistance to the service of a document is encountered or is reasonably anticipated, request a member of the South African Police Service to assist him or her with the service of any document provided for in the Act and these regulations.

(4) The complainant or respondent who requires a document to be served in terms of the Act or these regulations shall be responsible for the costs of such service: Provided that the clerk of the court may, after consideration of such proof as he or she may require, direct that the State must be responsible for the costs of any service in terms of the Act or these regulations if he or she is satisfied that the complainant or respondent as the case may be, or both the complainant and respondent, do not have the means to pay for such costs at the time

when service is required.

16. Short title.-These regulations shall be called the Domestic Violence Regulations, 1999, and shall come into operation on 15 December 1999.

Annexure

Form 1
NOTICE TO COMPLAINANT IN A CASE OF DOMESTIC VIOLENCE

[Regulation 2]

SECTION 2 (*b*) OF THE DOMESTIC VIOLENCE ACT, 1998 (ACT NO. 116 OF 1998)

This notice explains your rights and the steps you may take to protect yourself, your children and/or other members of the shared household. If, after reading this notice, there is anything you do not understand I will to the best of my ability explain the contents to you. If I or other members of the South African Police Service present are unable to answer any of your questions regarding this notice, you may contact the clerk of the magistrate's court for further information.

1. I, as a member of the South African Police Service will render such assistance to you as you may require in the circumstances including assisting or making arrangements to-
   - find a suitable shelter; and/or
   - get medical treatment.
2. You may lay a criminal complaint against the person who committed the act of domestic violence (who will now be called the respondent) if the conduct of the respondent constitutes a criminal offence which will be investigated by the police.
3. In addition, you may apply, on any day and at any time, for a protection order at the Magistrate's Court in whose area-
   - you reside, carry on business or are employed, permanently or temporarily;
   - the respondent resides, carries on business or is employed; or
   - the act of domestic violence occurred.
4. I will provide you with an application form if you want to apply for such an order. It is not necessary to lay a criminal charge in order to obtain a protection order.
5. The Court will consider your application and may thereafter issue a temporary order which will-
   - only come into effect after it has been delivered to the respondent (the cost of which you have to pay unless you do not have the means to pay therefor); and
   - be valid for a certain period of time.
6. After such period of time the court will consider to issue a permanent order.
7. In your application you may request the court to prohibit the respondent from-
   - committing any act of domestic violence;
   - getting the help of another to commit any act of domestic violence;
   - entering your workplace, home or the shared residence or any part thereof;
   - preventing you or any child who normally lives in the shared residence from entering or remaining in the residence or any part thereof;
   - committing any other act determined by the court.
8. You may request the court not to disclose your physical address to the respondent. The court may also, in order to protect you and to provide for your safety, health and well-being-
   - order that the respondent pay rent, mortgage or other monetary relief (such as medical expenses and loss of income);
   - refuse the respondent contact with your children;
   - order the seizure of any arm or dangerous weapon in the possession or under the control of the respondent;
   - order that a peace officer accompany you to assist you with the collection of your personal property;
   - impose any other condition it deems reasonably necessary.
9. The court will, when an order is made, issue a warrant of arrest for the respondent. This means that the respondent may be arrested if he or she fails to comply with any provision of the protection order and after you have given the police the warrant and an affidavit explaining that the respondent has breached the order.

WARNING: It is a criminal offence if you knowingly give false information when applying for

a protection order or when laying a criminal charge, you will be prosecuted and may be convicted.

Form 2
APPLICATION FOR PROTECTION ORDER

[Regulation 4]

SECTION 4 (1) OF THE DOMESTIC VIOLENCE ACT, 1998 (ACT NO. 116 OF 1998)

PART A: APPLICATION (To be completed by applicant)

1. PARTICULARS OF COMPLAINANT (Victim of domestic violence)

Surname:	
Full names:	
Id. No/Date of birth:	
Home or temporary address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	
Nature of domestic relationship with person who committed the act of domestic violence (Respondent):	
Occupation:	

2. PARTICULARS OF PERSON MAKING THE APPLICATION ON BEHALF OF THE COMPLAINANT (if applicable)

Surname:	
Full names:	
Id. No/Date of birth:	
Home address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	
Occupation:	
Capacity in which application is made:	
Nature of relationship with the complainant:	
State reason(s) why application is made on behalf of the complainant:	
Indicate whether written consent of complainant has been obtained: (*Delete whichever is not applicable*)	Written consent *has been obtained and is attached/is not necessary since the complainant is- Ø a minor (under the age of 21 years); Ø mentally retarded; Ø unconscious; Ø unable to provide consent because

3. PARTICULARS OF PERSON WHO COMMITTED ACT OF DOMESTIC VIOLENCE

(hereafter called the Respondent) - in so far as such particulars are available

Surname:	
Full names:	
Id. No/Date of birth:	
Home address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	
Occupation:	

4. PERSONS AFFECTED BY DOMESTIC VIOLENCE

4.1 Particulars of children and adults sharing the residence:

Name:	Age:	Relationship to complainant

4.2 How are these persons affected?

4.3 Do any of these persons suffer disabilities? If so give details:

5. INFORMATION REGARDING ACTS OF DOMESTIC VIOLENCE

Give full details regarding all incidents of domestic violence and also indicate whether firearms or other dangerous weapons were used, what injuries have been sustained and whether medical treatment was obtained:

6. INFORMATION REGARDING URGENCY OF APPLICATION

Submit the reasons why the Court has to consider the application as a matter of

urgency and why undue hardship may be suffered if the application is not dealt with immediately

7. TERMS OF PROTECTION ORDER

It is requested that the Respondent must be ordered (mark appropriate box and complete where necessary):

(*a*)	Not to commit any act of domestic violence	
(*b*)	Not to get the help of another person to commit any act of domestic violence	
(*c*)	Not to enter the shared residence, situated at	
(*d*)	Not to enter a specified part of the shared residence, namely	
(*e*)	Not to enter the Complainant's residence, situated at	
(*f*)	Not to enter the Complainant's place of employment, namely	
(*g*)	Not to prevent the Complainant or any child who ordinarily live(s) or lived in the shared residence from entering or remaining in the shared residence or any part thereof, to wit	
(*h*)	Not to commit any other act, namely	

8. ADDITIONAL CONDITIONS

It is also requested that the Court must order that (mark appropriate box and complete where necessary):

(*a*)	A peace officer, namely, is to accompany the Complainant to assist with arrangements regarding the collection of the Complainant's personal property set out in paragraph 9, below.	
(*b*)	A member of the South African Police Service is to seize the following arm(s) or dangerous weapon(s) in the possession of the Respondent:	
(*c*)	The Respondent is to pay the following rent or mortgage payments:	
(*d*)	The Respondent is to pay the following emergency monetary relief:	
(*e*)	The Respondent is refused any contact with the following child or children:	
(*f*)	The Respondent is granted the following contact with the above-mentioned child or children:	
(*g*)	The physical address of the Complainant's residence not be disclosed to the Respondent	
(*i*)	Other conditions requested:	

(Editor's Note: Paragraph (*h*) omitted from GNR.1311 of 1999.)

9. PERSONAL PROPERTY

Property description:	Grounds on which property is considered to be personal property:	Address where property is kept:

10. I am likely to report a breach of the Protection Order at the

Police Station.

