COMPILED ANNEXES TO THE

AFRICAN CONTINENTAL FREE TRADE AREA PROTOCOL ON DIGITAL TRADE

ANNEX ON

RULES OF ORIGIN

PART I

GENERAL PROVISIONS

Article 1
Definitions

For the purpose of this Annex:

a. **"Annex"** means the Annex on Rules of Origin to the Protocol;

b. **"Content"** means a digital product as defined in Article 1(h) of the Protocol;

c. **"Digital Platform"** means a digital interface or application which enables interactions and transactions between businesses and/or consumers to facilitate digital trade, including, but not limited to, online marketplaces, collaborative or sharing economy platforms, communication platforms, online social networks, online search engines, web browsers, online maps, news aggregators, music platforms, video and other media sharing platforms, digital payment systems, application stores, online advertising platforms, operating systems, and online intermediary services;

d. **"Enterprise"** means any juridical person duly constituted, registered, or otherwise incorporated and operated under the applicable laws and regulations of a State Party;

e. **"Juridical Person"** means a legal entity duly constituted, registered, or otherwise incorporated and operated under the applicable laws and regulations of a State Party;

f. **"Natural Person"** means a national of a State Party in accordance with its laws and regulations. For greater certainty, a natural person who holds dual nationality shall be deemed to be exclusively a national of the country of his or her effective nationality or where he or she ordinarily or permanently resides;

g. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol; and

h. **"Rules of Origin"** means rules established in this Annex to determine the origin of African-owned enterprises, African digital platforms and African content, and digital products, as stipulated in Article 5 of the Protocol.

Article 2
Objectives

The objectives of this Annex are to:

a. give effect to Article 5 of the Protocol;
b. facilitate the development of the AfCFTA digital market;
c. promote the development and growth of African-owned enterprises, African digital platforms, and African content;
d. promote trade in African content by African-owned enterprises and the use of African digital platforms; and
e. establish transparent and predictable criteria for determining eligibility for preferential treatment under the Protocol.

PART II

SCOPE OF DIGITAL PRODUCTS

Article 3

Digital Products

1. In accordance with Article 1(h) of the Protocol, the scope of digital products covered by the Protocol includes:
    a. electronic programmes;
    b. texts;
    c. videos;
    d. images;
    e. sound recordings; or
    f. any other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically.

2. A digitised representation of a financial instrument, including money, shall not be covered as a digital product under the Protocol.

PART III

ORIGIN OF AN AFRICAN-OWNED ENTERPRISE, AFRICAN DIGITAL PLATFORM, AND AFRICAN CONTENT

Article 4

African-Owned Enterprise

1. An African-owned enterprise is a legal entity duly constituted, registered, or otherwise incorporated and operated under the applicable laws and regulations of a State Party, owned and controlled by a natural or juridical person of a State Party or State Parties, and which maintains substantial business operations in the territory of a State Party.

2. For greater certainty, an African-owned enterprise is:
    a. owned by natural or juridical person(s) of a State Party or State Parties if such person beneficially owns more than 50 per cent of the equity interest of the enterprise; and
    b. controlled by natural or juridical person(s) of a State Party or State Parties if such person has the power to appoint a majority of its directors or otherwise to legally direct the operations of the enterprise.

3. The substantial business operations referred to in this Article shall be assessed in accordance with the definition of substantial business activity in Article 1 of the Protocol on Investment.

4. State Parties shall, in line with Article 22(3) of the Protocol, encourage African-owned enterprises to establish and use computing facilities within State Parties.

Article 5

African Digital Platform

1. A digital platform as defined in Article 1(c) of this Annex is African if it is duly constituted, registered, or otherwise incorporated and operated under the applicable laws and regulations of a State Party, and owned and controlled by a natural or juridical person(s) of a State Party or State Parties.

2. For greater certainty, an African digital platform is:
    a. owned by a natural or juridical person(s) of a State Party or State Parties if such person(s) beneficially owns more than 50 per cent of the equity interest of the digital platform; and
    b. controlled by a natural or juridical person(s) of a State Party or State Parties if such person(s) has the power to appoint a majority of its directors or otherwise to legally direct the operations of the digital platform.

3. State Parties shall, in line with Article 22(3) of the Protocol, encourage African digital platforms to use computing facilities established within State Parties.

4. State Parties shall promote and encourage the establishment and use of African digital platforms by African-owned enterprises.

Article 6

African Content

1. Content is African if it is owned by a natural or juridical person of a State Party in accordance with the applicable laws and regulations of a State Party.

2. For greater certainty, African content shall be interpreted as a digital product originating from State Parties as stipulated in Article 6(1) of the Protocol.

Article 7

Eligibility for Preferential Treatment

1. African content traded by African-owned enterprises or persons of State Parties or on African digital platforms shall be eligible for preferential treatment under the Protocol.

2. State Parties shall, in the application of this Annex, accord favourable treatment to African start-ups, Micro, Small and Medium-Sized Enterprises (MSMEs), women, youth, indigenous peoples, rural and local communities, persons with disabilities, and other underrepresented groups.

PART IV

PROMOTION OF INTRA-AFRICAN DIGITAL TRADE

Article 8

Measures to Promote Intra-African Digital Trade

State Parties are encouraged to introduce measures to promote the development of African-owned enterprises, African digital platforms, and African content. Measures referred to in this Article include, but are not limited to:

a. providing technical and financial support targeted at developing African content, African-owned enterprises, and African digital platforms;

b. promoting and facilitating the use of the dot Africa (.africa) domain for use by African-owned enterprises, African digital platforms, and persons of State Parties;
c. establishing a fund under the AfCFTA Adjustment Fund that accepts voluntary contributions from State Parties, the private sector, development partners, and other relevant stakeholders for the development and growth of African content, African-owned enterprises, and African digital platforms;
d. promoting the development and enhancement of digital platforms to promote greater levels of participation of MSMEs, women, youth, indigenous peoples, rural and local communities, persons with disabilities, and other underrepresented groups in digital trade through, among others, funding via fee rebates for onboarding, subscription, and advertising credits or targeted promotions;
e. fostering the transfer of technology, skills, know-how, innovation, and other benefits between foreign and African-owned enterprises or digital platforms to strengthen African capabilities;
f. encouraging international enterprises, platforms, and content creators to contribute to the development of African owned-enterprises, digital platforms, and content creators through financial assistance and skills development;
g. addressing economic and development disparities of MSMEs, women, youth, indigenous peoples, persons with disabilities, rural and local communities, and other underrepresented groups; and
h. providing training in research, engineering, design, and other relevant areas pertaining to the development of African digital platforms, African content, and digital products.

PART V

FINAL PROVISIONS

Article 9

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex to facilitate its effective implementation and enforcement.

Article 10

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 11

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 12

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese and Spanish languages, all of which are equally authentic.

ANNEX ON

CRITERIA FOR DETERMINING THE LEGITIMATE AND LEGAL PUBLIC INTEREST REASONS FOR DISCLOSURE OF SOURCE CODE

PART I

GENERAL PROVISIONS

Article 1

Definitions

For the purpose of this Annex:

a. **"Algorithm"** means a defined set of digital sequential procedures used to solve a particular problem or execute or perform a particular task;
b. **"Annex"** means Annex on Criteria for Determining the Legitimate and Legal Public Interest Reasons for Disclosure of Source Code to the Protocol;
c. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol;
d. **"Software"** means a programme or series of programmes, containing instructions for a computer required either for the operational processes of the computer itself or for the execution of specific tasks; and
e. **"Source Code"** means a set of programmed instructions written by a programmer, using a specific programming language to execute or perform particular tasks or functions, which is typically a human-readable version and can be executed by a computer to form the foundation of a software.

.

Article 2

Objectives

The objectives of this Annex are to:

a. give effect to Article 24(2) of the Protocol;
b. promote legitimate and legal public interests and technology transfer in digital trade regulation without prejudice to legitimate commercial interests, technological innovation, as well as the protection and enforcement of intellectual property rights in the AfCFTA digital market; and
c. strike an appropriate balance between public and private interests in respect of socio-economic and technological development.

