



NINETY-SIXTH ORDINARY SESSION OF THE COUNCIL OF MINISTERS

Freetown, 16 – 17 July, 2026

DIRECTIVE C/DIR.2/7/26 ON FIGHTING CYBERCRIME

THE COUNCIL OF MINISTERS,

MINDFUL of the ECOWAS Revised Treaty as amended, particularly articles 10, 11 and 12, establishing the Council of Ministers and defining its composition and functions;

MINDFUL of the said Treaty, particularly articles 27, 32 and 33, on Science and Technology, and Communication and Telecommunications;

MINDFUL of the ECOWAS Revised Treaty, particularly article 57, on judicial and legal cooperation, which provides that Member States undertake to promote judicial cooperation with a view to harmonizing judicial and legal systems;

MINDFUL of Convention A/P1/7/92 of ECOWAS relating to Mutual Assistance in Criminal Matters;

MINDFUL of Convention A/P1/94 relating to Extradition;

MINDFUL of Supplementary Act A/SA 1/01/07 on the harmonization of the policies and regulatory framework of the Information and Communication Technology sector (ICT);

MINDFUL of Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS;

MINDFUL of Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS;

CONSIDERING the existing cooperation between Member States on matters of criminal policing, which provides for the pooling of expertise and sharing of experiences by security services with a view to establishing effective methods of investigation and enforcement;

CONSIDERING ALSO that rapid technological developments, including the evolution of computer systems, networks and digital services, have created new forms of criminal conduct and amplified existing threats to the confidentiality, integrity and availability of data and systems;

NOTING that regional and global best practices on combating cybercrime have advanced significantly since the adoption of Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, requiring ECOWAS to update its framework in line with these developments;

CONSCIOUS of the need to equip the Community with modern, harmonised and robust legal tools in order to effectively prevent, detect, investigate and prosecute cybercrime, and to strengthen trust in digital technologies;

DESIROUS of ensuring that the ECOWAS legal framework remains aligned with evolving international standards, while reflecting the specific needs and priorities of the region;

PRESCRIBES:

CHAPTER I – DEFINITIONS

Article 1: Definitions

For the purposes of this Directive, unless the contrary intention appears:

1. **"access"** means gaining access to the whole or any part of any computer system whether or not through enabling entry, control or the right to use the whole or any part of any computer system;
2. **"access to computer program or computer data"** means access to any computer program or computer data held in any computer system if by causing a computer system to perform any function whereby a person:
 - i. alters, modifies or erases the computer program or computer data or any aspect or attribute related to the computer program or computer data; or
 - ii. copies, transfers or moves it to-
 - a. any computer system, device or computer data storage medium other than that in which it is held; or
 - b. to a different location in the same computer system, device or computer data storage medium in which it is held; or
 - iii. uses it; or
 - iv. has it output from the computer system in which it is held, whether by having it displayed or in any other manner;

and references to access to a computer program or computer data (and to an intent to secure such access) shall be read accordingly.

For the purposes of paragraph (iii) above a person uses a program if the function he causes the computer system to perform:

- i. causes the computer program to be executed; or
- ii. is itself a function of the computer program.

For the purposes of paragraph (iv) above:

- i. a computer program is output if the instructions of which it consists are output; and
- ii. the form in which any such instructions or any other computer data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer system) is immaterial;

- 3. “**child**” means every human being below the age of 18 years;
- 4. “**critical infrastructure**” means any computer systems, computer programs, computer data or assets, whether physical or virtual, so vital to the Member State that the incapacity or destruction of such computer systems, computer programs, computer data or assets would have a debilitating impact on domestic or border security, national economic security, national public health or safety, or any combination of those matters, and includes any other computer systems, computer programs, computer data or assets that are designated as critical information infrastructure by the authority competent for such designation under the law of the Member State. Critical infrastructure may include critical information infrastructure.
- 5. “**computer data**” means any representation of facts, information or concepts in a form suitable for processing in a computer system;
- 6. “**computer data storage medium**” means any device, whether physical or virtual, containing, designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed or decentralised form for use by a computer system, from which information is capable of being retrieved or reproduced, and any references to any computer program or computer data held in

a computer system include references to any computer program or computer data held in any removable storage medium which is for the time being in the computer system; and a computer system is to be regarded as containing any computer program or computer data held in any such medium;

7. "**computer program**" means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function, and references to a computer program include references to part of a computer program;
8. "**computer system**" means any device or a group of interconnected or related devices, one or more of which, pursuant to a computer program, performs automatic processing of computer data;
9. "**confiscation**", which includes forfeiture where applicable, means the permanent deprivation of property by order of a court or other competent authority;
10. "**content data**" means the substance, purport or meaning of a specified communication that is intercepted under Articles 33 and 43 of this Directive;
11. "**device**" includes-
 - i. physical or virtual device;
 - ii. any electronic or virtual tool that is not in physical form;
 - iii. any computer program or computer data held in electronic form;
 - iv. a password, access code or similar data, in electronic or other form, by which the whole or any part of a computer system is capable of being accessed; or
 - v. automated, self-executing, adaptive or autonomous devices, computer programs or computer systems;
12. "**emergency**" means a situation in which there is a significant and imminent risk to the life or safety of any natural person;
13. "**intercept**" means, for the purpose of:
 - (i) Article 3, listening to or recording a function of a computer system, or acquiring the substance, meaning or purport thereof; and

(ii) Articles 33 and 43, collection, recording or acquisition of content data;

14. “**freezing**” or “**seizure**” means temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a judicial or other competent authority;

15. “**proceeds of crime**” means any property derived from or obtained, directly or indirectly, through the commission of an offence;

16. “**publishing**” includes:

- i. distributing, transmitting, disseminating, broadcasting, circulating, delivering, displaying, exhibiting, lending for gain, exchanging, bartering, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way;
- ii. printing, copying, or making in any other manner (whether of the same or of a different kind or nature) for the purpose of doing any of the acts referred to in subparagraph (i).

17. “**predicate offence**” means any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in Article 21 of this Directive;

18. “**racist and xenophobic material**” means any written material (whether in digital, electronic or any other form), any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

19. “**seize**” means the power to:

- i. seize or similarly secure a computer system or part of it, or a computer data storage medium;
- ii. make and retain a copy of a computer program or computer data,

- iii. maintain the integrity of the relevant stored computer program or computer data;
- iv. render inaccessible, or remove, computer program or computer data in the accessed computer system; and
- v. obtain output of computer data from a computer system.

20. **“service provider”** means:

- i. a public or private entity that provides users of its services the ability to communicate by means of a computer system; and
- ii. any other entity that processes or stores computer data on behalf of that entity or those users.

21. **“subscriber information”** means any information contained in the form of computer data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established-

- i. the type of communication service used, the technical provisions taken thereto and the period of service;
- ii. the subscriber's identity, postal, geographic electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or
- iii. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement; and

22. **“traffic data”** means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or the type of underlying service.

CHAPTER II – CYBERCRIME OFFENCES

Article 2: Unauthorised access

1. Each Member State shall adopt necessary measures to criminalise under their domestic law the intentional act of causing a computer system to perform any function with the intent to secure access to the whole or any part of any computer system, computer program or computer data, or to enable any such access to be secured, where,
 - a. the access intended to be secured, or enabled to be secured, is unauthorised; and
 - b. at the time of causing the computer system to perform the function, the person knows that the access he or she intends to secure, or enable to be secured, is unauthorised.
2. For the purposes of paragraph 1 of this article, access of any kind by any person to any computer system, computer program or computer data shall be considered unauthorised if:
 - a. that person is not entitled to control access of the particular kind or type in question with respect to the computer, computer system, computer program or computer data; and
 - b. that person does not have the consent of the person entitled to grant such consent, for the particular kind or type of access in question; or if such person has exceeded the authorisation, entitlement or consent referred to in sub-paragraphs 2 (a) and (b) of this article.
3. The intention referred to in paragraph 1 of this article shall not be required to relate to or be directed at:
 - a. any particular computer program or computer data;
 - b. a computer program or computer data of any particular kind; or
 - c. a computer program or computer data held in a particular computer system.
4. Paragraph 1 of this article shall not apply where access is undertaken pursuant to legal authority, a court order, a warrant or the lawful exercise of powers under national law.
5. For the purposes of this article, the absence of authorisation shall include instances where there may exist a general authorisation to access a computer system, but where a specific type, nature or method of access is not authorised.