DEPONENT
(Person who applies for order)

DATE

PART B: CERTIFICATION (for official use)

11. I hereby certify that before administering the *oath/taking the affirmation I asked the Deponent the following questions and noted *her/his answers in *her/his presence as indicated below:

(*a*) Do you know and understand the contents of the above declaration?

Answer

(*b*) Do you have any objection to taking the prescribed oath?

Answer

(*c*) Do you consider the prescribed oath to be binding on your conscience?

Answer

I hereby certify that the Deponent has acknowledged that *she/he knows and understands the contents of this declaration which was *sworn to/affirmed before me, and the Deponent's *signature/thumb print/mark was placed thereon in my presence.

Dated at this day of 20

Justice of the Peace/Commissioner of Oaths

Full names

Designation

Area for which appointed

Business address

* Delete whichever is not applicable

Form 3
INFORMATION NOTICE TO COMPLAINANT

[Regulation 5]

SECTION 4 (2) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT 116 NO. OF 1998)

1. You may lay a criminal complaint against the person who committed the act of domestic violence (hereafter called the respondent) if the conduct of the respondent constitutes a criminal offence which will be investigated by the police.
2. You may apply, on any day and at any time, for a protection order at the Magistrate's Court in whose area-
   . you reside, carry on business or are employed, permanently or temporarily;
   . the respondent resides, carries on business or is employed;
   . the act of domestic violence occurred.
3. I am able to provide you with an application form if you want to apply for such an order. It is not necessary to lay a criminal charge in order to obtain a protection order.
4. The Court will consider your application and may thereafter issue a temporary order which will-
   . only come into effect after it has been delivered to the respondent (the cost of which you will have to pay unless you do not have the means to pay therefor); and
   . be valid for a certain period of time.
5. After such period of time the Court will consider to issue a permanent order.
6. In your application you may request the Court to prohibit the respondent from-
   . committing any act of domestic violence;
   . enlisting the help of another to commit any act of domestic violence;
   . entering your home or the shared residence or any part thereof;
   . entering a specified part of the shared residence;

- entering your workplace;
- preventing you or any child who normally lives in the shared residence from entering or remaining in the residence or any part thereof;
- committing any other act determined by the Court.

7. You may request the Court not to disclose your address to the respondent. The Court may also, in order to protect you and to provide for your safety, health and well-being-
   - order that the respondent pay rent, mortgage or other monetary relief (such as loss of earnings and medical expenses);
   - refuse the respondent contact with your children;
   - order the seizure of any arm or dangerous weapon in the possession or under the control of the respondent;
   - order that a peace officer accompany you to assist you with the collection of your personal property; and
   - impose any other condition it deems reasonably necessary.
8. The Court will, when an order is made, issue a warrant of arrest for the respondent, which means that the respondent may be arrested if he or she fails to comply with any provision of the protection order.

WARNING: It is a criminal offence if you should knowingly make a false allegation against the respondent in an affidavit.

Form 4
INTERIM PROTECTION ORDER

[Regulation 6]

SECTION 5 (2) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF

HELD AT APPLICATION NO.

In the matter between:

APPLICANT:
(*Id. No./Date of Birth:)

AND

RESPONDENT:
(*Id. No./Date of Birth:)

1. PARTICULARS OF RESPONDENT

Home address:

(Tel. No.)

Work address:

(Tel. No.)

Occupation:

2. PARTICULARS OF APPLICATION

The Applicant has applied for a Protection Order against the **Respondent** as per the affidavit(s) and record of oral evidence (if any) attached, which application has been considered by the Court.

3. ORDER BY COURT AND PARTICULARS OF ORDER

3.1 The Court orders that:

3.1.1 *The application for a Protection Order is dismissed; or

3.1.2 *An Interim Protection Order is granted; and the Respondent is ordered-

3.1.2.1 *not to commit the following act(s) of domestic violence

;

3.1.2.2 *not to enlist the help of another person to commit the acts of domestic violence specified in paragraph 3.1.2.1;

3.1.2.3 *not to enter the shared residence at
;

3.1.2.4 *not to enter the following parts of the shared residence
at

3.1.2.5 *not to enter the Complainant's residence at
;

3.1.2.6 *not to enter the Complainant's place of employment at
;

3.1.2.7 *not to prevent the Complainant or any child who ordinarily live(s) or lived in the shared residence at
from entering or remaining in the shared residence, or any part thereof;

3.1.2.8 *not to commit any of the following acts, to wit ;

3.1.2.9 *to make rent or mortgage payments in the sum of R per month/ annum;

3.1.2.10 *to pay the sum of R to the Complainant as emergency monetary relief.

4. ADDITIONAL ORDERS

4.1 It is further ordered that:

4.1.1 *A peace officer, namely , accompanies the Applicant to the following residence in order to assist with arrangements regarding the collection of personal property, i.e.
;

4.1.2 *A member of the South African Police Service at
seizes the following arm(s) or dangerous weapon(s) in the possession of the Respondent, i.e.
;

4.1.3 *The Complainant's physical address not be disclosed to the Respondent;

4.1.4 *The Respondent is ordered not to have any contact with the following child(ren):
;

4.1.5 *The Respondent is allowed contact with the following child(ren)
,
on the following basis ;

4.1.6 *The Respondent

4.2 A Warrant is authorised for the arrest of the Respondent, the execution of which is suspended subject to the Respondent's compliance with the provisions of the Protection Order as stated above.

4.3 A copy of this order and the warrant of arrest must be forwarded to the Police Station, once this interim order has been served on the Respondent.

5. DATE OF CONFIRMATION OF ORDER

5.1 **The Respondent** is hereby informed of his/her right to appear in the Magistrate's Court at
on the day of
at 08:30 in order to give reasons why the interim protection order should not be confirmed and made final; and of his/her right to have the matter heard on an earlier date after at least 24 hours' written notice to the applicant and the aforesaid court.

5.2 **The Respondent** is further informed that if he or she does not appear in court on the above-mentioned date and time, and the court is satisfied that this notice was properly served on him or her, and is satisfied that he or she committed or is committing an act of domestic violence, this order will be confirmed and made final.

MAGISTRATE DATE

* Delete whichever is not applicable

Form 5

NOTICE TO RESPONDENT TO SHOW CAUSE (SUBMIT REASONS)

WHY A PROTECTION ORDER SHOULD NOT BE ISSUED

[Regulation 7]

SECTION 5 (4) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF

HELD AT APPLICATION NO.

In the matter between:

APPLICANT:
(*Id. No./Date of Birth:)

AND

RESPONDENT:
(*Id. No./Date of Birth:)

NOTICE TO RESPONDENT:

1. **Particulars of Respondent:**

Home address:

(Tel. No.)

Work address:

(Tel. No.)

2. **Particulars of Application**

On (date), the Applicant applied for a protection order against you. The Court considered the application but has not issued an interim protection order but will on the undermentioned date decide whether or not to issue a protection order against you.

3. **Protection Order**

3.1 You are hereby called upon to give reasons why a protection order should not be issued against you by the above-mentioned Court on the day of at 08:30, on the basis of the application and supporting affidavits, if any, of which certified copies are attached hereto.

3.2 If you so wish, the matter can be heard on a earlier date after you have given at least 24 hours' written notice to the applicant and the Court.

3.3 The Court will issue a protection order against you if you do not appear in the court on the above-mentioned date and time, and if the Court is satisfied that this notice was properly served on you and that you have committed an act of domestic violence.