PART II

LEGITIMATE AND LEGAL PUBLIC INTEREST OBJECTIVES

Article 3

Legitimate and Legal Public Interests

A regulatory body or judicial authority of a State Party may, in accordance with Article 24(2) of the Protocol, require a person of another State Party to preserve and make available the source code of the software or an algorithm expressed in that source code, subject to safeguards against unauthorised disclosure under the law or practice of a State Party, in order to pursue legitimate and legal public interest objectives including to:

a. maintain public order and safety;
b. protect public morals;
c. protect human, animal or plant life or health;
d. protect essential security interests;
e. protect and access critical infrastructure;
f. prevent deceptive and fraudulent practices; or
g. prevent arbitrary or unjustifiable discrimination.

PART III

SAFEGUARDS AND PROCEDURES

Article 4

Safeguards

1. A regulatory body or judicial authority of a State Party, requiring transfer or access to a source code or algorithm thereof under this Annex, shall protect the source code of the software or an algorithm expressed in that source code preserved and availed to them by a person of the State Party in accordance with Article 3 of this Annex against unlawful access, acquisition, or appropriation by a third party.

2. A regulatory body or judicial authority of a State Party, requiring transfer or access to a source code or algorithm thereof under this Annex, shall not apply Article 3 of this Annex in a manner which:
    a. constitutes a disguised restriction to digital trade or dishonest commercial practice;
    b. constitutes a means of arbitrary or unjustifiable discrimination;
    c. unreasonably prejudices the legitimate interests of the affected person of a State Party;
    d. is inconsistent with the protection and enforcement of intellectual property rights in the AfCFTA digital market; or
    e. restricts digital trade more than necessary to achieve legitimate and legal public interest objectives.

3. For greater certainty, dishonest commercial practices referred to in paragraph 2 of this Article include practices such as breach of contract, breach of confidence, and inducement to breach, and the acquisition of preserved or availed source code of software or an algorithm expressed in that source code or algorithm thereof by third parties.

4. For greater certainty, a third party referred to in this Article includes a natural or juridical person other than the owner of the source code, including a public authority, agency, or body of a State Party or a Third Party as defined in Article 1(u) of the Protocol.

Article 5

Cybersecurity

1. A regulatory body or judicial authority of a State Party, requiring transfer or access to a source code or algorithm expressed in that source code in accordance with Article 3 of this Annex, shall adopt or maintain measures necessary to protect such source code or algorithm thereof against data leaks as well as cybercrimes and cyberthreats.

2. A regulatory body or judicial authority of a State Party, requiring or obtaining access to a source code or algorithm expressed in that source code in accordance with Article 3 of this Annex, shall demonstrate competence to any relevant authority mutually agreed to by both parties in the management of cybersecurity incidents, mitigating malicious intrusions, or using mechanisms necessary to address cybersecurity incidents.

3. A regulatory body or judicial authority of a State Party, which does not comply with the obligations referred to in paragraphs 1 and 2 of this Article shall be denied access to a source code or algorithm expressed in that source code.

Article 6

Fair and Reasonable Procedures

1. Where a source code or algorithm thereof has been requested and availed in accordance with Article 3 of this Annex, a regulatory body or judicial authority of a State Party shall, within three (3) months from the date of submission of the source code or algorithm expressed in that source code by a person of a State Party, inform the affected person of a State Party of the decision concerning the request.

2. Each State Party shall adopt or maintain transparent, fair, and reasonable procedures, which provide an affected person of another State Party with prompt and impartial review and appeal of the decision referred to in paragraph 1 of this Article, and where applicable, appropriate remedies.

3. State Parties shall promptly publish or make publicly available decisions or procedures referred to in this Article, subject to Article 41 of the Protocol.

Article 7

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application affecting or pertaining to requiring access to or transfer of source code of software or an algorithm expressed in that source code; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new laws and regulations or amendments to existing laws and regulations, or any measures pertaining to, affecting or requiring access to or transfer of source code of software or an algorithm expressed in that source code.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

PART IV

FINAL PROVISIONS

Article 8

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex to facilitate its effective implementation and enforcement.

Article 9

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 10

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement.

Article 11

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON

ONLINE SAFETY AND SECURITY

Article 1

Definitions

For the purpose of this Annex:

a. **"Annex"** means the Annex on Online Safety and Security to the Protocol;
b. **"Child"** means a natural person below the age of 18 years;
c. **"Child Sexual Abuse Material"** means any written, audio, or visual depiction, including any photograph, film, video, or image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
    i. the production of such visual depiction involves a child;
    ii. such visual depiction is a digital image, computer image, or computer-generated image where a child is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge; and
    iii. such visual depiction has been created, adapted, or modified to appear that a child is engaging in sexually explicit conduct.
d. **"Competent Authority"** means a public body, agency, regulator, or any authority designated or empowered by the domestic law of a State Party to execute and enforce measures pertaining to online safety and security covered under this Annex;
e. **"Critical Infrastructure"** means services and facilities, including digital and physical assets, systems, and networks, that are essential for the proper functioning of the national economy, public health, or safety and security of a State Party;
f. **"Cyberbullying"** means the use of electronic means to intentionally harass, threaten, embarrass, humiliate, or otherwise target another natural person**;**
g. **"Digital Platform"** means a digital platform as defined in Article 1(c) of the Annex on Rules of Origin to the Protocol;
h. **"Illegal Content"** means any information that, in itself or in relation to an activity, including the sale of products or the provision of services, violates the laws and regulations of any State Party;
i. **"Online Threat"** means any activity, behaviour, or content that poses a risk to online safety and security;
j. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol;
k. **"Racism"** means any written material, picture, or any other representation of ideas or theories that advocates, encourages, or incites hatred, discrimination, or violence against any person or group of persons for reasons based on race, colour, ancestry, national or ethnic origin, or religion; and
l. **"Sensitive Personal Data"** means sensitive personal data as defined in Article 1(l) of the Annex on Cross-Border Data Transfers to the Protocol.

Article 2

Objectives

The objectives of this Annex are to:

a. give effect to Article 29(2) of the Protocol;

b. foster a safe and secure online environment that supports digital trade, innovation, socio-economic growth and development, and the protection of human rights;
c. strengthen multi-stakeholder cooperation and collaboration between State Parties, law enforcement authorities, regulators, relevant industry, consumers, and civil society on online safety and security concerns in digital trade; and
d. establish predictable and transparent harmonised rules for online safety and security in digital trade.

Article 3

Protection of Personal Data, Cybersecurity, Online Consumer Protection and Unsolicited Commercial Electronic Communications

State Parties shall adopt or maintain measures for the protection of personal data, and to ensure cybersecurity, online consumer protection, and to combat unsolicited commercial electronic communications in accordance with Articles 21, 25, 27 and 28 of the Protocol.

Article 4

Critical Infrastructure

1. State Parties shall adopt or maintain laws and regulations for the maintenance and protection of critical infrastructure from any disruption, destruction, or interference.

2. State Parties shall adopt a risk-based approach to identify and address critical infrastructure where a cybersecurity incident could result in catastrophic continental, regional, or national effects on public health and safety, economic, and financial security or essential security interests.

Article 5

Duty of Care

1. Each State Party shall adopt or maintain laws and regulations to foster a safe and secure online environment that supports digital trade.

2. Each State Party shall require enterprises constituted, registered, or otherwise incorporated or operating in its jurisdiction to:
    a. comply with the relevant laws, regulations, or measures on online safety and security; and
    b. adopt, maintain, and publish their policies and procedures on online safety and security.

3. The laws and regulations referred to in paragraph 1 of this Article shall, among others, require digital platforms to implement necessary measures to:
    a. combat the online sale of illegal content, digital products, and services;
    b. counter the online registration, sale, or dissemination of illegal content and digital products, including information and images that include hate speech, online sexual abuse, child sexual abuse material, pornographic content or material, cyberbullying, incitement to violence, and racism;
    c. publish, in a machine-readable format and an easily accessible manner, guidelines on what content is prohibited, to whom it is prohibited, how complaints are submitted or handled, as well as what and how decisions are made, in a timely, non-discriminatory and non-arbitrary manner;
    d. prohibit targeted advertising based on the use of sensitive personal data and the personal data of children;
    e. prohibit interfaces and practices aimed at misleading users; and
    f. put in place appropriate measures to ensure the highest level of privacy, safety, and security of children on their service.

4. State Parties shall harmonise their laws and regulations on online safety and security taking into account international, continental, and regional standards and practices.

5. State Parties shall ensure that laws and regulations referred to in this Article are not adopted or applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on digital trade, and do not impose restrictions on digital trade that are greater than necessary to achieve the objective.

6. This Annex shall not be applied and interpreted to restrict any legally protected speech, including works of artistic or newsworthy value, such as commentary, criticism, satire, or parody.