Article 3 :Unauthorised interception

1. Each Member State shall adopt necessary measures to establish as a criminal offence under their domestic law the intentional and unauthorised act of intercepting or causing the interception, whether temporarily or permanently and whether directly or indirectly, by technical means of any non-public:
 - a. transmission of computer data to, from or within a computer system; or
 - b. electromagnetic emissions from a computer system carrying such computer data.
2. For the purposes of this Article, interception shall be considered unauthorised where the person intercepting, or causing the interception:
 - a. is not the person with responsibility for the computer system concerned;
 - b. is not the person entitled to determine whether such interception may take place;
 - c. does not have the consent of a person who is entitled to grant such consent; and
 - d. if such person has exceeded the authorisation, entitlement or consent.
3. The intention referred to in paragraph 1 of this article shall not be required to relate to or be directed at:
 - a. any particular computer system, computer program or computer data;
 - b. a computer program or computer data of any particular kind; or
 - c. a computer program or computer data held in a particular computer system.
4. For the purposes of this Article, it shall be immaterial whether an unauthorised interception, or any intended effect of such interception, is permanent or temporary.
5. Paragraph 1 of this article shall not apply where interception is undertaken pursuant to legal authority, a court order, a warrant or the lawful exercise of powers under national law.

Article 4: Unauthorised interference with computer program or computer data

1. Each Member State shall adopt necessary measures to criminalise offence under their domestic law the intentional and unauthorised act of interference or causing

unauthorised interference with a computer program or computer data, whether temporarily or permanently.

2. For the purposes of paragraph 1 of this Article, “interference with computer program or computer data” means:

- a. damaging, deleting, deteriorating, altering, erasing or suppressing a computer program or computer data;
- b. adding any computer program or computer data to the contents of a computer system;
- c. preventing or hindering access to, or the availability of, any computer program or computer data;
- d. impairing the operation of any computer program or the reliability of any computer data;
- e. altering the integrity or the content of any computer program or computer data;
- f. impairing the reliability, availability or security of any computer program or computer data;
- g. enabling any of the acts mentioned paragraph 2 (a) to (f) of this article to be carried out.

3. For the purpose of this Article, interference shall be considered unauthorised if the person doing or causing such interference:

- a. is not entitled to determine whether the interference may be undertaken;
- b. does not have the consent of a person who is entitled to grant such consent; and
- c. has exceeded the authorisation, entitlement or consent.

4. Any interference with data undertaken in accordance with statutory authority, judicial order, or the lawful exercise of powers under domestic law shall be deemed to be authorised.

5. The intention referred to in paragraph 1 of this article shall not be required to relate to or be directed at:

- a. any particular computer system, computer program or computer data;
- b. a computer program or computer data of any particular kind; or
- c. a computer program or computer data held in a particular computer system.

6. For the purpose of this Article, it shall be immaterial whether an unauthorised interference with data or any intended effect of such interference is permanent or temporary.
7. Paragraph 1 of this Article shall not apply where interference with data is undertaken pursuant to legal authority, a court order, a warrant or the lawful exercise of powers under national law.

Article 5: Unauthorised interference with computer system

1. Each Member State shall adopt necessary measures to criminalise under their domestic law, the intentional and unauthorised act of interfering with or causing interference with a computer system, whether temporarily or permanently.
2. For the purposes of this Article, “interference with a computer system” means inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer program or computer data to cause:
 - a. hindering of the functioning of a computer system, in whole or in part;
 - b. impairment to the operation, reliability or security of a computer system;
 - c. hindrance or obstruction of access to a computer system; or
 - d. enabling any of the acts referred to in paragraphs 2 (a) to (c) of this article to be carried out.
3. For the purposes of this Article, interference with a computer system shall be considered unauthorised if the person doing or causing such interference:
 - a. is not entitled to determine whether the interference may be undertaken;
 - b. does not have the consent of a person who is entitled to grant such consent; and
 - c. if such person has exceeded the authorisation, entitlement or consent.
4. Nothing in this Article shall require Member States to criminalise conduct that constitutes only a minor interference with a computer system, that is, conduct which is so trivial or negligible in its effect that it does not cause, or create a risk of causing, any material harm.

5. The intention referred to in paragraph 1 of this article shall not be required to relate to or be directed at:
 - a. any particular computer system, computer program or computer data;
 - b. a computer program or computer data of any particular kind; or
 - c. a computer program or computer data held in a particular computer system.
6. For the purposes of this Article, it shall be immaterial whether an unauthorised interference with a computer system, or any intended effect of such interference, is permanent or temporary.
7. Paragraph 1 of this article shall not apply where interference with a computer system is undertaken pursuant to legal authority, a court order, a warrant or the lawful exercise of powers under national law.

Article 6 : Misuse of devices

1. Each Member State shall adopt necessary measures to criminalise under their national law, the intentional and unauthorised act of:
 - a. either:
 - i. manufacturing, producing, making, generating, adapting, transferring, importing, exporting, distributing, sharing, supplying, offering to supply, selling, or otherwise making available any device, primarily for use, with the intent or belief that it be primarily used to commit or assist in the commission of an offence established pursuant to Articles 2, 3, 4 or 5 of this Directive; or
 - ii. acquiring, obtaining, or procuring any device, primarily for use, with the intent or belief that it be primarily used to commit or assist in the commission of an offence under the Articles listed in paragraph (a) (i) of this article.
 - b. possessing such number of the devices referred to in paragraph 1(a) of this article as may be determined by the Member State under its national law, with the intent

that such devices be used to commit or assist in the commission of an offence under the Articles listed in paragraph 1(a) of this article.

2. For the purposes of this Article, the term "device" shall include:
 - a. a computer system or part thereof;
 - b. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed;
 - c. any computer program, including malware, designed or adapted primarily for the purpose of committing an offence established in accordance with this Directive.
3. It shall not constitute an offence under this Article where the manufacture, production, making, generation, adaptation, transfer, procurement, import, distribution, possession, or making available of such device is:
 - a. not primarily designed or adapted for the purpose of committing an offence established in accordance with this Directive;
 - b. undertaken for authorised training, testing, network analysis, protection of a computer system, research and development, or for another similar legitimate use; or
 - c. undertaken in compliance with, and in accordance with, a judicial warrant, statutory authority, or other lawful exercise of power under national law.

Article 7: Computer-related forgery

1. Each Member State shall adopt necessary measures to criminalise under their national law the intentional and unauthorised act of inputting, altering, deleting, or suppressing computer data, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, whether or not the data is directly readable or intelligible.

2. Each Member State may take measures to ensure that aggravated circumstances are provided for, including where the offence established in accordance with paragraph 1 of this article is committed dishonestly or with similar intent for wrongful gain, for wrongful loss, or for any economic benefit for oneself or for another person.

Article 8: Computer-related fraud

1. Each Member State shall adopt necessary measures to criminalise under its domestic law the conduct of any person who, with fraudulent or dishonest intent, procures by means of an unauthorised act that causes, in whole or in part, loss of any data, program, property, valuable security, consideration, or computer system, for:
 - a. wrongful gain;
 - b. wrongful loss; or
 - c. any economic benefit for oneself or for another person.
2. For the purposes of paragraph 1 of this article, an “act” includes, but is not limited to:
 - a. any unauthorised access to a computer system or to a computer program or computer data;
 - b. any input, alteration, modification, deletion, suppression, or generation of any computer program or computer data;
 - c. any interference, hindrance, impairment, or obstruction with the functioning of a computer system; or
 - d. copying, transferring, or moving any computer data or computer program to a computer system, device, or storage medium other than that in which it is lawfully held, or to a different location within any such system, device, or storage medium; or
 - e. using such computer data or computer program; or
 - f. obtaining any computer data or computer program output from the computer system in which it is held, whether by display or by any other means; or
 - g. any deception as to factual circumstances made through a computer system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do.

Article 9: Offences against critical infrastructure

Each Member State shall take measures to ensure that aggravated circumstances apply where an offence established under Chapter II of this Directive, or any other conduct prescribed by Member States, including any action resulting in physical damage, is committed against critical infrastructure.

Article 10: Offences related to online child sexual abuse or child sexual exploitation material

1. Each Member State shall adopt necessary measures to establish as a criminal offence under their national law the intentional act of:
 - a. publishing child sexual abuse or child sexual exploitation material through a computer system;
 - b. producing child sexual abuse or child sexual exploitation material for the purpose of its publication through a computer system;
 - c. possessing or controlling child sexual abuse or child sexual exploitation material in a computer system or on a computer data storage medium;
 - d. soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through a computer system;
 - e. disseminating, distributing or otherwise making available of child sexual abuse or child sexual exploitation material through a computer system; or
 - f. financing the offences established in accordance with paragraphs 1 (a) to (e) of this article.
2. For the purposes of this article “child sexual abuse or child sexual exploitation material” shall include visual material, and may include written or audio content, that depicts, describes or represents:
 - a. a child engaged in real or simulated sexually explicit conduct;
 - b. a child in the presence of a person engaging in any sexual activity;
 - c. a person who appears to be a child whose sexual parts are displayed for primarily sexual purposes;
 - d. a child subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature;
 - e. a person who appears to be a child engaged in sexually explicit conduct; or
 - f. realistic images representing a child engaged in sexually explicit conduct.