CLERK OF THE COURT DATE

Form 6
PROTECTION ORDER

[Regulation 8 (*a*)]

SECTION 6 OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

(*This form must be completed if an interim protection order was issued in terms of section 5 (2)*)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF

HELD AT APPLICATION NO.

In the matter between:

APPLICANT:

(*Id. No./Date of Birth:)

AND

RESPONDENT:

(*Id. No./Date of Birth:)

Whereas the Applicant successfully applied for a protection order which was issued on the day of , and **after** considering the facts of the matter;

The Court orders that the attached interim protection order be:

1. *Confirmed;

2. *Amended as follows:

; or

3.*Set Aside.

A copy of this order and interim protection order, as well as the warrant of arrest for the Respondent must be forwarded to the Police Station.

Dated at this day of 20

MAGISTRATE DATE

* Delete whichever is not applicable

Form 7
PROTECTION ORDER

[Regulation 8 (*b*)]

SECTION 6 OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

(*This form must be completed if an interim protection order was not issued*).

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF

HELD AT APPLICATION NO.

In the matter between:

APPLICANT:

(*Id. No./Date of Birth:)

AND

RESPONDENT:

(*Id. No./Date of Birth:)

1. **PARTICULARS OF RESPONDENT**

Home address:

(Tel. No.)

Work address:

(Tel. No.)

Occupation:

2. **PARTICULARS OF APPLICATION**

Whereas the Applicant has applied for a Protection Order against the Respondent as per the affidavit(s) and record of oral evidence (if any) attached, and an interim protection order was not issued, and after consideration of the application the Court now makes the order hereunder.

3. **ORDER BY COURT**

3.1 The Court orders that:

3.1.1 *The application for a Protection Order is dismissed; or

3.1.2 *An Interim Protection Order is granted; and the Respondent is ordered-

3.1.2.1 *not to commit the following act(s) of domestic violence

;

3.1.2.2 *not to enlist the help of another person to commit the acts of domestic violence specified in paragraph 3.1.2.1;

3.1.2.3 *not to enter the shared residence at

;

3.1.2.4 *not to enter the following parts of the shared residence

at

;

3.1.2.5 *not to enter the Complainant's residence at

;

3.1.2.6 *not to enter the Complainant's place of employment at

;

3.1.2.7 *not to prevent the Complainant or any child who ordinarily live(s) or lived in the shared residence at
from entering or remaining in the shared residence, or any part thereof;

3.1.2.8 *not to commit any of the following acts, to wit ;

3.1.2.9 *to make rent or mortgage payments in the sum of R per month/ annum;

3.1.2.10 *to pay the sum of R to the Complainant as emergency monetary relief.

4. **ADDITIONAL ORDERS**

4.1 It is further ordered that:

4.1.1 *A peace officer, namely , accompanies the Applicant to the following residence in order to assist with arrangements regarding the collection of personal property, i.e.

;

4.1.2 *A member of the South African Police Service at
seizes the following arm(s) or dangerous weapon(s) in the possession of the Respondent, i.e.

;

4.1.3 *The Complainant's physical address not be disclosed to the Respondent;

4.1.4 *The Respondent is ordered not to have any contact with the following child(ren):

;

4.1.5 *The Respondent is allowed contact with the following child(ren)

,
on the following basis ;

4.1.6 *The Respondent

4.2 A Warrant is authorised for the arrest of the Respondent, the execution of which is suspended subject to the Respondent's compliance with the provisions of the Protection Order as stated above.

4.3 A copy of this order and the warrant of arrest must be forwarded to the Police Station, once this order has been served on the Respondent.

MAGISTRATE DATE

* Delete whichever is not applicable

Form 8
WARRANT OF ARREST

[Regulation 9]

SECTION 8 (1) (*a*) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF HELD AT APPLICATION NO. In the matter between: APPLICANT: (*Id. No./Date of Birth:) AND RESPONDENT: (*Id. No./Date of Birth:)

TO ALL MEMBERS OF THE SOUTH AFRICAN POLICE SERVICE:

Whereas the attached Protection Order was granted against the Respondent by the Magistrate's Court for the district of on the day of 20 ; and

Whereas the Complainant has stated in the affidavit attached that the Respondent has breached (a) condition(s) of the Protection Order;

Therefore you are hereby authorised and ordered to forthwith arrest the Respondent in terms of the provisions of the Domestic Violence Act, 1998, if there are reasonable grounds to suspect that the Complainant may suffer imminent harm as a result of the alleged breach of the protection order by the Respondent.

GIVEN UNDER MY HAND AT THIS DAY OF 20 .

MAGISTRATE DATE

* Delete whichever is not applicable

Form 9
AFFIDAVIT FOR PURPOSES OF FURTHER WARRANT OF ARREST

[Regulation 10]

SECTION 8 (3) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF HELD AT APPLICATION NO. In the matter between: APPLICANT: (*Id. No./Date of Birth:) AND RESPONDENT: (*Id. No./Date of Birth:)

PART A: AFFIDAVIT (To be completed by complainant)

1. PARTICULARS OF COMPLAINANT

Surname:	
Full names:	
Id. No/Date of birth:	
Home or temporary address:	

Home/contact telephone number:	
Work address:	
Work telephone number:	
Occupation:	

2. PARTICULARS OF PROTECTION ORDER

A protection order was granted and a warrant of arrest authorised on:	(Date)
In the Magistrate's Court at:	
Against:	(Name of Respondent)

3. PARTICULARS OF RESPONDENT

Surname:	
Full names:	
Id. No/Date of birth:	
Home address:	
Home telephone number:	
Work address:	
Work telephone number:	

4. PARTICULARS OF APPLICATION

4.1 I require a *second/further warrant of arrest for my protection.

4.2. The existing warrant of arrest has been-

(*a*) *executed and cancelled; or

(*b*) *lost/destroyed, under the following circumstances:

Signature of Deponent Date

* Delete whichever is not applicable

PART B: CERTIFICATION (for official use)

I hereby certify that before administering the *oath/taking the affirmation I asked the Deponent the following questions and noted *her/his answers in *her/his presence as indicated below:

(*a*) Do you know and understand the contents of the above declaration?
Answer

(*b*) Do you have any objection to taking the prescribed oath?
Answer

(*c*) Do you consider the prescribed oath to be binding on your conscience?
Answer

I hereby certify that the Deponent has acknowledged that *she/he knows and understands the contents of this declaration which was *sworn to/affirmed before me, and the Deponent's *signature/thumb print/mark was placed thereon in my presence.