Article 6

Competent Authorities

1. Each State Party shall establish or designate a competent authority responsible for the enforcement of online safety and security regulations or measures set forth in this Annex.

2. State Parties shall promptly notify, through the Secretariat, the other State Parties of their competent authorities referred to in paragraph 1 of this Article.

3. The Secretariat shall make publicly available and communicate to all State Parties the names and contact details of competent authorities designated by State Parties responsible for the enforcement of online safety and security regulations in their respective jurisdictions.

4. State Parties shall ensure that their competent authorities:
    a. cooperate and collaborate with the competent authorities of other State Parties in addressing cross-border online safety and security concerns; and
    b. perform their duties in an impartial, transparent, and timely manner.

5. State Parties shall, to the extent of their capabilities, provide their competent authorities with the necessary resources, including technical, financial, and human resources to adequately ensure online safety and security.

6. State Parties shall, taking into account the principles of legitimacy, necessity, and proportionality, adopt or maintain measures as may be necessary to provide powers to competent authorities for the blocking, filtering, and removing of illegal content on specified legal grounds for the purpose of ensuring online safety and security.

7. State Parties shall adopt or maintain measures to enhance and, where necessary, establish channels of communication between their competent authorities in order to facilitate a secure and rapid exchange of information concerning all aspects of the online safety and security covered under this Annex.

Article 7

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application related to online safety and security; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new or amendments to existing laws and regulations, or any measures related to online safety and security.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

Article 8

Cooperation

1. State Parties shall cooperate with each other in accordance with the provisions of this Article and through the application of relevant international and regional instruments, arrangements agreed on the basis of unilateral or reciprocal legislation, and domestic laws, to the extent possible, for the purposes of investigations or proceedings concerning online safety and security.

2. State Parties shall cooperate to advance collaborative solutions to online safety and security in digital trade, through, among others:
    a. a multi-stakeholder approach involving governments, law enforcement authorities, relevant industry, consumers, civil society, and technical communities;
    b. exchange of information and best practices;
    c. mutual legal assistance;
    d. public awareness campaigns to promote and enhance online safety and security;
    e. joint research and development of online safety and security tools and technologies; and
    f. education, training, and capacity building for law enforcement and judicial authorities and other relevant stakeholders.

3. State Parties shall, where necessary, collaborate with relevant regional, continental, and international bodies in the implementation of this Annex.

Article 9

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex in order to facilitate its effective implementation and enforcement.

Article 10

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 11

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 12

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili,

Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON
CROSS-BORDER DATA TRANSFERS

PART I
GENERAL PROVISIONS
Article 1
Definitions

For the purpose of this Annex:

a. **"Annex"** means the Annex on Cross-Border Data Transfers to the Protocol;

b. **"Competent Authority"** means a public body, agency, regulator, or any authority designated or empowered by the domestic law of a State Party to execute and enforce data protection laws covered under this Annex;

c. **"Consent"** means any freely given, express, informed, and unequivocal indication or will of the data subject by which he or she explicitly accepts or signifies agreement to the transfer or processing of his or her personal data;

d. **"Cross-Border Data Transfers"** means the transfer of data, including personal data, by electronic means across the jurisdictions of State Parties;

e. **"Data"** means any information and data, other than personal data as defined in Article 1(q) of the Protocol, required, stored, used, processed, or collected by a person of a State Party;

f. **"Data Subject"** means any natural person that is the subject of personal data;

g. **"Digital Trade"** means digital trade as defined in Article 1(g) of the Protocol;

h. **"Interoperability"** means interoperability as defined in Article 1(f) of the Annex on Digital Identities to the Protocol;

i. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol;

j. **"Personal Data"** means personal data as defined in Article 1(q) of the Protocol;

k. **"Processing of Personal Data"** means any operation, set of operations, or activity which is performed on personal data, whether by automatic means, such as the collection, recording, organisation, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, and locking, encryption, erasure, or destruction of personal data; and

l. **"Sensitive Personal Data"** means any personal data relating to racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, financial data, data concerning health or data concerning a natural person's sex life or sexual orientation, or any other personal data that, if released, would cause harm, damage, or detriment to an individual's rights, interests, or well-being.

Article 2

Objectives

The objectives of this Annex are to:

a. give effect to Article 20(3) of the Protocol;
b. eliminate regulatory and administrative barriers to cross-border data transfers within the AfCFTA digital market;
c. facilitate cross-border data transfers while protecting personal data in order to boost digital trade, innovation, and inclusive socio-economic growth within the AfCFTA digital market;
d. establish predictable and transparent harmonised rules, and common principles, and standards for safe and secure cross-border data transfers within the AfCFTA digital market;
e. enhance the competitive capacity of enterprises of the State Parties and accelerate their beneficial integration into the global digital market; and
f. foster cooperation and collaboration among State Parties on cross-border data transfers to achieve the objectives of the AfCFTA related to the sustainable socio-economic development of African economies and societies.

Article 3

Scope of Application

1. This Annex shall apply to electronic cross-border data transfers, including personal data, provided the activity is for the conduct of digital trade by a person of a State Party.

2. This Annex shall not apply to:
   a. cross-border data transfers for purposes which fall outside the scope of digital trade as defined in Article 1(g) of the Protocol; and
   b. data or information held or processed by or on behalf of a State Party, or measures related to that data or information, including measures related to its collection, except for open government information as provided for in Article 39 of the Protocol.

PART II

PRINCIPLES AND STANDARDS FOR PERSONAL DATA PROTECTION

Article 4

Personal Data Protection Legal Frameworks

1. Pursuant to Article 21(1) of the Protocol, each State Party shall adopt or maintain a legal framework that provides for the protection of the personal data of natural persons engaged in digital trade.

2. The legal frameworks referred to in paragraph 1 of this Article shall comply with the principles and standards stipulated in Articles 5 to 14 of this Annex.

Article 5

Principles for Personal Data Protection

State Parties shall, in their legal frameworks, adopt or maintain foundational principles of personal data protection, including:

a. lawfulness, fairness, and transparency;
b. data minimisation;

c. purpose limitation;
d. storage limitation;
e. accuracy;
f. security, confidentiality, and integrity; and
g. accountability.

Article 6

Rights of Data Subjects

State Parties shall, in their legal frameworks:

a. provide for the rights of data subjects with respect to their personal data, including the right to access, rectify, erase, data portability, object to processing of personal data, and to be informed about the processing of their personal data; and
b. ensure that a person of a State Party involved in the processing of personal data provides, in a transparent and accessible manner, their policies and practices with respect to personal data, including:
    i. personal data being collected;
    ii. the purpose for which the personal data is collected;
    iii. to whom personal data might be disclosed;
    iv. retention period; and
    v. information on how to contact the persons about their practices and handling of personal data.

Article 7

Data Minimisation

State Parties shall, in their legal frameworks:

a. ensure that the collection of personal data is limited to data relevant to the purpose of collection and any such data should be obtained by lawful and fair means, and where applicable, with notice to and consent of the data subject; and
b. ensure that a person of a State Party neither collects nor retains personal data which is not necessary for the conduct of digital trade, nor combines personal data stored, or relating to the use of personal data, from different services offered by that person or from third party services, which are not necessary for the conduct of digital trade, unless the data subject has provided consent.

Article 8

Security Measures

State Parties shall, in their legal frameworks, require a person of a State Party involved in the processing of personal data to protect personal data that they hold with appropriate safeguards against risks, including, but not limited to, loss, theft or unauthorised access, destruction, use, modification, transfer or disclosure of personal data, or other forms of misuse.

Article 9

Personal Data Protection by Design and Default

State Parties shall, in their legal frameworks, require a person of a State Party involved in the processing of personal data to protect the data both at the time of the determination of the means for processing and at the time of the processing, by incorporating appropriate technical and organisational measures designed to implement the data protection principles in an

effective manner, and integrate the necessary safeguards into the processing of personal data in order to protect the rights of the data subjects.

Article 10

Remedies

State Parties shall, in their legal frameworks:

a. provide for appropriate remedies for data protection violations, including redress and establishment of a mechanism to prevent violations from continuing and other relevant remedies commensurate with the extent of actual or potential harm to data subjects resulting from such violations; and
b. require a person of a State Party to notify promptly the competent authorities referred to in Article 11 of this Annex as well as the affected data subjects in the event of a significant breach affecting the protection of personal data under its control.