3. Each Member State may require that the material identified in paragraph 2 of this Article be limited to material that:
 - a. depicts, describes or represents an existing person; or
 - b. visually depicts child sexual abuse or child sexual exploitation.
4. In accordance with their national law and consistent with applicable international obligations, a Member State may take steps to exclude the criminalisation of:
 - a. conduct by children for self-generated material depicting them; or
 - b. the consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this Article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.
5. Nothing in this Directive shall affect any international obligations which are more conducive to protect the rights of the child.

Article 11: Solicitation or grooming for the purposes of committing a sexual offence against a child

A Member State shall adopt necessary measures to criminalise under its domestic law the intentional act of communicating, soliciting, grooming, or making any arrangement, by means of a computer system, with a minor, for the purpose of committing a sexual offence against that minor, including the commission of any offence established in accordance with Article 10 of this Directive.

Article 12 – Non-consensual dissemination of intimate images

1. Each Member State shall adopt necessary measures to criminalise the intentional act of publishing, by means of a computer system, an intimate image of a person, without the consent of the person depicted in the image.

2. For the purposes of paragraph 1 of this article, “intimate image” means any visual recording of an individual, whether a photograph, video, or other depiction made by any means, that is sexual in nature, or in which the person is nude, partially nude, engaged in sexual activity, or depicted in circumstances where a reasonable expectation of privacy existed at the time of the offence.
3. Each Member State shall provide that criminal liability requires the following mental elements:
 - a. the disclosure was made intentionally or recklessly as to the emotional harm and distress that may be caused to the victim; or
 - b. the disclosure was made with intent to obtain wrongful gain or cause wrongful loss.
4. Each Member State shall recognise defences or exceptions where:
 - a. the person depicted voluntarily consented to the disclosure;
 - b. the disclosure was made in good faith for law enforcement, judicial or medical purposes; or
 - c. the image was lawfully made available in a commercial context.
5. Each Member State shall extend the offence to cover threats to distribute an intimate image without consent.

CHAPTER III - OTHER OFFENCES

Article 13 – Cyberstalking

1. Each Member State shall adopt necessary measures to criminalise the act of intentionally pursuing a course of conduct, by means of a computer system, that amounts to stalking of another person.
2. For the purposes of paragraph 1 of this Article, a “course of conduct” may include one or more of the following acts, whether conducted directly or indirectly, and when carried out repeatedly or systematically:

- a. contacting or attempting to contact a person by any electronic means, including email, text messaging, social media, or internet-based communications;
 - b. publishing or causing to be published any material relating, or purporting to relate, to a person, or purporting to originate from a person;
 - c. monitoring the use by a person of a computer system or any form of electronic communication;
 - d. interfering with, damaging, or gaining access to property in the possession of a person; or
 - e. leaving or transmitting offensive or threatening material to a person, directly or indirectly.
3. For the purposes of paragraph 2 of this Article, each Member State shall, under their national law, determine the number of occurrences or the circumstances that shall constitute conduct as being “repeated” or “systematic.”
4. Each Member State shall provide that criminal liability requires the following mental elements:
 - a. the conduct was carried out with intent to harass, intimidate, torment, or embarrass;
 - b. the person knew, or ought to have known, that the conduct would cause harassment; and
 - c. the conduct was intended to cause fear for the safety of the person or anyone known to them.
5. Each Member State shall ensure that the offence established pursuant to paragraph 1 of this Article has the following effects:
 - a. causing the person reasonably, in all the circumstances, to fear for their safety or the safety of another;
 - b. causing the person apprehension or fear of violence to themselves, another person, or against their property; or
 - c. causing detriment, reasonably arising in all the circumstances, to the health, reputation, relationships, or career of a person.
6. Each Member State shall recognise defences or exceptions where:

- a. the conduct was pursued for the purpose of preventing or detecting crime;
- b. the conduct was authorised by law or carried out in compliance with a lawful requirement;
- c. the conduct was reasonable in the circumstances; or
- d. the conduct was done reasonably in the course of a lawful trade, business, occupation, or for the purposes of obtaining or giving information in which the person has a legitimate interest.

7. Each Member State may provide that aggravated circumstances are established where:

- a. the victim is a minor;
- b. the offence was committed in the context of an intimate or trust-based relationship; or
- c. the conduct resulted in substantial harm to the health, safety, or wellbeing of the victim.

Article 14 – Cyberbullying

1. Each Member State shall adopt necessary measures to criminalise the act of intentionally engaging in conduct, by means of a computer system, that amounts to bullying, harassment, or intimidation of another person, when committed repeatedly or systematically.
2. For the purposes of this article, a Member State shall, under their national law, determine the number of occurrences or the circumstances that shall constitute conduct as being “repeated” or “systematic.”
3. A Member State shall ensure that criminal liability shall include mental elements related to the following:
 - a. the person knew, or ought to have known, that the conduct would cause harassment or substantial emotional distress;
 - b. the conduct was carried out recklessly as to whether it would cause harassment, intimidation, or distress; or
 - c. the conduct was intended to cause fear for the safety of the person or another.

4. Each Member State shall ensure that the offence established pursuant to paragraph 1 of this article has the following effects, an act:
 - a. that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them;
 - b. that causes that other person or any other person harassment, alarm or distress; or
 - c. that causes that other person reasonably, in all the circumstances, apprehension of violence or damage to any person or property.
5. Each Member State shall recognise defences or exceptions where, the conduct was:
 - a. pursued for the purpose of preventing or detecting crime;
 - b. authorised by law or carried out in compliance with a lawful requirement;
 - c. reasonable in the circumstances; or
 - d. done reasonably in the course of a lawful trade, business, occupation, or for the purposes of obtaining or giving information in which the person has a legitimate interest.
6. Member State may provide that aggravated circumstances are established where:
 - a. the victim is a child;
 - b. the offence was committed in the context of an intimate or trust-based relationship; or
 - c. the conduct resulted in substantial harm to the health, safety, or wellbeing of the victim.

Article 15: Unauthorised disclosure

Each Member State shall adopt necessary measures to criminalise under its domestic law the intentional and unauthorised disclosure by means of a computer system of any:

- a. computer data; or
- b. any password, access code or any other means of gaining access to any computer program or computer data held in any computer system.

Article 16: Dissemination of racist and xenophobic material through computer system

Each Member State shall adopt necessary measures to criminalise, under its national law, the conduct of any person who intentionally distributes or otherwise makes available to the public, through a computer system, racist or xenophobic material.

Article 17: Racist and xenophobic-motivated threat

1. Each Member State shall adopt necessary measures to criminalise, under its national law, the conduct of any person who, intentionally, through a computer system, threatens the commission of a serious offence against any person or group of persons on the grounds that they belong to a group distinguished by race, colour, descent, or national or ethnic origin, as well as religion, where religion is used as a pretext for any of these factors.
2. For the purposes of this Article, each Member State may determine what constitutes a “serious offence” under its national law.

Article 18: Racist and xenophobic-motivated insult

Each Member State may adopt necessary measures to criminalise, under its national law, the conduct of any person who, intentionally and publicly, through a computer system, insults any person or group of persons on the grounds that they belong to a group distinguished by race, colour, descent, or national or ethnic origin, as well as religion, where religion is used as a pretext for any of these factors.

Article 19: Denial, gross minimisation, approval or justification of genocide or crimes against humanity

Each Member State may adopt necessary measures to criminalise, under its national law, the conduct of any person who,, with the intent to incite hatred, discrimination, or violence against any individual or group of individuals on the grounds of race, colour, descent, or national or ethnic origin, as well as religion where used as a pretext for any of these factors, distributes or otherwise makes available to the public, through a computer system, any material which denies, grossly minimises, approves, or justifies acts constituting genocide or crimes against humanity as defined under international law.

Article 20 – Infringement of copyright and related rights

Each Member State shall adopt necessary measures to criminalise, under its national law, the infringement of copyright and any related rights, as defined under the law of the Member State, where such acts are committed wilfully, on a commercial scale and by means of a computer system, pursuant to its international obligations.