Dated at this day of 20

Justice of the Peace/
Commissioner of Oaths

Full names

Designation
Area for which appointed
Work address

* Delete whichever is not applicable

Form 10
AFFIDAVIT REGARDING CONTRAVENTION
OF PROTECTION ORDER

[Regulation 11]

SECTION 8 (4) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

APPLICANT: (*Id. No./Date of Birth:) AND RESPONDENT: (*Id. No./Date of Birth:)

PART A: AFFIDAVIT (To be completed by complainant)

1. PARTICULARS OF COMPLAINANT

Surname:	
Full names:	
Id. No/Date of birth:	
Home or temporary address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	
Occupation:	

2. PARTICULARS OF PROTECTION ORDER

A protection order was granted and a warrant of arrest authorised on:	(Date)
In the Magistrate's Court at:	
Against:	(Name of Respondent)
A copy of the Protection Order (Indicating what orders were made), and the original warrant of arrest are attached.	
A certified copy of the Protection Order and warrant of arrest where forwarded to the following Police Station:	

3. PARTICULARS OF RESPONDENT

Surname:	
Full names:	
Id. No/Date of birth:	
Home address:	
Home telephone number:	

Work address:	
Work telephone number:	

4. INFORMATION REGARDING BREACH OF PROTECTION ORDER

Date(s) of breach of protection order:	
Place(s) where breach of protection order took place:	
Full details on how the conditions of the protection order were breached:	
Reasons, if any, for believing that imminent harm may be suffered as a result of the breach of the protection order by the Respondent:	

Signature of Deponent Date

* Delete whichever is not applicable

PART B: CERTIFICATION (for official use)

I hereby certify that before administering the *oath/taking the affirmation I asked the Deponent the following questions and noted *her/his answers in *her/his presence as indicated below:

(*a*) Do you know and understand the contents of the above declaration?
Answer

(*b*) Do you have any objection to taking the prescribed oath?
Answer

(*c*) Do you consider the prescribed oath to be binding on your conscience?
Answer

I hereby certify that the Deponent has acknowledged that *she/he knows and understands the contents of this declaration which was *sworn to/affirmed before me, and the Deponent's *signature/thumb print/mark was placed thereon in my presence.

Dated at this day of 20

Justice of the Peace/
Commissioner of Oaths

Full names
Designation
Area for which appointed
Work address

* Delete whichever is not applicable

Form 11
NOTICE TO APPEAR BEFORE COURT

[Regulation 12 (1)]

SECTION 8 (4) (*c*) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

CASE NO.

IN THE MAGISTRATE'S COURT FOR THE DISTRICT

HELD AT COURT

DATE OF TRIAL

TO:

Name of Respondent:		
Home address:		
Sex:	Occupation/Status:	Id No./Date of birth:

You are hereby notified that you must appear personally before the above-mentioned Court on the date stated above at 08:30 on the following charge:

PARTICULARS OF CHARGE:

You are guilty of the offence of contravening section 17 (*a*) of the Domestic Violence Act, 1998 (Act No. 116 of 1998), in that upon or about the day of
and at or near
in the district of you

Note: (1) Please produce this document to the Clerk of the Court on the date of trial.
(2) By failing to appear before the Court as notified you may be convicted of an offence and upon conviction be sentenced to a fine or imprisonment for a period not exceeding six months.

CERTIFICATE:

I (rank and name), in my capacity as a member of the South African Police Service stationed at , hereby certify that I have handed the original of this notice to the Respondent mentioned therein at (place) on (date) and that I explained the contents thereof to the said Respondent.

(Name, rank and service no. of Member and date)

Form 12
APPLICATION FOR VARIATION OR SETTING ASIDE
OF PROTECTION ORDER

[Regulation 13]

SECTION 10 (1) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF

HELD AT APPLICATION NO.

In the matter between:

APPLICANT:

(*Id. No./Date of Birth:)

AND

RESPONDENT:

(*Id. No./Date of Birth:)

PART A: AFFIDAVIT (To be completed by complainant)

1. PARTICULARS OF APPLICANT

Surname:	
Full names:	
Id. No/Date of birth:	
Home or temporary address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	

* Delete whichever is not applicable

2. PARTICULARS OF RESPONDENT

Surname:	
Full names:	
Id. No/Date of birth:	
Home address:	
Home/contact telephone number:	
Work address:	
Work telephone number:	

3. PARTICULARS OF PROTECTION ORDER

A protection order was granted on:	(Date)
In the Magistrate's Court at:	
Against:	(Name of Respondent)

4. APPLICATION REGARDING PROTECTION ORDER

I wish to apply for:	*(*a*) The setting aside of the above-mentioned Protection Order
	*(*b*) The variation of the Protection Order as follows:

The reasons for my request are as follows:	

Signature of Deponent Date

* Delete whichever is not applicable

PART B: CERTIFICATION (for official use)

I hereby certify that before administering the *oath/taking the affirmation I asked the Deponent the following questions and noted *her/his answers in *her/his presence as indicated below:

(*a*) Do you know and understand the contents of the above declaration?

Answer

(*b*) Do you have any objection to taking the prescribed oath?

Answer

(*c*) Do you consider the prescribed oath to be binding on your conscience?

Answer

I hereby certify that the Deponent has acknowledged that *she/he knows and understands the contents of this declaration which was *sworn to/affirmed before me, and the Deponent's *signature/thumb print/mark was placed thereon in my presence.

Dated at this day of 20

Justice of the Peace/
Commissioner of Oaths

Full names

Designation

Area for which appointed

Work address

* Delete whichever is not applicable

Form 13

NOTICE OF VARIATION OR SETTING ASIDE
OF PROTECTION ORDER

[Regulation 14 (1)]

SECTION 10 (3) OF THE DOMESTIC VIOLENCE ACT, 1998
(ACT NO. 116 OF 1998)

IN THE MAGISTRATE'S COURT FOR THE DISTRICT OF
HELD AT APPLICATION NO.
In the matter between:
APPLICANT:
(*Id. No./Date of Birth:)
AND
RESPONDENT:
(*Id. No./Date of Birth:)

1. **Whereas** a Protection Order was granted against the Respondent on the day of *19/20 in the Magistrate's Court,

; and

2. **Whereas** the *App1icant/Respondent has applied for the *amendment /setting aside of the said Protection Order;

3. **Therefore** the Court orders that-

3.1 *The Protection Order is set aside; or

3.2 *The Protection Order is varied as follows:

Dated at this day of 20

MAGISTRATE DATE

* Delete whichever is not applicable

GN 207 of 3 March 2006: National Instruction 7/1999 - Domestic violence

National Instruction 7/1999 published in *Government Gazette* No. 20778, dated 30 December 1999, is hereby repealed and replaced by National Instruction 7/1999 Version 02.00 and is hereby published in terms of section 18 (3) of the Domestic Violence Act, 1998 (Act No. 116 of 1998) for general information.

ARRANGEMENT OF REGULATIONS

1. Background.-The Domestic Violence Act, 1998 (Act No. 116 of 1998), (hereinafter referred to as the Domestic Violence Act) imposes certain obligations on a member who receives a complaint of domestic violence. This instruction is intended to provide clear direction to a member on how to respond to a complaint of domestic violence in order to comply with the obligations imposed upon him or her in terms of the Domestic Violence Act.