Articles 11

Competent Authorities

1. Each State Party shall establish or designate a competent authority responsible for the enforcement of personal data protection laws.
2. State Parties shall notify, through the Secretariat, the other State Parties of their competent authorities referred to in paragraph 1 of this Article.
3. The Secretariat shall make publicly available and communicate to all State Parties the names and contact details of competent authorities of the State Parties designated to enforce their respective personal data protection laws.
4. State Parties shall ensure that their competent authorities:
   a. cooperate and collaborate with the competent authorities of other State Parties in addressing cross-border personal data protection violations; and
   b. perform their duties and responsibilities in an impartial, transparent, and timely manner.
5. State Parties shall, to the extent of their capabilities, provide their competent authorities with all necessary resources, including technical, financial, and human resources to adequately perform their duties and responsibilities.
6. State Parties shall adopt or maintain measures to enhance and, where necessary, establish channels of communication between their competent authorities in order to facilitate a secure and rapid exchange of information concerning all aspects of the personal data protection covered under this Annex.

Article 12

Publication of Policies and Procedures

Each State Party shall require a person of a State Party involved in the processing of personal data in its jurisdiction to adopt or maintain and publish their policies and procedures related to the protection of personal data.

Article 13

Sharing and Disclosure of Personal Data to Third Parties

1. State Parties shall, in their legal frameworks, require that a person of a State Party must not share or disclose personal data to any third party unless:

a. prior notification is given to the data subject, and consent has been given by the data subject or competent authority of the State Party; or
b. where prior notification is given to the data subject, and the disclosure is necessary to fulfil a contractual obligation of the data subject.

2. The third party to whom personal data has been shared or disclosed in accordance with paragraph 1 of this Article shall not share or disclose such personal data unless consent has been given by the data subject or competent authority of the State Party.

3. This Article does not apply in circumstances where disclosure to third parties is necessary for compliance with a legal obligation or mandated by the law, including, for the purposes of verification of identity, the prevention, detection, or investigation of cybercrimes, and the prosecution and punishment of offences.

4. For greater certainty, a third party in this Article refers to a natural or juridical person, other than the data subject, including public authority, agency, or body of a State Party, or a Third Party as defined in Article 1(u) of the Protocol.

Article 14

Access by State Parties

1. A State Party shall not require access to:
   a. personal data held by a person of another State Party as a condition for conducting digital trade in its territory; and
   b. the personal data of data subjects of other State Parties held by its natural or juridical persons conducting digital trade in the territory of those State Parties.

2. This Article does not preclude a regulatory body or judicial authority of a State Party from requiring a person of another State Party to make available personal data to the regulatory body or judicial authority for a specific investigation, inspection, enforcement action, or judicial proceeding, or when required for a legitimate and legal public interest, subject to safeguards against unauthorised disclosure of personal data under the law or practice of a State Party.

3. The safeguards and procedures outlined in Articles 4, 5, and 6 of the Annex on Criteria for Determining the Legitimate and Legal Public Interest Reasons for Disclosure for Source Code to the Protocol shall apply *mutatis mutandis* to paragraph 3 of this Article.

Article 15

Interoperability and Harmonisation

1. State Parties shall promote interoperability of their relevant legal frameworks to facilitate cross-border data transfers while protecting personal data.
2. State Parties may enter into mutually beneficial and reciprocal data sharing and data systems interoperability agreements or arrangements, that take into account principles of transparency and non-discrimination and comply with relevant data protection laws of the State Parties or the principles and standards stipulated in Articles 5 to 14 of this Annex.
3. State Parties shall harmonise their data protection laws, including administrative and procedural matters, with the principles and standards stipulated in Articles 5 to 14 of this Annex with a view to achieving a harmonised continental legal framework for data protection within the AfCFTA digital market.

PART III

FACILITATING CROSS-BORDER DATA TRANSFERS

Article 16

Principles for Cross-Border Data Transfers

1. Pursuant to Article 20(1) of the Protocol, a State Party shall not, except as otherwise provided for in this Annex, apply measures that restrict the cross-border transfer of data, including personal data between its territory and the territory of another State Party if the transfer is for the conduct of digital trade by a person of another State Party.

2. For greater certainty, the measures referred to in paragraph 1 of this Article include, but are not limited to, any prohibition, condition, restriction, or limitation, whether temporary or permanent, provided for in the laws, regulations, administrative requirements, or practices of a State Party to the transfer of data, including personal data, provided the activity is for the conduct of digital trade by a person of another State Party.

3. State Parties shall adopt or maintain reasonable and appropriate measures to ensure that cross-border data transfers, including personal data, by persons of State Parties for the conduct of digital trade are uninterrupted and secure.

4. State Parties shall refrain from restricting cross-border data transfers, including personal data, by a person of a State Party, to a State Party where a legal framework stipulated in Article 21(1) of the Protocol and principles and standards set out in Articles 5 to 14 of this Annex exist.

5. State Parties shall adopt or maintain reasonable and appropriate measures to identify and remove barriers to cross-border data transfers.

Article 17

Equivalent Level of Protection

Each State Party shall accord an equivalent level of protection to the data, including personal data, transferred by a person of another State Party as it accords to the data, including personal data, of its own persons.

Article 18

Non-Discrimination

1. A State Party shall accord no less favourable treatment to the data, including personal data, of the person of other State Parties than it accords to like data, including personal data, of its own persons.

2. A State Party shall accord no less favourable treatment to the data, including personal data, of the person of another State Party than it accords to like data, including personal data, of the persons of other State Parties or persons of Third Parties.

Article 19

Cross-Border Data Transfer Mechanisms

1. State Parties shall facilitate safe and secure cross-border data transfers by encouraging and supporting the establishment of mechanisms that take into account principles of transparency, non-discrimination, and interoperability, and comply with relevant data protection laws of the State Parties or the standards stipulated in Part II of this Annex, including, but not limited to:
    a. regional data centres and cloud systems;
    b. establishment of data centres or disaster recovery sites located in State Parties;
    c. the development of industry-specific self-regulatory data codes of conduct;
    d. principles-based certification systems for cross-border data transfers, which include allowing competent authorities to certify data protection compliance and implement a system of periodic assessment of data protection compliance of the certified persons of State Parties; and
    e. cross-border data transfer mechanisms tailored to the needs and challenges of the micro, small and medium enterprises, women, youth, indigenous peoples, rural and local communities, persons with disabilities, and other underrepresented groups.

2. State Parties shall encourage the development of mechanisms to promote compatibility between their different legal frameworks. Such mechanisms may include the recognition of regulatory outcomes, whether accorded unilaterally or by mutual arrangement or agreement.

3. State Parties shall, where necessary, collaborate with relevant stakeholders to develop frameworks or mechanisms referred to in this Article.

4. State Parties shall ensure that the mechanisms referred to in this Article facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating barriers to cross-border data transfers, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

Article 20

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application pertaining to or affecting the cross-border data transfers and protection of personal data; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new or amendments to existing laws and regulations, or any measures pertaining to or affecting the cross-border data transfers and protection of personal data.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

Article 21

Cooperation

1. State Parties shall cooperate, through, among others:
   a. sharing information pertaining to data protection including, but not limited to, research, surveys and reports;
   b. joint promotional, educational, and training programmes to raise public awareness and enhance understanding of data protection and compliance with data protection laws and regulations;
   c. undertaking consultation and capacity-building activities on data protection;
   d. mutual legal assistance; and
   e. sharing experiences on techniques in investigating cross-border violations of data protection and regulatory strategies in resolving disputes involving such violations including, among others, complaints handling and alternative dispute resolution mechanisms.

2. State Parties shall engage in dialogue with relevant stakeholders, including, but not limited to, relevant industry, consumers, academia, professional, and standard-setting bodies to obtain input on data protection and cross-border data transfers to seek cooperation in furthering the objectives of this Annex.

3. State Parties shall cooperate on facilitating cross-border data transfers and protection by creating a framework under which the competent authorities may, voluntarily, share information and request and render assistance in matters related to cross-border data transfers and protection.

4. State Parties shall periodically review and update their cross-border data transfers and data protection standards to ensure alignment with best practices and technological advancements related to the protection and transfer of data.

5. State Parties shall develop instruments that facilitate cross-border data transfers, including but not limited to guidelines, recommendations, and standards.