Article 21 – Laundering of proceeds of crime

1. Each Member State shall adopt, in accordance with fundamental principles of its national law, necessary measures to establish as criminal offences, when committed intentionally:
 - a. the conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions;
 - b. the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime.
2. Subject to the basic concepts of its legal system:
 - a. the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

- b. participation in, association with or conspiracy to commit, attempts to commit, aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this Article.
3. For purposes of implementing or applying paragraph 1 of this Article:
- a. Each Member State shall establish as predicate offences relevant offences established in accordance with Chapter II of this Directive;
 - b. In the case of Member State whose legislation sets out a list of specific predicate offences, it shall, at a minimum, include in that list a comprehensive range of offences established in accordance with Chapter II of this Directive;
 - c. For the purposes of paragraph 3 (b) of this article, predicate offences shall include offences committed both within and outside the jurisdiction of the Member State in question.
 - d. Offences committed outside the jurisdiction of a Member State shall constitute predicate offences only when:
 - i. the relevant conduct is a criminal offence under the national law of the State where it is committed and
 - ii. would be a criminal offence under the national law of the Member State implementing or applying this Article, had it been committed there;
 - e. Each Member State shall furnish copies of its laws that give effect to this Article and of any subsequent changes to such laws or a description thereof to the ECOWAS Commission;
 - f. If required by fundamental principles of the national law of a Member State, it may be provided that the offences set forth in paragraph 1 of this Article do not apply to the persons who committed the predicate offence;
 - g. Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this Article may be inferred from objective factual circumstances.

Article 22 :Special categories of cybercrime involving emerging technologies

1. Each Member State may adopt necessary measures to ensure that cybercrime offences committed through or facilitated by emerging technologies, including technologies such as artificial intelligence, machine learning systems, quantum computing, blockchain platforms, deepfake technologies, and autonomous systems, are recognised and criminalised under domestic law.

2. Each Member State may treat as aggravated and subject to enhanced penalties as prescribed by domestic law any offence established under Chapter II of this Directive when committed through the use of emerging technologies that are designed or adapted primarily to facilitate the commission of an offence established under Chapter II of this Directive in a manner that:
 - a. obscures the identity or location of the perpetrator;
 - b. amplifies the scale, speed, or impact of the offence;
 - c. targets critical infrastructure, democratic institutions, or vulnerable populations;
or
 - d. involves automated or self-replicating systems capable of causing widespread harm.
3. Each Member State may establish mechanisms to monitor developments in emerging technologies, update national cybercrime legislation and relevant enforcement protocols accordingly, and endeavour that law enforcement and judicial authorities receive appropriate training for the detection, investigation, and prosecution of offences involving such technologies.
4. Member States may cooperate to harmonise definitions, investigative standards, and prosecutorial approaches relating to the criminal use of emerging technologies, and shall exchange information, best practices, and technical expertise through ECOWAS cooperation mechanisms.

Article 23: Attempt and aiding or abetting

Each Member State shall adopt necessary measures to criminalise, under its national law, the conduct of any person who intentionally:

- a. abets the commission of any offence established in accordance with this Directive;
- b. aids another person to commit such an offence;
- c. attempts to commit such an offence; or
- d. undertakes any act preparatory to or in furtherance of the commission of such an offence.

Article 24: Corporate criminal liability

1. Each Member State shall adopt necessary measures to ensure that legal persons can be held liable for offences established in accordance with this Directive, where such offences are committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
 - a. a power of representation of the legal person;
 - b. an authority to take decisions on behalf of the legal person; or
 - c. an authority to exercise control within the legal person.
2. Each Member State shall adopt necessary measures to ensure that a legal person can also be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 of this article has made possible the commission of an offence established in accordance with this Directive, for the benefit of that legal person, by a natural person acting under its authority.
3. Each Member State shall ensure that legal persons under this Article shall not exclude criminal proceedings against natural persons who are perpetrators, instigators or accessories in the offences concerned.

Article 25: Prosecution, adjudication and sanctions

1. Each Member State shall ensure that offences established in accordance with this Directive are subject to effective, proportionate, and dissuasive sanctions, taking into account the gravity of the offence.
2. Each Member State may, in accordance with national law, provide for aggravating circumstances in relation to such offences, including where critical infrastructure is affected.
3. Each Member State shall ensure that prosecution and enforcement measures are carried out effectively and in a manner that deters the commission of offences, while respecting the rights of the defence and the right to a fair trial.

4. Each Member State shall take appropriate measures to protect children accused of offences established in accordance with this Directive, consistent with the Convention on the Rights of the Child and other applicable international obligations.
5. Nothing in this Directive shall affect the principle that the definition of offences and defences, and the rules governing prosecution and punishment, are determined by national law.

CHAPTER IV – PROCEDURAL PROVISIONS

Article 26: Scope of procedural provisions

1. Each Member State shall adopt necessary measures to ensure that the procedural powers and provisions adopted under this Directive apply to:
 - a. the investigation and prosecution of criminal offences established under this Directive;
 - b. the investigation and prosecution of other criminal offences committed by means of a computer system under national law; and
 - c. the collection of evidence in electronic form in relation to any criminal offence under this Directive or other domestic law.
2. Each Member State shall ensure that evidence shall not be excluded solely on the ground that it has been generated, transmitted, seized or identified by means of a computer system.
3. Nothing in this Chapter shall be construed to prejudice or limit the application of existing provisions of law in Member States that empower competent authorities to preserve, collect, or make use of evidence, whether electronic or otherwise, in the course of investigations and prosecutions.

Article 27: Conditions and safeguards

Each Member State shall ensure that the establishment, implementation and application of the powers and procedures referred to in this Chapter are subject to conditions and safeguards, including:

- a. protection of human rights and freedoms as guaranteed under applicable regional and international instruments;
- b. judicial or other independent supervision;
- c. grounds justifying application of the measures; and
- d. limitations on the scope and duration of such powers.

Article 28: Expedited preservation of stored computer data

1. Each Member State shall adopt necessary measures to enable the competent authorities to order or otherwise obtain the expeditious preservation of specified stored computer data, including traffic data, that is relevant for the purposes of a criminal investigation or proceeding, in particular where there are grounds to believe that such data may be vulnerable to loss or modification.
2. Where an order is issued under paragraph 1 of this article, each Member State shall ensure that the service provider or other person in possession or control of the specified stored computer data are required to preserve and maintain the integrity of that data for a period of time determined under national law, sufficient to enable the competent authorities to seek its disclosure.
3. Each Member State may provide that preservation orders under paragraph 2 of this Article shall apply for a maximum period of up to ninety (90) days, subject to renewal as provided for by national law.
4. Each Member State shall adopt such measures as may be necessary to oblige service providers or other persons required to preserve stored computer data under this Article to keep confidential the undertaking of such preservation for the period of time provided under national law.

Article 29: Expedited preservation and partial disclosure of traffic data

1. Each Member State shall adopt necessary measures, in respect of traffic data that are to be preserved under Article 28 of this Directive, to ensure that the expeditious preservation of such traffic data is available regardless of whether one or more service providers were involved in the transmission of a communication.

2. Each Member State shall adopt such measures as may be necessary to ensure the expedited disclosure to the competent authorities, or to a person designated by such authorities, of a sufficient amount of traffic data to enable the identification of the service providers and the path through which the communication or the indicated information was transmitted.

Article 30: Production orders

1. Each Member State shall adopt necessary measures to empower judicial or other competent authorities to order a person in possession or control of specified computer data stored in a computer system or computer data storage medium to produce such data.
2. Each Member State shall adopt necessary measures to empower judicial or other competent authorities to order service providers offering services within their territory to provide subscriber information in their possession or control.
3. Each Member State shall take the necessary measures to ensure that a production order may be issued only upon application that sets out, where reasonable and possible, where it is believed that:
 - a. specified computer data or subscriber information sought is likely to be available with a person or service provider mentioned in paragraph 1 of this article;
 - b. an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information is produced;
 - c. the type of evidence suspected is likely to be produced by a person or service provider mentioned in paragraph 1 of this article;
 - d. subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data or subscriber information;
 - e. an identified offence is an offence in respect of which the production order is sought;
 - f. measures taken shall ensure that the specified computer data or subscriber information will be produced whilst maintaining the privacy of other users, customers and third parties.
4. Each Member State may take necessary measures to provide service providers with the express right to challenge before the relevant judicial or competent authority a production order on the grounds of relevance, privilege, or other legal objection to the

order or otherwise protected from disclosure by law, or non-satisfaction of the requirements in this article.