2. Definitions.-In this instruction, unless the context otherwise indicates-

"complainant" means any person who is or has been in a domestic relationship with another person and who is alleged to be or to have been subjected by such other person (hereinafter referred to as the respondent) to an act of domestic violence and includes any child in the care of the complainant;

"domestic violence" means any one or more of the following forms of conduct performed by a respondent in respect of a complainant which consists of-

(*a*) physical abuse, consisting of any act or threatened act of physical violence;

(*b*) sexual abuse, consisting of conduct that abuses, humiliates, degrades or violates the sexual integrity of the complainant;

(*c*) emotional, verbal and psychological abuse, consisting of a pattern of degrading or humiliating conduct which may consist of-

- repeated insults, ridicule, or name calling;
- repeated threats to cause emotional pain; or
- the repeated exhibition of obsessive possessiveness or jealousy which is such as to constitute a serious invasion of the privacy, liberty, integrity or security of the complainant;

(*d*) economic abuse, which may consist of-

- the unreasonable withholding of economical or financial resources from a complainant who is legally entitled thereto or which the complainant requires of necessity, including the withholding of household necessities from the complainant or refusal to pay mortgage bond repayments or rent in respect of the shared residence; or
- the unreasonable disposal of household effects or other property in which the complainant has an interest;

(*e*) intimidation, by uttering or conveying a threat or causing the complainant to receive a threat which induces fear;

(*f*) harassment, consisting of a pattern of conduct which induces fear of harm to the complainant, including repeatedly-

- watching or loitering outside of or near the building or place where the complainant resides, works, carries on business, studies or happens to be;
- making telephone calls to the complainant, whether or not conversation ensues, or inducing another to do so;
- sending, delivering or causing the delivery of letters, telegrams, packages, facsimiles, electronic mail or other objects to the complainant;

(*g*) stalking, by repeatedly following, pursuing or accosting the complainant;

(*h*) damaging of property, consisting of the wilful damaging or destruction of property belonging to a complainant or in which the complainant has a vested interest;

(*i*) entry into the residence of the complainant without consent where the parties do not share the same residence; or

(*j*) any other controlling or abusive behaviour towards a complainant;

where such conduct harms, or may cause imminent harm to the safety, health or well-being of the complainant;

"domestic relationship" means a relationship between a complainant and the respondent where they-

(*a*) are or were married to each other in terms of any law, custom or religion;

(*b*) live or lived together in a relationship in the nature of a marriage (whether they are of the same or of the opposite sex);

(*c*) are the parents of a child or have or had parental responsibility for the child (whether or not at the same time);

(*d*) are family members related by consanguinity, affinity or adoption;

(*e*) are or were in an engagement, dating or customary relationship: including an actual or perceived romantic, intimate or sexual relationship of any duration; or

(*f*) share or recently shared the same residence;

"residence" also [means] institutions for children, the elderly and the disabled; and

"respondent" means any person who is or has been in a domestic relationship with a complainant and who allegedly commits or has committed domestic violence against the complainant.

3. Responsibilities of station commissioner.-(1) Every station commissioner must liaise with local representatives of the Department of Welfare, the local Community Police Forum and any other relevant local institution, to identify local organisations which are willing and able to provide counselling and other support services (including medical services and suitable shelter) to complainants.

(2) After having identified the organisations referred to in subparagraph (1), the station commissioner must liaise with the said organisations to determine-

(*a*) the specific services that are rendered by each;

(*b*) whether the services are rendered after hours, during weekends and on public holidays;

(*c*) whether the services are rendered free of charge or at a fee; and

(*d*) the contact particulars of each.

(3) The station commissioner must compile a list of the relevant organisations and include in it, in respect of

each organisation, at least the information referred to in subparagraph (2) as well as information relating to hospitals, ambulance services and medical practitioners that may be utilised to provide medical treatment to complainants.

(4) The original list referred to in subparagraph (3) must be kept by the station commissioner who must update it at least once every six months.

(5) The station commissioner must ensure that a copy of-

(*a*) the Domestic Violence Act;

(*b*) the Regulations promulgated in terms thereof;

(*c*) this National Instruction;

(*d*) the station orders issued by him or her in terms of subparagraph (6); and

(*e*) the list referred to in subparagraph (3);

are at all times available in the Community Service Centre and that a copy of the list referred to in subparagraph (3) is at all times available in each police vehicle at his or her station which is utilized to attend to complaints.

(6) The station commissioner must, taking into account the unique circumstances prevailing in his or her specific station area, available resources, etc., issue station orders-

(*a*) requiring a member under his or her command to inform a complainant of the services rendered by organisations mentioned in the list and how to inform the complainant thereof (e.g. by providing the complainant with a copy of the list or allowing the complainant to peruse the list or reading the information from the list to the complainant);

(*b*) setting out the steps that must be taken by such member to assist the complainant, when requested thereto by the complainant, to gain access to any service rendered by an organisation mentioned in the list or to obtain medical treatment should this be required; and

(*c*) in general, instructing members under his or her command on any other matter relating to the treatment of complainants of domestic violence which he or she deems necessary to determine in respect of his or her specific station area.

(7) Where a police station area forms part of a larger area consisting of more than one police station area and a radio control unit has been established to patrol and attend to complaints in such larger area, every station commissioner of a station in such larger area must, for information purposes, provide the commander of such radio control unit with a copy of-

(*a*) the list referred to in subparagraph (3) and, when he or she has updated the list, a copy of the updated version thereof; and

(*b*) a copy of the station orders issued in accordance with subparagraph (6) and, if he or she amends the orders, a copy of the updated version thereof.

4. Receiving complaints of domestic violence: responsibility of Community Service Centre commander.- (1) Every Community Service Centre commander must ensure that copies of the documentation referred to in paragraph 3 (5) (above) are at all times available in the Community Service Centre.

(2) If an incident of domestic violence is-

(*a*) telephonically reported to the Community Service Centre or to a radio control unit by the complainant or any other person; or is

(*b*) reported in person to the Community Service Centre by someone other than the complainant,

the Community Service Centre commander or member receiving the report must endeavour to obtain sufficient information concerning the incident to make it possible to comply with subparagraph (3).

(3) If an incident of domestic violence is reported in the manner referred to in subparagraph (2), the Community Service Centre commander or person answering the telephone, must-

(*a*) without any unreasonable delay, ensure that a police vehicle from the appropriate radio control unit or station is despatched to the complainant to attend to the matter;

(*b*) ensure that the crew of such vehicle is informed-

(i) whether any violence or threatened violence is allegedly or has allegedly been involved in the incident; and

(ii) who the complainant is.

(4) If a complainant reports an incident of domestic violence in person at the Community Service Centre, the Community Service Centre commander must ensure that the steps set out in paragraph 5 (2) (*a*) - (*d*) (below) are taken.

5. Responsibility of a member.-(1) A member who attends a scene of domestic violence must first of all determine whether the complainant is in any danger and take all reasonable steps to secure the scene as set out in paragraph 6 (below) and to protect the complainant from any danger.

(2) Once the scene has been secured, the member must-

(*a*) render such assistance to the complainant as may reasonably be required in the circumstances (this is more fully set out in paragraph 7 (below));

(*b*) if it is reasonably possible to do so, hand the Notice, contemplated in paragraph 10 (below), to the complainant and explain the contents of such notice to the complainant;

(*c*) assist the complainant or make arrangements for the complainant to find a suitable shelter and to obtain medical treatment, as set out in paragraphs 8 and 9 (below); and

(*d*) investigate the alleged incident of domestic violence and gather all available evidence in respect of any offence which may have been committed during such incident.

6. Securing a scene of domestic violence.-(1) Due to the high risk inherent to and volatility of domestic violence incidents, a member must be extremely careful when responding to a call to a scene of domestic violence and should, whenever reasonably possible, not go alone to the scene.

(2) Upon arriving at the scene, the member must attempt to locate the complainant and determine whether the complainant is in any danger.

(3) If the complainant is located and he or she is not inside a building or similar structure, the complainant must be interviewed to determine whether he or she is in any immediate danger. If the complainant does not seem to be in any immediate danger, the steps set out in paragraph 5 (2) (*a*) - (*d*) (above) must be followed. If the complainant is in any danger, the member must take the necessary steps to ensure the safety of the complainant.