Article 22

Data for Development

Pursuant to Article 20(3) of the Protocol, State Parties, taking into account the importance of data for development, shall:

   a. facilitate innovative ways to promote public benefits by sharing or using data in ways that would enable the data in Africa to be harnessed to realise its socio-economic value in public sector decision-making, planning, monitoring and evaluation;
   b. support data capabilities to take advantage of data-reliant technologies and services to foster sustainable development and benefit African economies and citizens;
   c. leverage data-driven business models that can foster intra-African digital trade and data-enabled entrepreneurship;
   d. promote interoperability, data sharing, and responsiveness to data demand through the setting of open data standards in data creation, which conform to the general principles of anonymity, privacy, security, and any sector-specific data considerations, to facilitate access to non-personal data and certain categories of personal data by African researchers, innovators, and entrepreneurs;
   e. promote research, development, and innovation in various data-driven areas;
   f. support the development of regional and continental data infrastructure to host advanced data-driven technologies and the necessary enabling environment and data-sharing mechanism to facilitate data movement across the continent; and

g. establish a continental Forum for African policymakers, competent authorities, relevant industry, and other relevant stakeholders to leverage data as the engine of a digital economy and society, facilitate exchanges among State Parties, and enable knowledge sharing on data value-creation and innovation and the implications of data usage on privacy and security of persons of State Parties.

PART IV

GENERAL EXCEPTIONS

Article 23

Application

1. The general exceptions stipulated in Articles 24, 25 and 26 of this Annex shall apply to cross-border transfer of data, including personal data.

2. State Parties shall ensure that the measures adopted or maintained pursuant to Part IV of this Annex are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on cross-border digital trade, and do not impose restrictions on transfers of data greater than are necessary to achieve the public policy objectives and protect essential security interests.

Article 24

Public Policy Objectives

Pursuant to Article 20(2) of the Protocol, a State Party may adopt or maintain measures inconsistent with this Annex to achieve legitimate public policy objectives, including the protection of essential security interests, maintenance of public order and safety, and the protection of public morals and public health.

Article 25

Appropriate Personal Data Protection Legal Framework

A State Party may restrict the cross-border transfer of data, including personal data, to another State Party that does not maintain a legal framework stipulated in Article 21(1) of the Protocol and does not provide for principles and standards set out in Articles 5 to 14 of this Annex.

Article 26

Sensitive Personal Data

1. A State Party may impose restrictions on cross-border transfer of sensitive personal data.

2. A State Party shall, in circumstances where the cross-border transfer of sensitive personal data is necessary to facilitate digital trade, allow such transfers provided:
    a. the receiving State Party has equivalent or comparable level of data protection provided under the laws and regulations of the sending State Party and standards stipulated in Part II of this Annex;
    b. consent has been granted by the data subject;
    c. authorisation has been granted by the competent authority;
    d. the person transferring the sensitive personal data exercises due diligence and takes reasonable measures to ensure that the person to whom the sensitive personal data is transferred shall protect such data in accordance with the laws of

the State Party and standards stipulated in Part II of this Annex; or

e. applicable security measures and procedures are complied with.

3. State Parties shall allow the transfer of sensitive personal data where:
   a. such data is made available publicly by the data subject;
   b. the data subject has given his or her consent to transfer of his or her such data;
   c. the transfer of such data is necessary to protect the vital interests of the data subject or of any other person where the data subject is physically or legally incapable of giving his or her consent; or
   d. the transfer of such data is required for the establishment, exercise, or defence of legal claims.

4. State Parties shall ensure that security measures and procedures for cross-border transfer of sensitive personal data are reasonable, transparent, predictable, and non-discriminatory.

5. The person, whether natural or juridical, to whom the sensitive personal data has been transferred shall not transfer the data to a third party unless consent has been given by the data subject or the competent authority.

6. For greater certainty, a third party referred to in paragraph 5 of this Article includes a natural or juridical person other than the data subject, including public authority, agency, or body of a State Party or a Third Party as defined in Article 1(u) of the Protocol.

PART V FINAL PROVISIONS

Article 27

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex to facilitate its effective implementation and enforcement.

Article 28

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 29

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement.

Article 30

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON
EMERGING AND ADVANCED TECHNOLOGIES

PART I
GENERAL PROVISIONS

Article 1
Definitions

For the purpose of this Annex:

a. **"Annex"** means the Annex on Emerging and Advanced Technologies to the Protocol;

b. "**Emerging and Advanced Technologies**" means developing, new, or developed technologies, including, but not limited to, the Internet of Things, Artificial Intelligence, Machine Learning, Robotics, 5G, 3D printing, Quantum Computing, Blockchain, Virtual Reality, and other existing and future technologies relevant to digital trade; and

c. "**Person of a State Party**" means a person of a State Party as defined in Article 1(p) of the Protocol.

Article 2
Objectives

The objectives of this Annex are to:

a. give effect to Article 34(3) of the Protocol;
b. promote research and development for building capacity and digital skills relating to the development and deployment of emerging and advanced technologies in digital trade;
c. facilitate, promote, and foster the deployment and use of emerging and advanced technologies in digital trade;
d. foster cooperation and collaboration among State Parties in the development and deployment of emerging and advanced technologies in digital trade;
e. encourage the regulation of emerging and advanced technologies in a manner that does not create barriers to digital trade; and
f. establish predictable and transparent harmonised rules, and common principles and standards for the adoption and regulation of emerging and advanced technologies in digital trade.

Article 3
Scope of Application

This Annex shall apply to the emerging and advanced technologies deployed and used in digital trade by the persons of State Parties.

PART II

FACILITATING THE DEPLOYMENT AND USE OF EMERGING AND ADVANCED TECHNOLOGIES IN DIGITAL TRADE

Article 4

Deployment and Use

1. State Parties shall facilitate, promote, and foster the deployment and use of emerging and advanced technologies in digital trade by persons of State Parties, including African-owned enterprises and African digital platforms.

2. State Parties shall adopt or maintain laws and regulations that facilitate, promote, and foster the development, access, deployment, and use of emerging and advanced technologies in digital trade by persons of State Parties, including African-owned enterprises and African digital platforms.

3. A State Party shall not deny a person of another State Party from conducting digital trade in its territory solely on the basis that such person deploys or uses emerging and advanced technologies.

Article 5

Non-Discrimination

1. A State Party shall accord no less favourable treatment to emerging and advanced technologies developed in the territory of other State Parties than it accords to like emerging and advanced technologies developed in its territory.

2. A State Party shall accord no less favourable treatment to emerging and advanced technologies developed in the territory of another State Party than it accords to like emerging and advanced technologies developed in the territory of other State Parties or Third Parties.

Article 6

Intellectual Property Rights

State Parties shall protect and enforce intellectual property rights related to emerging and advanced technologies deployed and used in digital trade in accordance with Article 17 of the Protocol on Intellectual Property Rights.

Article 7

Data Protection and Privacy

The provisions of Articles 20 and 21 of the Protocol and the provisions of Articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 21 of the Annex on Cross-Border Data Transfers to the Protocol shall apply *mutatis mutandis* to this Annex.

Article 8

Cybersecurity

The provisions of Article 25 of the Protocol shall apply *mutatis mutandis* to this Annex.

Article 9

Research and Development

1. State Parties shall promote research and development in emerging and advanced technologies in digital trade through, among others:
    a. building and strengthening cooperation and collaboration between relevant stakeholders, including governments, relevant industry, consumers, and academia on research and development in emerging and advanced technologies;
    b. improving financial, technological, and human resource development capacity for research and development in emerging and advanced technologies;
    c. developing regulatory frameworks that promote research and development in emerging and advanced technologies;
    d. promoting and facilitating public and private investments in research and development with a focus on innovation and start-ups in emerging and advanced technologies; and
    e. establishing continental, regional, and national institutions for digital innovation and research and development to ensure effective deployment and use of emerging and advanced technologies in digital trade.

2. State Parties agree to adopt measures that enhance the participation of African-owned enterprises, including micro, small and medium-sized enterprises, women, youth, persons with disabilities, indigenous peoples, rural and local communities, and other underrepresented groups in research, technology, and innovation activities related to emerging and advanced technologies.

Article 10

Regulatory Sandboxes

1. State Parties shall endeavour to establish regulatory sandboxes at the national levels to facilitate the development and testing of emerging and advanced technologies under regulatory oversight.

2. State Parties shall ensure that the regulatory sandboxes:
    a. provide a controlled environment that fosters innovation and facilitates the development, testing, and validation of use cases for emerging and advanced technologies for a limited period before their deployment and use in digital trade or entry into the AfCFTA digital market; and
    b. enable the testing of emerging and advanced technologies in real-world conditions for a limited period.