Article 31: Search and seizure of stored computer data

1. Each Member State shall adopt necessary measures to empower judicial or other competent authorities to order or similarly obtain the expeditious search, access, seizure or securing of computer data, computer programs or computer systems, where there are reasonable grounds to believe that such computer data, programs or computer systems are relevant for the purposes of a specific criminal investigation or proceeding.
2. Each Member State shall adopt necessary measures to ensure that, where its judicial or other competent authorities search or access a specific computer system or part of it, and have grounds to believe that the computer data or computer programs sought are stored in another computer system or part of it, and such data are lawfully accessible from or available to the initial system, those authorities are able to expeditiously extend the search to obtain access to that other computer system.
3. Each Member State shall ensure that the powers are exercised subject to appropriate safeguards, including judicial or other independent supervision, proportionality, and limitations on use of data for lawful purposes.
4. Each Member State shall take the necessary measures to ensure that an order for the search, access, seizure or securing of computer data, computer programs or computer systems may be issued upon application that sets out the following, where reasonable and possible:
 - a. an explanation of the reasons for believing that the material sought will be found during the exercise of the procedural power;
 - b. identification and specific description of the type of evidence suspected to be found;
 - c. identification and specific description of the relevant computer program or computer data sought, and the grounds for reasonably suspecting that such computer program or computer data is available on each individual computer system, device or computer data storage medium;

- d. identification and specific description of the individual computer systems, devices or computer data storage media to be searched or seized, together with the grounds for reasonably suspecting that they contain the relevant program, data or evidence;
 - e. a description of the technical measures to be taken to ensure that the search or seizure is carried out through appropriate forensic methods, such as mirroring or copying of relevant computer data, rather than through the physical removal of computer systems or devices, unless strictly necessary;
 - f. identification of any persons proposed to accompany the executing officer, together with the reasons necessitating their presence; and
 - g. a request, where appropriate, for the judicial or competent authority to accompany the executing officer during the execution of the procedural power.
5. Member States shall take the necessary measures to ensure that an executing officer shall, when executing this procedural power:
- a. at all times act with proportionality;
 - b. take all precautions to maintain integrity of the computer system, computer program and computer data subject of the search or seizure;
 - c. not disrupt or interfere with the integrity or running and operation of any computer system, computer program or computer data that is not the subject of the offences identified in the application;
 - d. avoid disruption to the continued legitimate business operations and the premises which may be subject to the procedural power;
 - e. at all times give due consideration to the rights of third parties;
 - f. avoid disruption to any computer system, computer program or computer data not connected with the computer system, computer program or computer data that is not the subject of the offences identified in the application or is not necessary for the investigation of such specified offence; and
 - g. only seize a computer system or computer data storage medium when it is not practical to seize or similarly secure the computer data or it is necessary to ensure that the computer data will not be destroyed, altered or otherwise interfered with.
6. Each Member State shall take the necessary measures to ensure that an executing officer shall, when following the execution of this procedural power or as soon as practicable after the search:

- a. make a list of what has been seized or similarly secured, with the date and time of seizure or similar securing; and
 - b. give a copy of that list to the person in control of the computer system, computer program or computer data.
- 7. Each Member State shall take necessary measures to ensure that an executing officer, on request, permit the following persons to access and copy computer data on the system or give such person a copy of the computer data:
 - a. who has custody or control of a computer system;
 - b. who has right to a computer program or computer data seized or similarly secured pursuant to this Article; or
 - c. acting on behalf of a person under paragraph 7(a) or (b) of this article, to access and copy the computer program or computer data on the computer system, or give such person a copy of the computer program or computer data.
- 8. Provided that an executing officer may refuse to give access or provide copies seized or similarly secured pursuant to this article if they have reasonable grounds to believe that granting access or providing copies would:
 - a. constitute a criminal offence; or
 - b. prejudice
 - i. an investigation; or
 - ii. any prosecution.
- 9. In such case, the aggrieved person may apply to the competent court for such access or copies.

Article 32: Real-time collection of traffic data

- 1. Each Member State shall adopt necessary measures to empower judicial or other competent authorities to:
 - a. collect or record, through the application of technical means in their territory, traffic data in real time associated with specified communications.
 - b. compel a service provider, within its existing technical capability, to:
 - i. collect or record, through the application of technical means in the territory of the Member State, traffic data in real time associated with specified communications; or
 - ii. cooperate with and assist the judicial or other competent authorities in the collection or recording of such traffic data.

2. Where, owing to the principles of its domestic legal system, a Member State cannot adopt the measures referred to in paragraph 1 of this Article, it may instead adopt such measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory through the application of technical means in that territory.
3. Each Member State shall adopt necessary measures to oblige service providers to keep confidential the fact of the execution of any power provided for in this Article, as well as any information relating to it, for the period of time provided under national law.
4. The application of measures under this article shall be subject to conditions and safeguards, including judicial or independent authorisation, proportionality, necessity, and limitations on the use and retention of the traffic data.
5. Each Member State shall take the necessary measures to ensure that an order for the collection or recording of traffic data may be issued only upon application that sets out, where reasonable and possible, why it is believed that:
 - a. the traffic data sought will be obtained if this procedural power is exercised;
 - b. the type of traffic data suspected to be found;
 - c. an identified offence is the offence for which the warrant is sought;
 - d. further disclosures are needed to achieve the purpose for which authorisation to exercise this procedural power, where authorisation to seek collection or recording on more than one occasion is needed;
 - e. measures taken shall ensure that the collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation;
 - f. the investigation may be frustrated or seriously prejudiced unless the collection or recording is permitted; and
 - g. to achieve the purpose for which the authorisation is being sought, collection or recording of the traffic data is necessary
6. Each Member State shall take the necessary measures to ensure that authorisation for the collection or recording of traffic data shall not be for a period beyond what is absolutely necessary and, in any event, not more than ninety (90) days, which period may be extended by notification to the judicial or competent authority of the Member State.

7. Each Member State may take the necessary measures to provide service providers with the express right to challenge before the relevant judicial or competent authority an order to conduct the real-time collection of traffic data on the ground of relevance, privilege, or other legal objection to the order or otherwise protected from disclosure by law, or non-satisfaction of the requirements in this article.

Article 33: Interception of content data

1. Each Member State shall adopt necessary measures, in relation to a range of serious criminal offences to be determined under national law, to empower judicial or other competent authorities to:
 - a. intercept, collect or record, through the application of technical means in their territory, the content data associated with specified communications in real time; and
 - b. compel a service provider, within its existing technical capability to:
 - i. intercept, collect or record, through the application of technical means in the territory of the Member State, the content data associated with specified communications in real time; or
 - ii. cooperate with and assist the judicial or other competent authorities in the interception, collection or recording of such content data.
2. Where, owing to the principles of its national legal system, a Member State cannot adopt the measures referred to in paragraph 1(a) of this article, it may instead adopt such measures as may be necessary to ensure the interception, collection or recording of the content data of specified communications transmitted in its territory, through the application of technical means in that territory.
3. Each Member State shall adopt necessary measures to oblige service providers to keep confidential the fact of the execution of any power provided for in this Article, as well as any information relating to it, for the period of time provided under national law.
4. The application of measures under this article shall be subject to conditions and safeguards, including judicial or independent authorisation, proportionality, necessity, and limitations on the use and retention of the content data.

5. Each Member State shall take the necessary measures to ensure that an order for the interception, collection or recording of content data may be issued only upon application that sets out, where reasonable and possible, where it is believed that:
 - a. the content data sought will be obtained if this procedural power is exercised;
 - b. the type of content data suspected to be found;
 - c. an identified offence is the offence for which the warrant is sought;
 - d. further disclosures are needed to achieve the purpose for which authorisation to exercise this procedural power, where authorisation to seek interception, collection or recording on more than one occasion is needed;
 - e. measures taken shall ensure that the interception, collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation;
 - f. the investigation may be frustrated or seriously prejudiced unless the interception, collecting or recording is permitted; and
 - g. to achieve the purpose for which the authorisation is being sought, interception, collecting or recording of the content data is necessary.
6. Each Member State shall take the necessary measures to ensure that authorisation for the interception, collection or recording of content data shall not be for a period beyond what is absolutely necessary and, in any event, not more than such period to be determined by national law.
7. Each Member State may take the necessary measures to provide service providers with the express right to challenge before the relevant judicial or competent authority an order to conduct the interception of content data on the ground of relevance, privilege, or other legal objection to the order or otherwise protected from disclosure by law, or non-satisfaction of the requirements in this article.

Article 34: Freezing, seizure and confiscation of the proceeds of crime

1. Each Member State shall adopt, to the greatest extent possible within their national legal system, such measures as may be necessary to enable the confiscation of:
 - a. proceeds of crime derived from offences established in accordance with this Directive or property the value of which corresponds to that of such proceeds;

b. property, equipment or other instrumentalities used in or destined for use in offences established in accordance with this Directive.

2. Each Member State shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this Article for the purpose of eventual confiscation.
3. Each Member State shall adopt, in accordance with their domestic law, necessary measures to regulate the administration by the judicial or other competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this Article.
4. Where proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this Article instead of the proceeds.
5. Where proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.
6. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, shall also be liable to the measures referred to in this Article, in the same manner and to the same extent as proceeds of crime.
7. For the purpose of this article and article 47 of this Directive, each Member State shall empower its judicial or other competent authorities to order that bank, financial or commercial records be made available or be seized.
8. Each Member State shall not decline to act under the provisions of this article on the ground of bank secrecy.
9. Each Member State may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of national law and with the nature of the judicial and other proceedings.
10. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

11. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with the provisions of the national law of a Member State.