(4) If it is established that the complainant is inside a building or similar structure, the member must determine whether there are reasonable grounds to suspect that an offence has been committed against the complainant.

(5) If a member has reasonable grounds to suspect that an offence has been committed and that the complainant may furnish information regarding the offence, such member-

(*a*) may, where necessary, if the complainant is inside a building or similar structure, exercise his or her powers in terms of sections 26 and 27 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) (hereinafter referred to as the Criminal Procedure Act), to enter the premises and building and interview and take a statement from the complainant, as this will enable him or her to determine whether the complainant is in any danger and what steps to take to protect the complainant from harm or further harm: Provided that a member may not, if the complainant is inside a private dwelling and the member is refused entry into the dwelling, forcibly enter the dwelling in terms of the said provisions;

(*b*) must, if the complainant is inside a private dwelling and the member is refused entry into the dwelling, take reasonable steps to communicate with the persons inside the dwelling to determine whether any person inside the dwelling is in any imminent danger, and-

(i) may, if he or she has reasonable grounds to believe that any person inside the dwelling is in imminent danger and that a forcible entry is necessary to protect the person, use minimum force to gain entry to the dwelling in order to protect the complainant or any other person from imminent physical harm (Circumstances which may indicate to the need for such action include cries for help, visible injuries or weapons, obvious signs that a struggle has occurred or the account of a witness that a crime has been committed and that the complainant could reasonably be expected to be injured and in need of urgent medical attention.); or

(ii) must, if he or she is satisfied that there are no reasonable grounds to believe that any person inside the dwelling is in any imminent danger, withdraw and make an entry in his or her Pocket Book (SAPS 206) setting out the reasons why he or she is so satisfied.

(6) If the member does not have reasonable grounds to believe that an offence has been committed and that the complainant is inside a building or structure (including a private dwelling), the member may not act in terms of sections 26 and 27 of the Criminal Procedure Act and must request permission to enter the building or structure and-

(*a*) if given permission to do so, enter the building or structure and interview the complainant to determine whether he or she is in any immediate danger. If the complainant does not seem to be in any immediate danger, the steps set out in paragraph 5 (2) (*a*)-(*e*) (above) must be followed. If the complainant is in any danger, the member must take the necessary steps to ensure the safety of the complainant; and

(*b*) if refused permission to do so, act as set out in subparagraph (5) (*b*) (above)

(7) Securing a scene of domestic violence may require the separation of the complainant and respondent and may include arresting the respondent in terms of section 3 of the Domestic Violence Act and section 40 (1) (*q*) of the

Criminal Procedure Act, which empowers a member to arrest without a warrant any person who is or has been in a domestic relationship with the complainant and whom the member reasonably suspects of having committed an offence containing an element of violence against the complainant (therefore including the offence of common assault). (See Standing Order 341 for general information concerning "Arrest").

(8) Where a member has reason to believe that a person-

(*a*) who has threatened or expressed the intention to kill or injure himself or herself or any other person by means of a firearm; or,

(*b*) who is in possession of a firearm and whose possession thereof is not in his or her interest or in the interest of any other person as a result of his or her mental condition, his or her inclination to violence (whether an arm was used in the violence or not), or his or her dependence on intoxicating liquor or a drug which has a narcotic effect,

such member may at any time, in terms of section 41 (1) of the Arms and Ammunition Act, 1969 (Act No. 75 of 1969), without a warrant enter upon and search such place or search such person and seize any arm or ammunition, for the purposes set out in section 11 of the said Act (which *inter alia* provides that the National Commissioner may declare a person to be unfit to possess arms).

(9) A member who seizes a firearm in accordance with subparagraph (8), must ascertain whether such firearm is licensed and, if not, include the offence in the docket.

7. Duty to render general assistance to the complainant.-(1) In terms of the Domestic Violence Act a complainant may approach the Service for assistance at any time, irrespective of when or where the incident took place. Where a criminal charge is laid by the complainant, it is the responsibility of the member receiving the complaint to open a docket and have it registered for investigation and the member may not avoid doing so by directing the complainant to counselling or conciliation services.

(2) When a member locates a complainant after having received a complaint of domestic violence or the complainant reports an incident of domestic violence at the Community Service Centre, such assistance as may reasonably be required in the circumstances must be rendered to the complainant.

(3) To comply with this duty, a member-

(*a*) must render such assistance as may be required by station orders provided for in paragraph 3 (6) (*c*) (above) including assistance to the complainant to lay a criminal charge; and

(*b*) may, where it is reasonable to do so, contact a family member or friend of the complainant to render support to the complainant.

(4) Any assistance rendered to the complainant in terms of subparagraphs (1)-(3) must-

(*a*) if it is rendered at the Community Service Centre, be recorded in the Occurrence Book; or

(*b*) if it is rendered at another place, be recorded in the Pocket Book (SAPS 206) of the member rendering the assistance.

8. Duty to assist the complainant to find suitable shelter.-(1) In terms of the Domestic Violence Act, a member must assist the complainant to find suitable shelter or make arrangements for the complainant to find suitable shelter.

(2) To comply with this duty, a member must comply with any station orders issued in this regard, as provided for in paragraph 3 (6) (above), and must at least-

(*a*) provide the complainant with the names, contact numbers and/or addresses of any organisation in the area which may be able to provide suitable shelter and relevant support and/or counselling services;

(*b*) at the request of the complainant and where it is reasonably possible to do so, contact on behalf of the complainant an organisation which may render relevant assistance to the complainant; and

(*c*) at the request of the complainant, assist in arranging transport for the complainant to a suitable shelter or an organisation that may be able to render relevant support and/or counselling (e.g. by contacting the family or friends of the complainant with a request to transport the complainant, arranging for a taxi at the expense of either the complainant or a willing family member or friend, etc.). A member may, only as a last resort, transport a complainant in a police vehicle to find a suitable shelter if such a vehicle is available and there is no other means of transport. In such an event the complainant must be informed that he or she is being transported at his or her own risk.

(3) Any assistance rendered to the complainant in terms of subparagraphs (1) and (2) must-

(*a*) if it is rendered at the Community Service Centre, be recorded in the Occurrence Book; or

(*b*) if it is rendered at another place, be recorded in the Pocket Book (SAPS 206) of the member rendering the assistance.

9. Duty to assist the complainant to obtain medical treatment.-(1) In terms of the Domestic Violence Act a member must assist the complainant to obtain medical treatment or make arrangements for the complainant to obtain medical treatment.

(2) To comply with this duty, a member must comply with any station orders issued by the station commissioner in this regard as provided for in paragraph 3 (6) (above) and must at least-

(*a*) ask the complainant whether he or she requires medical treatment; and, if so,

(*b*) assist or make arrangements for the complainant to receive medical treatment; and

(*c*) if a criminal charge has been laid, issue a J88 and SAPS 308 to the complainant for completion by a registered medical practitioner. (Where possible and provided transport is available, the member must arrange for the complainant to be taken to the registered medical practitioner.) A member may, only as a last resort, transport a complainant in a police vehicle to receive medical treatment if such a vehicle is available and there is no other means of transport. In such an event the complainant must be informed that he or she is being transported at his or her own risk.

(3) Any assistance rendered to the complainant in terms of subparagraphs (1) and (2) must-

(*a*) if it is rendered at the Community Service Centre, be recorded in the Occurrence Book together with a description of any injuries to the complainant that the member may have observed; or

(*b*) if it is rendered at another place, be recorded in the Pocket Book (SAPS 206) of the member rendering the assistance together with a description of any injuries that the member may have observed.