3. State Parties shall, where necessary, collaborate to establish regulatory sandboxes at continental or regional levels to facilitate the development and testing of emerging and advanced technologies by persons of State Parties, including African-owned enterprises.

Article 11

Monitoring, Evaluation and Reporting Frameworks

State Parties may develop monitoring, evaluation, and reporting frameworks with appropriate indicators and tools for tracking the performance of emerging and advanced technologies deployed and used in digital trade.

PART III

TECHNICAL STANDARDS AND REGULATIONS

Article 12

Principles for Developing Technical Standards and Regulations

1. State Parties shall adopt or maintain technical standards and regulations to ensure that the emerging and advanced technologies are deployed and used in digital trade in a safe, responsible, and ethical manner.

2. State Parties shall ensure that regulations and standards referred to in this Article are not adopted or applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on digital trade, and do not impose restrictions on the deployment and use of emerging and advanced technologies greater than are necessary to achieve the objective.

3. State Parties shall:
    a. harmonise their technical standards and regulations on the deployment and use of emerging and advanced technologies in digital trade; and
    b. promote interoperability of technical standards and regulations for emerging and advanced technologies to facilitate digital trade.

4. State Parties shall endeavour, when adopting or maintaining their technical standards and regulations for emerging and advanced technologies, to consult relevant industry, technical and professional societies, standardisation bodies, and other relevant stakeholders.

5. State Parties shall, when adopting or maintaining technical standards and regulations referred to in this Article:
    a. take into consideration regional, continental, and international standards, principles, and guidelines;
    b. adopt a risk-based approach or any other relevant approach, including transparent processes for assessing, managing, and mitigating risks associated with specific emerging and advanced technologies deployed and used in digital trade;
    c. assess whether potential risks can be mitigated or addressed using existing instruments and regulatory frameworks;
    d. consider whether any new or proposed regulation is proportionate in balancing potential harms with economic and social benefits;
    e. employ risk management best practices, including considering the risk-substitution impact of a specific emerging and advanced technology against a scenario where such technology has not been deployed but baseline risks remain in place; and
    f. promote the development of voluntary standards to manage risks associated with emerging and advanced technologies in a manner that is adaptable to the demands of dynamic and evolving technologies.

6. State Parties shall regularly review and update their technical standards and regulations on the deployment and use of emerging and advanced technologies as required to keep pace with technological advancements.

PART IV

GENERAL EXCEPTIONS, TRANSPARENCY AND NOTIFICATION, AND COOPERATION

Article 13

General Exceptions

Nothing in this Annex shall be construed to prevent a State Party from adopting or maintaining measures inconsistent with provisions of this Annex to achieve a legitimate public policy objective, including to protect public safety, health and welfare, protect essential security interests, prevent deceptive and fraudulent practices, and protect the environment, provided that the measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on digital trade, and do not impose restrictions on the deployment and use of emerging and advanced technologies greater than are necessary to achieve the objective.

Article 14

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application affecting the deployment and use of emerging and advanced technologies in digital trade; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new laws and regulations, amendments to existing laws and regulations, or any measures pertaining to or affecting the deployment and use of emerging and advanced technologies in digital trade.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

Article 15

Cooperation

1. State Parties shall cooperate through the exchange of information, knowledge and expertise, research and development, training activities, peer learning, technical assistance, public-private sector collaboration, capacity building, and sharing experiences and best practices relating to the adoption and regulation of emerging and advanced technologies in digital trade.

2. State Parties shall, where necessary, collaborate with relevant regional, continental, and international bodies in the development, promotion, facilitation, deployment, and use of emerging and advanced technologies in digital trade, and the implementation of this Annex.

PART V

FINAL PROVISIONS

Article 16

Regulations and Guidelines

State Parties may develop regulations and guidelines on any of the aspects of this Annex in order to facilitate its effective implementation and enforcement.

Article 17

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 18

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 19

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON DIGITAL IDENTITIES

PART I

GENERAL PROVISIONS

Article 1

Definitions

For the purpose of this Annex:

a. **"AfCFTA Digital Identity"** means a digital identity established pursuant to Article 13 of this Annex.
b. **"Annex"** means the Annex on Digital Identities to the Protocol;
c. **"Authentication"** means the process or act of verifying the digital identity of a natural or juridical person;
d. **"Conformity Assessment Procedure"** means any procedure used, directly or indirectly, to determine that relevant requirements in technical regulations or standards are fulfilled;
e. **"Digital Identity"** means digital identity as defined in Article 1(e) of the Protocol;
f. **"Interoperability"** means the ability of different systems, regulations, networks, databases, devices, or applications to communicate, execute programmes, or transfer data;
g. **"Personal Data"** means personal data as defined in Article 1(q) of the Protocol;
h. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol;
i. **"Standard"** means a document approved by a recognised body that provides, for common and repeated use, rules, guidelines, or characteristics for products or related processes and production methods, with which compliance is not mandatory; and
j. **"Technical Regulation"** means a document which lays down product characteristics or their related processes and production methods, including the applicable administrative provisions, with which compliance is mandatory.

Article 2
Objectives

The objectives of this Annex are to:

a. give effect to Article 14(2) of the Protocol;
b. support cross-border interoperability, mutual recognition, and authentication of digital identities among State Parties;
c. facilitate ease of doing business, including the movement of natural and juridical persons within the AfCFTA;
d. promote digital, financial, and broader socio-economic inclusion; and
e. enhance trust and security in digital trade under the AfCFTA.

Article 3

Scope of Application

This Annex shall apply to the digital identity systems adopted or maintained by State Parties in accordance with Article 14(1) of the Protocol.

PART II

OBLIGATIONS OF STATE PARTIES

Article 4

Digital Identity Systems

1. Pursuant to Article 14(1) of the Protocol, State Parties shall adopt or maintain digital identity systems for both natural and juridical persons in accordance with their laws and regulations.

2. State Parties shall ensure that the digital identity systems referred to in paragraph 1 of this Article include enrollment, issuance, and management of digital identity credentials.

3. State Parties shall adopt or maintain digital identity systems with robust features and authentication factors which may include, but are not limited to, biometrics, signatures, physical form factors, pincodes, digital formats, online portals, unique identification numbers, images, and multi-factor authentications such as One-Time Passwords, taking into account relevant regional, continental, and international standards.

Article 5

Authentication

State Parties shall provide mechanisms to validate and authenticate digital identities which may include:

a. web-based authentication;
b. application programming interface-based authentication;
c. multi-factor authentication;
d. certificate-based authentication; or
e. any other recognised validation and authentication mechanisms.

Article 6

Notification of Digital Identity Systems and Issuing Authorities

1. Each State Party shall promptly, through the Secretariat, notify other State Parties of their digital identity systems and relevant authorities responsible for issuing the digital identities

for natural and juridical persons in its jurisdiction.

2. The Secretariat shall establish and maintain a database of the digital identity systems of State Parties and their respective issuing authorities.

3. Where any State Party or State Parties have a concern with respect to the digital identity system notified or implemented by another State Party, the concerned State Party or State Parties may request, through the Secretariat, the necessary information or consultations with the other State Party. The relevant provisions of Article 40 of the Protocol shall apply in the implementation of this paragraph.

4. A State Party shall promptly, through the Secretariat, notify other State Parties of any breach of, or threat to security, loss of integrity, or unavailability of its digital identity system, or the likelihood thereof, having, or which may have, significant impact on its digital identity systems. Such State Party shall promptly take appropriate measures to mitigate such breach, threat, loss, or likelihood thereof.

Article 7

Non-Discrimination

1. A State Party shall accord no less favourable treatment to the digital identities of other State Parties than it accords to its own like digital identities.

2. A State Party shall accord no less favourable treatment to the digital identities of other State Parties than it accords to like digital identities of other State Parties or Third Parties.

Article 8

Comparable and Equivalent Level of Protection

1. Each State Party shall accord a comparable level of protection to the digital identities issued by other State Parties as it accords to its own digital identities.

2. State Parties shall provide protection to the digital identities of persons engaged in digital trade that is equivalent to that provided for other forms of identities issued under its laws or regulations.

Article 9

Data Protection and Privacy

The provisions of Articles 20, 21, and 25 of the Protocol and the provisions of Articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 21 of the Annex on Cross-Border Data Transfers to the Protocol shall apply *mutatis mutandis* to this Annex.