Article 35: Liability of service providers

1. Each Member State shall adopt necessary measures to ensure that service providers are not subject to civil or criminal liability for information transmitted, routed, relayed, cached, stored, or otherwise made available through their services, unless it is established that the service provider had:
 - a. actual notice and specific actual knowledge of the unlawful activity or information; and
 - b. wilful and malicious intent to facilitate, aid, or abet such unlawful activity, beyond mere omission or failure to act.
2. The burden of proof in establishing liability under paragraph 1 of this Article shall rest with the party alleging such notice, knowledge, or intent.
3. Each Member State shall require that any such allegation against a service provider shall clearly and specifically identify the content, material, or conduct giving rise to the claimed liability.
4. Each Member State shall ensure that service providers are not, under any circumstance, held liable solely for maintaining or making available the provision of their services.
5. Each Member State shall ensure that service providers are not liable for the disclosure of data or other information where such disclosure is undertaken only to the extent required under national law or in compliance with a lawful order issued pursuant to provisions of this Chapter.
6. Each Member State shall adopt necessary measures to ensure that service providers are not subject to general obligations to proactively monitor, inquire into, or seek facts or circumstances relating to the content or information they transmit, route, cache, store, or otherwise make available.

7. Each Member State shall adopt necessary measures to ensure that service providers shall establish accessible and transparent reporting mechanisms and inform users of their rights and remedies.

Article 36 – Assistance to victims

1. Each Member State shall recognize the importance of ensuring the protection and effective assistance of a victims of cybercrime, with particular attention to any case involving a child.
2. Each Member State shall consider establishing appropriate mechanisms to address the physical, psychological, and economic harm suffered by victims.
3. Each Member State shall consider implementing effective procedures to:
 - a. safeguard the privacy and identity of victims, including the protection of their personal data;
 - b. provide avenues for compensation, including through the use of victim assistance funds, where such funds exist.
4. Member States shall engage in international cooperation aimed at preventing, mitigating, and addressing harms suffered by victims of cybercrime.

CHAPTER V – REGIONAL AND INTERNATIONAL COOPERATION

Article 37: General principles related to mutual assistance

1. Each Member State shall designate a central authority responsible for:
 - a. sending and answering requests for mutual legal assistance;
 - b. ensuring the execution of such requests or their transmission to the authorities competent for execution; and
 - c. carrying out the functions and powers provided under this Directive with respect to international cooperation.
2. Each Member State shall communicate the names and addresses of the authorities designated in pursuance of this Article to the ECOWAS Commission.

3. The ECOWAS Commission shall set up and keep updated a register of central authorities designated by the Member States. Each Member States shall ensure that the details held on the register are correct at all times.
4. Each Member State shall ensure that the central authority affords mutual legal assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences within the scope defined under article 26 of this Directive.
5. Each Member State shall ensure that, in urgent circumstances, the central authority may make or receive requests for mutual legal assistance, or related communications, by expedited means of communication, including electronic communications, provided that appropriate levels of security and authentication are maintained, including the use of encryption where necessary. Formal confirmation shall follow where required by the requested or requesting Member State.
6. Except as otherwise specifically provided in articles in this Chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Member State, or by applicable mutual assistance treaties or if the Member States concerned agree based upon this Directive, including the grounds on which the requested Member State may refuse co-operation.
7. The requested Member State shall not exercise the right to refuse mutual assistance in relation to the offences referred to in articles 2 to Articles 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
8. Where mutual legal assistance is conditional upon the existence of dual criminality, Each Member State shall ensure that the condition is deemed fulfilled, irrespective of whether their national law places the offence within the same category of offence or denominates the offence by the same terminology as the requesting Member State, if the conduct underlying the offence is a criminal offence under their national law.
9. Mutual assistance requests under this Chapter shall be executed in accordance with the procedures specified by the requesting Member State, except where incompatible with the law of the requested Member State.
10. Unless otherwise specified, the requested Member State may refuse assistance if:

- a. the request concerns an offence which the requested Member State considers a political offence or an offence connected with a political offence, or
- b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
- c. the request is not made in conformity with the provisions of this Article;
- d. there is an absence of dual criminality;
- e. the authorities of the requested Member State would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;
- f. the assistance would be contrary to the legal system of the requested Member State relating to mutual legal assistance for the request to be granted; or
- g. the requested Member State has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.
- h. if at the time of disclosure, it subsequently becomes clear to the requested Member State that the request pertains to paragraph 10 (b), (c), (d) and (g) of this article.

11. Reasons shall be given for any refusal of mutual legal assistance.

12. The requested Member State shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting Member State and for which reasons are given, preferably in the request.

13. The requested Member State shall respond to reasonable requests by the requesting Member State on the status, and progress in its handling, of the request.

14. The requested Member State may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

15. Before refusing or postponing assistance, the requested Member State shall, where appropriate after having consulted with the Member State, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

16. The requested Member State shall promptly inform the requesting Member State of the outcome of the execution of a request for assistance. Reasons shall be given for any

refusal or postponement of the request. The requested Member State shall also inform the requesting Member State of any reasons that render impossible the execution of the request or are likely to delay it significantly.

17.

- a. The requesting Member State may request that the requested Member State keep confidential the fact of any request made under this Chapter as well as its subject, except to the extent necessary for its execution. If the requested Member State cannot comply with the request for confidentiality, it shall promptly inform the requesting Member State, which shall then determine whether the request should nevertheless be executed.
- b. The requested Member State may make the supply of information or material in response to a request dependent on the condition that it is:
 - i. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
 - ii. not used for investigations or proceedings other than those stated in the request.
- c. Where the requesting Member State cannot comply with a condition referred to in paragraph 17 (b) of this article, it shall promptly inform the other Member State, which shall then determine whether the information should nevertheless be provided. When the requesting Member State accepts the condition, it shall be bound by it.
- d. Any Member State that supplies information or material subject to a condition referred to in paragraph 17 (b) of this Paragraph may require the other Party to explain, in relation to that condition, the use made of such information or material.

18.

- a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Member States to judicial authorities of the requested Member State. In any such cases, a copy shall be sent at the same time to the central authority of the requested Member State through the central authority of the requesting Member State.
- b. Any request or communication may be transmitted through the International Criminal Police Organisation (INTERPOL) or the West African Police Information System (WAPIS).
- c. Where a request is sent directly to a judicial authority of the requested Member State that is not competent to deal with it, the judicial authority of the requested

Member shall refer the request to the central authority of the requested Member State and inform the judicial authority that made the request of such referral.

- d. Requests or communications that do not involve coercive measures may be transmitted directly by the judicial authority of the requesting Member State to the judicial authority of the requested Member State.
- e. The judicial authority of the requested Member State shall only carry out the measures under this paragraph if permitted under the national law of the requested Member State.
- f. The judicial authority of a requested Member State shall only make disclosure to the judicial authority of the requesting Member State based upon any request for mutual assistance upon approval by the central authority.

Article 38: Spontaneous information

- 1. Each Member State shall adopt necessary measures to enable their competent authority to, without prior request, forward to a third country information obtained within the framework of its own investigations, where it considers that such disclosure may:
 - a. assist the third country in initiating or carrying out investigations or proceedings;
or
 - b. lead to a request for cooperation under this Directive or other applicable international instruments to which a Member State is a party.
- 2. Each Member State shall ensure that the competent authority, prior to providing the information, requests that it be kept confidential or used subject to specified conditions.
- 3. Each Member State shall ensure that where the receiving State cannot comply with such conditions, it shall notify the transmitting authority, which shall then determine whether the information should nevertheless be provided. Where the receiving State accepts the information subject to conditions, it shall be bound by them.
- 4. Each Member State shall ensure that any evidence or information received pursuant to this article shall not be denied admissibility in criminal proceedings solely on the grounds that it was transmitted without a formal mutual legal assistance request.
- 5. Each Member State shall ensure that the receipt of spontaneous information pursuant to this article shall not preclude the receiving State from submitting subsequent requests for mutual legal assistance related to the same facts, conduct, or evidence.