10. Provide complainant with Notice and explain content to complainant.-(1) In order to ensure that a complainant is informed of his or her rights as well as the remedies at his or her disposal in terms of the Domestic Violence Act, the member must, where reasonably possible to do so, hand to the complainant a copy of the Notice as provided for in the Domestic Violence Act (Form 1 to the Regulations in terms of the Act) in the official language of the complainant's choice.

(2) The remedies at the disposal of a complainant in terms of the Domestic Violence Act, are as follows-

(*a*) the right to lay a criminal charge;

(*b*) the right to apply for a protection order; or

(*c*) the right to lay a criminal charge as well as apply for a protection order.

It is important to inform the complainant that laying a criminal charge is not a prerequisite for applying for a protection order.

(3) As the Notice must be provided to the complainant in the official language of his or her choice, the member must ascertain what language the complainant understands.

(4) Once a member has determined what language the complainant understands, the following steps must be taken:

(*a*) If the language is one of the official languages of the Republic, the member must-

(i) if the member can speak and understand that language, hand a copy of the Notice to the complainant in that language and explain the contents thereof to the complainant;

(ii) if he or she cannot speak and understand that language and-

(*aa*) someone is available who can speak and understand that language, request such person to explain the contents of the Notice to the complainant in that language; or

(*bb*) if no one is available who can speak and understand that language, take all reasonable steps to find someone who can speak and understand that language. If such a person is found, paragraph (*aa*) must be complied with.

For the purpose of this paragraph, use must be made of the different translations of the Notice into the official languages of the Republic.

(*b*) If the language is not one of the official languages of the Republic the member must-

(i) if he or she can communicate in that language, convey the contents of the Notice to the complainant in that language;

(ii) if he or she cannot communicate in that language and-

(*aa*) someone is available who can communicate in that language, request such person to convey the contents of the Notice to the complainant in that language; or

(*bb*) if no one is available who can communicate in that language, take all reasonable steps to find someone who can communicate in that language. If such a person is found, paragraph

(*aa*) must be complied with.

(*c*) Any steps taken in terms of subparagraphs (*a*) (ii) (*bb*) or (*b*) (ii) (*bb*) must-

(i) if they are taken at the Community Service Centre, be recorded in the Occurrence Book; or

(ii) if they are taken at another place, be recorded in the Pocket Book (SAPS 206) of the member taking the steps.

(5) The member must request the complainant to sign in the Occurrence Book or in his or her Pocket Book, whichever may be applicable, at the relevant entry referred to in subparagraph (4) (*c*). By so doing, the complainant acknowledges that he or she has been informed of his or her rights and remedies in terms of the Domestic Violence Act and that he or she understands the contents thereof.

(6) If the complainant refuses to sign in the Occurrence Book or in the Pocket Book or is unable to do so, a third person, who witnessed the rights and remedies being explained to the complainant, must be requested to sign in the Occurrence Book or Pocket Book to certify that he or she has witnessed this and that the complainant refused to sign in the Occurrence Book or Pocket Book, whichever may be applicable.

11. Specific powers and duties of members in terms of the Domestic Violence Act.-(1) Seizure of arms and dangerous weapons in terms of a court order:

(*a*) The court may, in terms of section 7 (2) (*a*) of the Domestic Violence Act, order a member to seize any arm or dangerous weapon in the possession or under the control of a respondent.

(*b*) Any such firearm seized must be handed in at the police station to be dealt with in accordance with section 11 of the Arms and Ammunition Act, 1969.

(*c*) Any dangerous weapon seized must be handed in at the police station and a SAPS 13 tag must be attached to such weapon and the weapon must be retained in police custody for such period of time as the court may determine and may only be returned to the respondent or, if the respondent is not the owner of the dangerous weapon, to the owner thereof, by order of court and on such conditions as the court may determine.

(*d*) The normal procedures, as set out in Standing Orders 332-336, and which are applicable to exhibits or lost or stolen property must be followed, bearing in mind the provisions of section 9 (3) of the Act which provides that such dangerous weapon may only be disposed of in accordance with an order of court.

(2) Arresting a person with a warrant who contravenes a protection order:

(*a*) Where a respondent has contravened any prohibition, condition, obligation or order contained in a protection order, a complainant may hand the warrant of arrest together with an affidavit, wherein it is stated that the respondent contravened such protection order, to any member.

(*b*) If, upon receipt of the warrant of arrest together with the affidavit, referred to in subparagraph (*a*) (above), it appears to the member that there are reasonable grounds to suspect that the complainant may suffer imminent harm as a result of the alleged breach of the protection order, the member must arrest the respondent for contravening the protection order on the strength of the warrant.

(*c*) In considering whether or not the complainant may suffer imminent harm, a member must take the following into account:

(i) the risk to the safety, health or well-being of the complainant;

(ii) the seriousness of the conduct comprising the alleged breach of the protection order; and

(iii) the length of time since the alleged breach has occurred:

Provided that if the respondent is under the influence of liquor to such an extent that a Notice (referred to in subparagraph (*d*) (below)) cannot be handed to him or her, the respondent must be arrested.

(*d*) If the member is of the opinion that there are insufficient grounds to arrest the respondent, he or she must immediately hand a Notice to the respondent as provided for in Form 11 to the Regulations. The member must insert the first court day thereafter as date of appearance on the form and complete the certificate, provided for in the Notice. The member must put the duplicate original of this Notice in the docket which is opened for the contravention. This docket must be taken to court on the first court day thereafter.

(*e*) Whenever a warrant of arrest is handed to a member of the Service as contemplated in subparagraph (*a*) (above), the member must inform the complainant of his or her right to simultaneously lay a criminal charge against the respondent if applicable, and explain to the complainant how to lay such a charge.

(3) Service of documents:

A member may be ordered by the court to serve an interim or final protection order. If a member is ordered to

serve an interim protection order, the member must serve the order without delay as it only becomes binding on the respondent once the order has been served on him or her. As long as an interim protection order remains unserved, the complainant may be in danger. A final protection order becomes binding immediately upon it being issued even though it may not have been served.

(4) Accompanying complainant to collect personal property:

(*a*) The court may in a protection order, order a peace officer (which includes any member) to accompany the complainant to a specified place to assist with arrangements regarding the collection of the personal property specified in the order. It is important to note that the purpose of accompanying the complainant is to ensure the safety of such complainant and not to involve the member in any dispute regarding the ownership of such personal property. Such member must take reasonable steps to ensure the safety of the complainant during the collection of the property.

(*b*) The complainant and the member may enter the premises mentioned in the protection order in order to collect the personal property of the complainant as stipulated in the protection order. Before entering a private dwelling, the complainant and the member must however audibly demand admission and must notify the occupant of the purpose for which they seek to enter the dwelling.

(*c*) If, after having audibly demanded admission to a private dwelling, consent to enter is refused by the respondent, he or she contravenes the protection order and is therefore guilty of contempt of court. In such a case, the member may use such force as may be reasonably necessary in the circumstances to overcome any resistance against entry, including the breaking open of any door or window of such premises and enter the premises and arrest the respondent, whereafter the complainant may collect the said personal belongings.

(*d*) If a member is approached by a complainant to accompany him or her and it is not possible to do so immediately, the member must, if no other peace officer is available to accompany the complainant, arrange a reasonable time when it will be suitable to do so.