PART III

TECHNICAL REGULATIONS AND STANDARDS

Article 10

Principles for Developing Technical Regulations, Standards, and Conformity Assessment Procedures

1. State Parties shall ensure that technical regulations, standards, and conformity assessment procedures pertaining to digital identities are not developed, adopted, or applied in a manner which would constitute a means of arbitrary or unjustifiable

discrimination, or a disguised restriction on digital trade, and do not impose restrictions on the use of digital identities greater than are necessary to achieve the objective.

2. State Parties shall, when adopting technical regulations, standards, and conformity assessment procedures pertaining to digital identities, take into consideration relevant regional, continental, and international standards, principles, and guidelines.

3. State Parties shall harmonise their technical regulations, standards, and conformity assessment procedures pertaining to digital identities to facilitate digital trade.

4. State Parties shall promote interoperability of technical regulations, standards, and conformity assessment procedures pertaining to digital identities to facilitate digital trade.

5. State Parties shall endeavour, when adopting or maintaining technical regulations, standards, and conformity assessment procedures pertaining to digital identities, to solicit and consider input from relevant industry, relevant technical and professional societies, standardisation bodies, and other relevant stakeholders.

6. State Parties shall regularly review and update their technical regulations, standards, and conformity assessment procedures pertaining to digital identities as required to keep pace with technological advancements.

Article 11

Mutual Recognition

1. State Parties shall recognise the legal validity of digital identities issued by the relevant authorities of other State Parties.

2. State Parties shall adopt certification mechanisms and disciplines for the mutual recognition of digital identities, provided that the following conditions are met:
    a. the digital identity system is notified pursuant to Article 6 of this Annex;
    b. the digital identity system must be interoperable with the systems of other State Parties in accordance with the principles outlined in Article 12 of this Annex; and
    c. the level of assurance associated with the digital identity must be appropriate for the intended use case. State Parties may agree on a common framework for assurance levels, or they may recognise each other's national frameworks, provided they offer equivalent levels of assurance.

3. State Parties may conduct joint assessments of each other’s digital identity systems to verify compliance with the conditions for mutual recognition.

4. State Parties shall, as appropriate, establish a trusted list of recognised digital identity systems that meet the conditions for mutual recognition established in this Article.

5. A State Party may refuse to recognise a digital identity issued by another State Party if there is evidence that the conditions for mutual recognition are not met, provided the refusing State Party provides a clear explanation and justification for such a decision.

Article 12

Interoperability

State Parties shall promote interoperability in technologies and applications for digital identities by adopting principles or common technical specifications including, but not limited to, open

standards, digitally-signed logs, time-stamps, secure audit trails, secure communications, data sovereignty, privacy-by-design, or any other relevant key features.

Article 13

AfCFTA Digital Identity

1. State Parties shall establish an AfCFTA Digital Identity to facilitate the movement of natural and juridical persons doing business under the AfCFTA, taking into account the features stipulated in Article 4 of this Annex.

2. The AfCFTA Digital Identity referred to in paragraph 1 of this Article shall be accepted by State Parties voluntarily and shall be issued by the African institution(s) designated by the participating State Parties. Such institution(s) shall, in developing the AfCFTA Digital Identity, comply with the applicable laws and regulations, data privacy and security requirements, and provisions relating to the development of technical regulations, standards, and conformity assessment procedures set forth in this Annex and other relevant provisions of the Protocol.

3. The African institution(s) responsible for issuing the AfCFTA Digital Identity, as well as the regulations and procedures for the administration and operation of the AfCFTA Digital Identity shall be determined by the Council of Ministers.

Article 14

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application affecting or pertaining to digital identities; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new laws and regulations, amendments to existing laws and regulations, or any measures pertaining to or affecting or pertaining to digital identities.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

Article 15

Cooperation

1. State Parties shall cooperate through:
    a. the exchange of information, knowledge and expertise, research and development, training activities, peer learning, and sharing experiences and best practices relating to digital identity policies and regulations, technical assistance, technical implementation, and security standards;
    b. joint promotional, education, and training programmes to raise public awareness and enhance understanding of digital identity and compliance with data protection laws and regulations; and
    c. creating a framework under which their respective competent authorities may voluntarily share information and request and render assistance in matters related to cross-border use of digital identities.

2. State Parties shall engage in a dialogue with relevant stakeholders, including, but not

limited to, the relevant industry, consumers, academia, and professional, and standard-setting bodies on matters pertaining to digital identities.

3. State Parties shall, where necessary, collaborate with relevant regional, continental, and international bodies in the development of digital identities and the implementation of this Annex.

PART IV

FINAL PROVISIONS

Article 16

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex to facilitate its effective implementation and enforcement.

Article 17

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 18

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 19

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON

CROSS-BORDER DIGITAL PAYMENTS

PART I

GENERAL PROVISIONS

Article 1

Definitions

For the purpose of this Annex:

a. **"African Local Currency"** means a form of money issued by the central bank or monetary authority under the laws and regulations of a State Party as a medium of exchange within the territory of that State Party;
b. **"Annex"** means the Annex on Cross-Border Digital Payments to the Protocol;
c. **"Digital Currency"** means a currency in a digital form, including, but not limited to, cryptocurrency based on distributed ledger technology, central bank digital currency, digital fiat currency, and any variants, including stablecoins;
d. **"Digital Payment"** means digital payment as defined in Article 1(f) of the Protocol;
e. **"Financial Technology"** means as defined in Article 1(b) of the Annex on Financial Technology of the Protocol;
f. **"Person of a State Party"** means person of a State Party as defined in Article 1(p) of the Protocol.

Article 2
Objectives

The objectives of this Annex are to:

a. give effect to Article 15(3) of the Protocol;
b. promote the development of affordable, real-time, safe, secure, inclusive, responsible, and universally accessible cross-border digital payments and settlement systems to boost intra-African trade;
c. establish predictable and transparent harmonised rules, and common principles and standards for cross-border digital payments and settlement systems within the AfCFTA;
d. promote interoperability between the different digital payment and settlement systems of the State Parties;
e. promote the use of African local currencies in cross-border digital payment and settlement systems within the AfCFTA; and
f. facilitate the attainment of the objective of the Treaty Establishing the African Economic Community to establish the African Monetary Union, African Central Bank, and single African currency.

Article 3

Scope of Application

1. This Annex shall apply to cross-border digital payments, whether wholesale or retail, by a person of a State Party where payment instruments and channels include, but are not limited to, credit transfers, electronic funds transfers, mobile money, mobile applications, quick-response codes, digital wallets, and credit, debit, and prepaid cards, supported by payment and settlement systems recognised or adopted by State Parties at the continental, regional, and national levels.

2. This Annex shall apply to digital payment systems recognised and operated in accordance with the laws and regulations of the State Parties.

3. This Annex shall not apply to:

   a. domestic digital payments or transactions that are initiated and terminated within a State Party even if the payment transactions are facilitated by an international counterparty;
   b. payments made exclusively in cash; and
   c. payments made in paper-based cheques, paper-based vouchers, paper-based traveller's cheques, and paper-based postal money orders.

4. This Annex shall not derogate from or modify the rights and obligations of the State Parties under the Protocol on Trade in Services. For greater certainty, in the event of any conflict or inconsistency between this Annex and the Protocol on Trade in Services, the provisions of the Protocol on Trade in Services shall prevail to the extent of the conflict or inconsistency.

PART II

PROMOTION OF DIGITAL PAYMENTS

Article 4

Enabling Regulatory Framework

1. Each State Party shall adopt or maintain a legal and regulatory framework for digital

payments that shall, among others, not arbitrarily or unjustifiably discriminate between financial institutions and other payment service providers, including financial technologies and mobile network operators in relation to access to services and infrastructure as well as any decision making necessary for the operation of digital payment systems.

2. State Parties shall, in their legal and regulatory framework referred to in paragraph 1 of this Article, endeavour to allow digital payment service providers, including financial technology enterprises, retailers, and mobile network operators to issue digital payment instruments and channels and provide digital payment services directly and independently without the requirement to partner with a financial institution.

Article 5

Competition and Innovation

1. State Parties shall facilitate innovation and competition in digital payments by enabling the introduction of new financial and digital payment products and services, by adopting regulatory and technological sandboxes.