Article 39: Expedited preservation of stored computer data

1. Each Member State shall adopt necessary measures to enable their competent authority to, upon request of a third country or applicable competent multilateral organisation, order or otherwise obtain the expeditious preservation of specified stored computer data located within their territory or under their control, where the requesting authority intends to submit a request for mutual legal assistance for the search, access, seizure, securing or disclosure of such computer data.
2. Each Member State shall ensure that a request for preservation includes, to the extent possible:
 - a. the identity of the authority seeking the preservation;
 - b. the offence that is the subject of the investigation or proceedings, including a brief summary of the relevant facts;
 - c. the stored computer data to be preserved and its relationship to the offence;
 - d. any available information identifying the custodian of the stored computer data or the location of the computer system;
 - e. the necessity of the preservation; and
 - f. confirmation that the requesting authority intends to submit a request for mutual legal assistance relating to the search, access, seizure, securing or disclosure of the computer data.
3. Each Member State shall ensure that their competent authority takes appropriate measures to preserve the specified computer data expeditiously in accordance with the procedures and powers provided under domestic law implementing this Directive.
4.
 - a. A Member State may not refuse preservation under this article with respect to any offence established pursuant to Chapter I of this Directive solely on the grounds that the condition of dual criminality has not been met.
 - b. For any other offence, where a Member State that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data, such Member State may reserve the right to refuse the request for preservation under this article with respect to any other offences where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5. In addition, a request for preservation may only be refused if:
 - a. the request concerns an offence which the requested Member State considers a political offence or an offence connected with a political offence;
 - b. the requested Member State considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests; or
 - c. if at the time of disclosure, it subsequently becomes clear to the requested Member State that the request pertains to paragraph 5 (a) or (b) of this article.
6. Where a requested Member State believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Member State's investigation, it shall promptly so inform the requesting Member State, which shall then determine whether the request should nevertheless be executed.
7. Each Member State shall ensure that any preservation effected in response to such a request shall be for a period of not less than sixty (60) days, to allow the requesting authority to submit the corresponding mutual legal assistance request. Following receipt of a request, the computer data shall continue to be preserved until a final decision has been taken on that request.

Article 40: Expedited disclosure of preserved traffic data

1. Where, in the course of executing a request under Article 39 or otherwise in relation to a specified communication, a Member State discovers that a service provider in a foreign state was involved in the transmission of the communication, the Member State shall expeditiously disclose to the requesting foreign government or applicable competent multilateral organisation a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 of this Article may only be withheld where:
 - a. the request concerns an offence which the requested Member State considers a political offence or an offence connected with a political offence;
 - b. the requested Member State considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests; or
 - c. at the time of disclosure, it subsequently becomes clear to the requested Member State that the request pertains to paragraph 2 (a) or (b) of this Article.

- d. the authorities of the Member State would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction; or
- e. the Member State has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

Article 41: Mutual assistance in the search, seizure and disclosure of stored computer data

1. Each Member State shall adopt necessary measures to empower their competent authorities, upon request by the Government of a third country or applicable competent multilateral organisation to order or otherwise carry out the search or similar access to, seizure or similar securing of, and disclosure of computer programs or computer data stored by means of a computer system within their territory, including data preserved pursuant to article 39 of this article.
2. Requests for mutual legal assistance under this article shall, as far as practicable and available, specify:
 - a. the authority conducting the investigation or proceeding to which the request relates;
 - b. the nature of the criminal matter, with a summary of relevant facts and applicable law;
 - c. the purpose of the request and the type of assistance sought;
 - d. in the case of restraint or confiscation of assets believed to be located in the requested Member State, particulars of the offence, of any investigation or proceeding commenced in respect of the offence, and a copy of any relevant restraining or confiscation order;
 - e. details of any procedure to be followed in giving effect to the request, particularly in relation to the taking of evidence;
 - f. any confidentiality requirements and the reasons for them;
 - g. the period within which the requesting Member State seeks compliance;
 - h. where applicable, details of the property, computer, computer system or device to be traced, restrained, seized or confiscated, and the grounds for believing that the property is located in the requested Member State;

- i. details of the stored computer data or computer program to be seized and its relationship to the offence;
 - j. any available information identifying the custodian of the stored computer data or computer program or the location of the computer system or device;
 - k. arrangements concerning the allocation of costs or damages arising from execution of the request; and
 - l. any other information relevant to effective execution.
- 3. Upon receiving a request under this Article, the competent authority of the requested Member State shall take all appropriate measures, including seeking any necessary judicial or administrative authorisations, to execute the request in accordance with domestic procedures and powers under this Directive.
- 4. Where necessary and consistent with national law, the competent authority may seek the cooperation or participation of the requesting Member State or applicable competent multilateral organisation in the execution of the search and seizure.
- 5. The requested Member State may transmit the results of the search and seizure, together with any electronic evidence obtained, to the requesting Member State or applicable competent multilateral organisation.
- 6. Mutual assistance under this Article may be refused on the grounds mentioned in paragraph 9 of article 37 of this Directive.

Article 42: Mutual assistance in the real-time collection of traffic data

- 1. Each Member State shall adopt necessary measures to empower their competent authorities, upon request by a foreign Government or applicable competent multilateral organisation to provide assistance in the real-time collection or recording of traffic data associated with specified communications transmitted by means of a computer system within the territory of the Member State.
- 2. A request for assistance under this article shall, as far as practicable and available, specify:
 - a. the name of the requesting authority;
 - b. the offence that is the subject of a criminal investigation or proceeding and a summary of the related facts;

- c. the authority or service provider with access to the relevant traffic data;
 - d. any available data that identifies the owner or user of the data or the location of the computer system;
 - e. the intended purpose for which the traffic data is sought;
 - f. sufficient information to identify the traffic data;
 - g. any further details relevant to the traffic data;
 - h. justification for the need to collect the traffic data;
 - i. the period for which traffic data are to be collected and a corresponding justification of its duration; and
 - j. the terms or limitations governing the use or onward disclosure of the traffic data to third parties.
3. Upon receiving a request under this Article, a Member State shall take all appropriate measures to obtain any necessary authorisation, including warrants, to execute the request in accordance with the procedures and powers provided under this Directive.
 4. Where consistent with national law, the Member State may seek the cooperation of the requesting third country Government or relevant competent multilateral organisation in the execution of measures under this Article.
 5. Upon carrying out the measures under this Article, the Member State may transmit the results of the real-time collection of traffic data associated with specified communications to the requesting third country Government or relevant competent multilateral organisation.
 6. Mutual assistance under this Article may be refused on the grounds mentioned in paragraph 9 of article 37 of this Directive.

Article 43: Mutual assistance in interception of content data

1. Each Member State shall adopt necessary measures to empower their competent authorities, upon request by a foreign Government or applicable competent multilateral organisation to provide assistance in the interception, collection or recording of content data associated with specified communications transmitted by means of a computer system in the territory of a Member State.
2. A request for assistance under this Article shall so far as practicable specify:

- a. the authority seeking the use of powers under this Article;
 - b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
 - c. the name of the authority with access to the relevant communication;
 - d. the location at which or nature of the communication;
 - e. the intended purpose for the required communication;
 - f. sufficient information to identify the communications;
 - g. details of the data of the relevant interception;
 - h. the recipient of the communication;
 - i. the intended duration for the use of the communication;
 - j. the necessity for use of powers under this Article; and
 - k. the terms for the use and disclosure of the communication to third parties.
3. Upon receiving the request under this Article, the Member State shall, if the request is in relation to an offence punishable for at least such period as may be prescribed under its domestic law, take all appropriate measures to obtain necessary authorisation including any warrants to execute upon the request in accordance with the procedures and powers provided under this Directive.
 4. Upon obtaining necessary authorisation including any warrants to execute upon the request, the Member State may seek the support and cooperation of the third country Government or applicable competent multilateral organisation during the search and seizure.
 5. Upon conducting the measures under this Article, the Member State may transmit the results of such measures as well as interception, collection or recording of content data associated with specified communications to the third country Government or relevant competent multilateral organisation.
 6. Mutual assistance under this Article may be refused on the grounds mentioned in paragraph 9 of Article 37 of this Directive.

Article 44: Trans-border access to stored computer data where publicly available or with consent

1. Each Member State shall ensure that their competent authorities are empowered, without requiring prior authorisation from another Member State, to:

- a. access publicly available stored computer data, regardless of the geographical location of such data;
- b. access or receive, through a computer system within their territory, stored computer data located in another Member State, where the lawful and voluntary consent of the person having the authority to disclose the data has been obtained; or
- c. access or receive, through a computer system in the Member State, stored computer data located outside the Member State, where there is a situation in which:
 - i. there is a significant and imminent risk to the life or safety of individuals, or
 - ii. there has been significant economic harm, either in terms of quantum or the number of victims in the Member State,
 and the use of other mutual assistance procedures would irreparably prejudice ability of the Member State to investigate and prosecute an offence, provided that the competent authority shall notify the country where the data was located as soon as practicable after accessing or receiving the computer data.