(*e*) If a peace officer accompanies a complainant in accordance with a protection order to collect his or her personal property, the peace officer must ensure the safety of the complainant while he or she removes the property specified in such protection order.

12. Keeping of records relating to incidents of domestic violence.-(1) All domestic violence incidents which are reported to a police station must be recorded in the Domestic Violence Register (SAPS 508 (*b*)) and it is the responsibility of the station commissioner to ensure that an accurate record is kept of all domestic violence incidents.

(2) If a complainant arrives at a police station to lay a criminal charge resulting from a domestic violence incident and indicates that the incident was first reported at an office of a municipal police service the member must-

(*a*) request the complainant to hand over the copy of the Report of Domestic Violence Incident-form (SAPS 508(*a*)) which was furnished to him or her by the member of the municipal police service. If the complainant does not have a copy thereof, the member must contact the particular office of the municipal police service to get a copy thereof;

(*b*) record the incident of domestic violence in red ink in the Domestic Violence Register (SAPS 508(*b*));

(*c*) in Column 6 (Pocket Book reference Column) of the Domestic Violence Register, record the monthly serial number of the relevant entry in the Domestic Violence Register of that specific office of the municipal police service (as captured on the copy of the SAPS 508(*a*)); and

(*d*) open a docket and have it registered on the CAS system.

(3) Members must fully document their responses to every incident of domestic violence on a "Report of Domestic Violence Incident"-form (SAPS 508 (*a*)) regardless of whether or not a criminal offence has been committed. A file with reference 39/4/2/3 must be opened every month and all the forms SAPS 508 (*a*) which are completed during that month, must be filed in it. The month concerned must be recorded after the reference number, for example all the SAPS 508 (*a*) forms which are completed during January 2000 must be filed with the reference 39/4/2/3 (1/2000).

(4) If a member attends a scene of domestic violence and no charges are laid or arrests made, the member must record the reasons why this was not done in his or her Pocket Book (SAPS 206).

(5) Certified copies of protection orders and of the warrants of arrest as provided for in the Domestic Violence Act, will be forwarded by the clerk of the court to the Community Service Centre of the complainant's choice. Particulars of the protection order must be entered in the appropriate columns of the Domestic Violence Register (SAPS 508 (*b*)) where an entry has already been made in respect of the complainant. Where no entry exists, a new entry must be made.

(6) A copy of every protection order and warrant of arrest that is received, must be filed in a separate file (under reference 39/4/3/1) which must be opened in accordance with the Registration and Record Control Procedure which forms part of the Record Classification System which was implemented on 15 September 1997. Every file must be allocated a case number to facilitate finding it (e.g. 39141311 (1) Koos Nel). The number of the case (in the above example (1)), must correspond with the number appearing in the index system created as set out in the fourth paragraph under section 16.2 of the Registration and Record Control Procedure. These files must be kept in a place which is accessible after hours, to ensure that they are readily available for checking purposes in

the event of an alleged breach of the protection order.

(7) Disposal of the aforementioned files must take place in accordance with the approved disposal authorisation.

13. Complaints regarding non-compliance by members and notification of such non-compliance to the Independent Complaints Directorate.-(1) In terms of the Domestic Violence Act, a failure by a member to comply with an obligation imposed in terms of the Act or this National Instruction constitutes misconduct. Disciplinary proceedings must therefore be instituted, in accordance with regulation 8 of the Discipline Regulations, against a member who fails to comply with an obligation imposed in terms of the Domestic Violence Act or this National Instruction.

(2) It is the responsibility of the commander of a member to institute disciplinary proceedings against such member who failed to comply with an obligation imposed in terms of the Act or this National Instruction. Where the commander is of the opinion that disciplinary proceedings should not be instituted against such member, the commander must apply to the Independant Complaints Directorate for exemption. Such an application must contain a full report, which includes the reasons for the application for exemption, and must be forwarded to the offices of the Area Commissioner within 30 days after the receipt of the complaint.

(3) The Area Commissioner must, if he or she agrees that no disciplinary action should be taken, submit the application referred to in subparagraph (2) above, within 14 days after the receipt of the application, to the Provincial Commissioner, who must, if he or she agrees that no disciplinary action should be taken, immediately submit such application to the provincial office of the Independant Complaints Directorate.

(4) The provincial office of the Independant Complaints Directorate has agreed to inform the Provincial Commissioner in writing, within 30 days after the receipt of the application for exemption, whether exemption has been granted or not and, in the event that the exemption has not been granted, of the reasons why such exemption was not granted.

(5) Progress reports pertaining to disciplinary proceedings instituted against members in terms of section 18 (4) of the Act, must on a monthly basis be forwarded by a commander to the Area Commissioner.

14. Keeping of record of complaints against members.-(1) Every station commissioner must keep a record of-

(*a*) the number and particulars of complaints received against members under his or her command in respect of any failure to comply with obligations in terms of the Domestic Violence Act or these instructions;

(*b*) the disciplinary proceedings instituted as a result thereof and the decisions which emanated from such proceedings; and

(*c*) steps taken as a result of recommendations made by the Independant Complaints Directorate.

(2) Every allegation of misconduct regarding an alleged failure by a member to comply with any obligation in terms of the Domestic Violence Act, the Regulations in terms of that Act or the National Instruction issued in this respect, that was received during the previous month, must be recorded on the SAPS 508-form. This return must be submitted to the relevant Area Commissioner before the third working day of each month.

(3) A consolidated return on SAPS 508 must be submitted by the Area Commissioner to the Provincial Commissioner before the seventh working day of each month. The Provincial Commissioner must furnish a consolidated return before the tenth working day of each month to the provincial office of the Independant Complaints Directorate and to the Divisional Commissioner: Crime Prevention for submission to Parliament, as required by section 18 (5) (*d*) of the Act.

(4) If disciplinary proceedings against a member have not been completed, the return of the subsequent month must again contain particulars concerning the complaint. In such a case, the monthly serial number in the first column must remain the same. (Example: The February return will, once again, refer to a complaint received in January, but which was not finalized in January before the January return was completed. Such an entry must appear on the return before any new complaints that were received in February. The January complaint will keep the January serial number, example 13/1/2000.)

(5) The Codes which must be recorded in column 6, are the following:

DS1 Remedial steps after initial interview (not serious)

DS2 Verbal warning after initial interview (not serious)

DS3 Written warning (not serious)

DS4A Departmental investigation (serious): still under investigation

DS4B Departmental investigation (serious): guilty (state sentence)

DS4C Departmental investigation (serious): not guilty

15. Reporting on incidents of domestic violence.-(1) Before the third working day of each month, the station commissioner must submit a return to the relevant area commissioner containing the following information:

(*a*) the number of incidents of domestic violence reported to that station during the previous month;

(*b*) the number of incidents of domestic violence referred to the station during the previous month by offices of a municipal police service (the number of entries in red ink in the register);

(*c*) the number of members trained on the handling of incidents of domestic violence at that station during the previous month; and

(*d*) the number of dockets relating to domestic violence opened and registered on the CAS system or in the CR during the previous month.

(2) A consolidated return of the aforementioned information received from all stations in the area must be submitted by the area commissioner to the provincial commissioner before the seventh working day of each month.

(3) The provincial commissioner must furnish a consolidated return of the aforementioned information received from all areas before the tenth working day of each month to the Divisional Commissioner: Crime Prevention.