2. Each Member State shall ensure that such measures are implemented in accordance with their domestic law and with due regard to applicable international obligations

Article 45: Law enforcement cooperation

1. Member States shall cooperate closely with one another, consistent with their respective national legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences established in accordance with this Directive. Member States shall, in particular, take effective measures to:
 - a. enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services, taking into account existing channels, including those of the International Criminal Police Organization (INTERPOL) or the West African Police Information System (WAPIS), in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences established in accordance with this Directive, including, if the Member States concerned deem it appropriate, links with other criminal activities;
 - b. cooperate with other Member States in conducting inquiries with respect to offences established in accordance with this Directive concerning:

- i. the identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;
 - ii. the movement of proceeds of crime or property derived from the commission of such offences;
 - iii. the movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;
 - c. provide, where appropriate, necessary items or data for analytical or investigative purposes;
 - d. exchange, where appropriate, information with other Member States concerning specific means and methods used to commit the offences established in accordance with this Directive, including the use of false identities, forged, altered or false documents and other means of concealing activities, as well as cybercrime tactics, techniques and procedures;
 - e. facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the Member States concerned, the posting of liaison officers;
 - f. exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences established in accordance with this Directive.
2. With a view to giving effect to this Directive, Member States shall:
- a. consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them.
 - b. in the absence of such agreements or arrangements between the Member States concerned, consider this Directive to be the basis for mutual law enforcement cooperation in respect of the offences established in accordance with this Directive.
 - c. whenever appropriate, make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

Article 46: Joint Investigations

1. Member States shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to offences established in accordance with this Directive that are the subject of criminal investigations, prosecutions or judicial proceedings in one or more Member States, the competent authorities concerned may establish joint investigative bodies.
2. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis.
3. The Member States involved shall ensure that the sovereignty of the Member State in whose territory such investigations are to take place is fully respected.

Article 47: Mechanisms for recovery of property through international cooperation in confiscation

1. Each Member State, in order to provide mutual legal assistance pursuant to article 48 of this Directive with respect to property acquired through or involved in the commission of an offence established in accordance with this Directive, shall, in accordance with its national law:
 - a. take such measures as may be necessary to permit its competent authorities to give effect to an order of confiscation issued by a court of another Member State;
 - b. take such measures as may be necessary to permit its competent authorities, where they have jurisdiction, to order the confiscation of such property of foreign origin by adjudication of an offence of money-laundering or such other offence as may be within its jurisdiction or by other procedures authorised under its national law; and
 - c. consider taking such measures as may be necessary to allow confiscation of such property without a criminal conviction in cases in which the offender cannot be prosecuted by reason of death, flight or absence or in other appropriate cases.
2. Each Member State, in order to provide mutual legal assistance upon a request made pursuant to paragraph 2 of Article 48 of this Directive, shall, in accordance with its national law:
 - a. take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a freezing or seizure order issued by a court or competent authority of a requesting Member State that provides a reasonable basis for the requested Member State to believe that there are sufficient grounds

- for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1(a) of this Article;
- b. take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a request that provides a reasonable basis for the requested Member State to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1(a) of this Article; and
 - c. consider taking additional measures to permit its competent authorities to preserve property for confiscation, such as on the basis of a foreign arrest or criminal charge related to the acquisition of such property.

Article 48: International cooperation for the purposes of confiscation

1. A Member State that has received a request from another Member State having jurisdiction over an offence established in accordance with this Directive for the confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in Article 34, paragraph 1, of this Directive situated in its territory may, to the greatest extent possible within its domestic legal system, submit:
 - a. the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or
 - b. to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting Member State in accordance with Article 34(1) of this Directive insofar as it relates to proceeds of crime, property, equipment or other instrumentalities situated in the territory of the requested Member State.
2. Following a request made by another Member State having jurisdiction over an offence established in accordance with this Directive, the requested Member State shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in Article 34(1) of this Directive for the purpose of eventual confiscation to be ordered either by the requesting Member State or, pursuant to a request under paragraph 1 of this Article, by the requested Member State.
3. The decisions or actions provided for in paragraphs 1 and 2 of this Article shall be taken by the requested Member State in accordance with and subject to the provisions of its

domestic law and its procedural rules or any bilateral or multilateral treaty, agreement or arrangement to which it may be bound in relation to the requesting Member State.

4. Each Member State shall furnish copies of its laws and regulations that give effect to this Article and of any subsequent changes to such laws and regulations or a description thereof to the ECOWAS Commission. Where a Member State elects to make the taking of the measures referred to in paragraphs 1 and 2 of this Article conditional on the existence of a relevant treaty, that Member State shall consider this Directive the necessary and sufficient treaty basis.
5. Cooperation under this Article may also be refused or provisional measures may be lifted where the requested Member State does not receive sufficient and timely evidence or where the property is of minimal value.
6. Before lifting any provisional measure taken pursuant to this Article, the requested Member State shall, wherever possible, give the requesting Member State an opportunity to present its reasons in favour of continuing the measure.
7. The provisions of this Article shall not be construed as prejudicing the rights of bona fide third parties. Member States shall consider concluding bilateral or multilateral treaties, agreements or arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this Article.

Article 49: 24/7 network

1. Each Member State shall designate a national point of contact available on a twenty-four hour, seven-day-a-week (24/7) basis, in order to provide immediate assistance for the purposes of investigations or proceedings concerning criminal offences within the scope of this Directive.
2. Each designated point of contact shall have the authority to:
 - a. provide technical advice to other points of contact;
 - b. facilitate the preservation of data and the partial disclosure of traffic data pursuant to article 28 and 29 of this Directive;
 - c. support the collection of evidence, the provision of legal information, and the location of suspects;
 - d. facilitate and expedite communication with the competent national authority responsible for mutual legal assistance;

- e. provide computer data to avert an emergency;
 - f. provide accessible contact details and procedural information to other points of contact;
 - g. promptly transmit formal requests received to the competent national authority;
 - h. maintain direct communication with foreign points of contact, law enforcement agencies, and international networks, and encourage information-sharing prior to the submission of mutual legal assistance requests;
 - i. exchange, where appropriate, information informally with foreign counterparts;
 - j. participate in joint investigations or task forces with foreign or regional authorities for the purpose of detecting, preventing, investigating, and prosecuting offences within the scope of this Directive; and
 - k. utilise secure platforms and networks for the exchange of information and data.
3. Each Member State shall ensure that the designated point of contact is adequately resourced and equipped with the technical capacity to communicate securely and efficiently with other points of contact on an expedited basis. Where the point of contact designated by a Member State is not part of authority or authorities of that Member State responsible for mutual legal assistance, the point of contact shall ensure that it is able to coordinate with that authority or those authorities on an expedited basis.
4. Each Member State shall ensure that trained and equipped personnel are available to ensure the operation of the 24/7 network.
5. Each Member State may use and strengthen existing authorised networks of points of contact, where applicable, and within the limits of their domestic laws, including the 24/7 networks established pursuant to other international or regional instruments or the 24/7 networks for computer-related crime of the INTERPOL and WAPIS for prompt police-to-police cooperation and other methods of information exchange cooperation.

CHAPTER VI – IMPLEMENTATION

Article 50: Implementation

1. Each Member State shall adopt the necessary legislative, regulatory and administrative measures to comply with this Directive not later than three (3) years from the date of signature of this Directive.

2. The measures referred to in Paragraph 1 of this Article shall make reference to this Directive or shall be accompanied by such reference upon their official publication.
3. Each Member State shall inform the ECOWAS Commission of the measures they will adopt to comply with this Directive.
4. Each Member State shall notify the President of the Commission of the difficulties they encounter in implementing this Directive. The President of the Commission shall report such difficulties at the next session of the Council of Ministers which shall, in turn, take the appropriate measures to ensure the effective implementation of this Directive.

CHAPTER VII – FINAL PROVISIONS

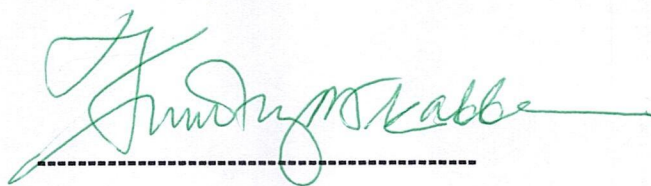
Article 51 – Publication

1. This **DIRECTIVE DIR.1/7/26** shall be published by the Commission in the Official Journal of the Community within thirty (30) days of its signature by the Chairperson of the Council of Ministers.
2. It shall also be published by each Member State in its National Gazette within the same timeframe.

Article 52 – Entry into force

This **DIRECTIVE DIR.1/7/26** shall enter into force upon Publication.

DONE IN FREETOWN, THIS 17TH DAY OF JULY 2026



H.E. ALHAJI MUSA TIMOTHY KABBA

FOR THE COUNCIL,

THE CHAIRPERSON