2. State Parties shall develop regulations that promote competition and innovation in the digital payment industry.

3. State Parties shall promote the adoption and use of emerging and advanced technologies as well as payment methods and platforms such as mobile money, e-money, central bank digital currencies, application programming interfaces, and regulatory and supervisory technologies to promote inclusive, efficient, effective, safe, and sustainable digital payments, subject to the Annex on Emerging and Advanced Technologies and the Annex on Financial Technology to the Protocol and in collaboration with relevant industry, central banks, and standard-setting bodies.

4. State Parties shall accelerate the adoption and use of digital payments through, among others:
    a. facilitating the provision of fast, low-cost, innovative digital payment products and services, such as instant payments, e-money, and mobile money;
    b. enabling digital payments for retail payments in an offline mode; and
    c. promoting digital payments literacy and awareness among African micro, small and medium-sized enterprises, women, youth, indigenous persons, rural and local communities, and persons with disabilities, and other underrepresented groups.

Article 6

Digital Currencies

1. State Parties shall, in accordance with their national laws and regulations, adopt or maintain digital currencies as a medium of exchange in their jurisdictions to, among others, facilitate cross-border digital payments for intra-African trade.

2. State Parties that have adopted or maintained digital currencies as a medium of exchange pursuant to paragraph 1 of this Article, may enter into agreements or arrangements on digital currencies to facilitate cross-border digital payments for intra-African trade.

Article 7

African Local Currencies

1. State Parties shall promote the use of African local currencies in the operationalisation of cross-border digital payment and settlement systems to boost intra-African trade.

2. State Parties shall cooperate to promote the convertibility of African local currencies to enhance intra-African trade and lower transaction costs of cross-border digital payments.

3. State Parties may enter into agreements or arrangements on a single currency or freely convertible currencies for digital payments, provided the freely convertible currency is an African local currency or any African currency introduced by such agreements or arrangements.

4. State Parties that are party to agreements or arrangements referred to in paragraph 3 of this Article shall:
    a. afford adequate opportunity for other interested State Parties to negotiate accession to such agreements or arrangements; and
    b. promptly inform, through the Secretariat, other State Parties of the opening of negotiations on such agreements or arrangements, to provide adequate opportunity to any other State Party or State Parties to indicate their interest in participating in the negotiations before they enter a substantive phase.

PART III

FACILITATION OF CROSS-BORDER DIGITAL PAYMENTS

Article 8

Non-Discrimination

1. A State Party shall accord no less favourable treatment to a digital payment and settlement system or payment instrument of another State Party than it accords to a like digital payment and settlement system or payment instrument of its own.

2. A State Party shall accord no less favourable treatment to a digital payment and settlement system or payment instrument of another State Party than it accords to like digital payment and settlement systems or payment instrument of the other State Parties or Third Parties.

3. Notwithstanding paragraphs 1 and 2 of this Article, two or more State Parties may maintain or enter into preferential agreements or arrangements to facilitate cross-border digital payments in accordance with the objectives of this Annex.

4. State Parties that are party to preferential agreements or arrangements referred to in paragraph 3 of this Article shall afford adequate opportunity for other interested State Parties to negotiate the preferences granted therein on a reciprocal basis.

Article 9

Interoperability

State Parties shall promote cross-border interoperability between existing and new digital payment and settlement systems, use cases, instruments, and channels to enhance the use and adoption of digital payments through, among others:

    a. adopting international messaging standards for electronic data exchange between financial institutions and digital payment service providers;
    b. facilitating the use of open application programming interfaces and platforms, through the development of open banking and open finance guidelines;
    c. eliminating regulatory and technical barriers to the interoperability of digital payment and settlement systems; and

d. collaborating with digital payment service providers, regulators, payment aggregators, and relevant industry associations on common standards and technical solutions.

Article 10

Mutual Recognition

1. A State Party shall recognise the payment instruments or digital payment and settlement systems recognised and operated in another State Party.

2. The recognition referred to in paragraph 1 of this Article shall be achieved, in accordance with national laws and regulations, through harmonisation or based on an agreement or arrangement between the State Parties concerned or may be accorded unilaterally.

3. Where a State Party accords recognition unilaterally, it shall afford the opportunity for any other State Party to demonstrate that their digital payment and payment systems should be recognised.

4. Where recognition is based upon an agreement or arrangement, other interested State Parties shall be afforded adequate opportunity to negotiate their accession to such agreement or arrangement.

5. A State Party shall not accord recognition of payment instruments or digital payment and settlement systems in a manner which would constitute a means of arbitrary or unjustifiable discrimination between State Parties or a disguised restriction on digital payments.

Article 11

Authentication

State Parties shall adopt or maintain measures that allow for the authentication of cross-border digital payments by including the use of, among others, certificate-based authentication, token-based authentication, biometric authentication, electronic know-your-customers, multi-factor authentication, digital identities, face recognition, or electronic signatures.

Article 12

Cross-Border Digital Payments and Transfers

1. A State Party shall not apply restrictions on cross-border digital payments and transfers that are necessary to conduct digital trade by a person of a State Party.
2. Notwithstanding paragraph 1 of this Article, a State Party may adopt or maintain restrictions on cross-border digital payments and transfers relating to the conduct of digital trade by a person of a State Party:
    a. in the event or threat of serious balance-of-payments deficits or external financial difficulties;
    b. in the event of money laundering and financing of terrorism and proliferation; or
    c. in exceptional circumstances where movements of capital cause or threaten to cause serious economic or financial difficulties in the State Party concerned.

3. The restrictions referred to in paragraph 2 of this Article shall:
    a. not discriminate between State Parties digital payments or financial institutions;
    b. be consistent with applicable international standards;
    c. avoid unnecessary damage to the legitimate commercial interests of the persons of a State Party and other State Parties;

d. not exceed those necessary to deal with the circumstances described in paragraph 2 of this Article; and
e. be temporary and phased out progressively upon improvement of the situation specified in paragraph 2 of this Article.

4. The State Party, adopting or maintaining restrictions referred to in this Article or any changes thereof, shall promptly notify, through the Secretariat, other State Parties.

5. This Article shall be without prejudice to Articles 13 and 14 of the Protocol on Trade in Services and Articles 22 and 23 of the Protocol on Investment.

Article 13

Fees and Charges

1. State Parties shall adopt or maintain laws and regulations that require digital payment service providers to publish or make publicly available their respective fees or charges levied, directly or indirectly, on digital payments in order to promote transparency and predictability in fees and charges on cross-border digital payments.

2. State Parties shall cooperate to lower the transaction costs including fees or charges levied, directly or indirectly, on cross-border digital payments, and ensure that such fees are proportional to the service rendered.

3. State Parties shall cooperate to reduce the regulatory compliance costs, including, but not limited to licensing fees, technology and infrastructure processing costs, fraud detection system requirements, legal, audit, and reporting costs, and penalties and fines.

Article 14

Digital Payment Infrastructure

1. State Parties shall cooperate to facilitate the integration of existing and future digital payment infrastructures to facilitate cross-border digital payments by:
   a. adopting relevant digital payments and settlement systems interoperability standards or guidelines adopted at the international, continental, and regional levels;
   b. encouraging their central banks to facilitate the interoperability of national, regional, and continental digital payment and settlement systems that handle both Real-Time Retail Payments (RTRPs) and Real-Time Gross Settlement (RTGS); and

   c. encouraging the Regional Economic Communities (RECs) and regional trading arrangements to promote the interoperability of RTGS to establish a continental integrated and interoperable digital payment and settlement system.

2. State Parties shall, where necessary, collaborate with all stakeholders, including Regional Economic Communities (RECs), central banks, payment service providers, regulators, and standard-setting bodies to develop digital payment infrastructures.

Article 15

Transparency and Notification

1. Each State Party shall promptly:
   a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application affecting or pertaining to digital payments; and

   b. notify, through the Secretariat, the other State Parties of the introduction of any new or amendments to existing laws and regulations, or any measures pertaining to or affecting digital payments.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

PART IV

SAFE AND SECURE CROSS-BORDER DIGITAL PAYMENTS

Article 16

Cybersecurity

1. Pursuant to Article 25 of the Protocol, State Parties shall adopt or maintain measures to combat cybercrime and cyberthreats in digital payments taking into account relevant international best practices and standards.

2. State Parties shall adopt laws and regulations that impose obligations on digital payment service providers to ensure early detection and response to, and protect against, among others, cybercrime and cyberthreats.

Article 17

Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation

1. Each State Party shall adopt or maintain laws and regulations to combat money laundering and financing of terrorism and proliferation in digital payments taking into account relevant international best practices and standards.

2. State Parties shall adopt or maintain laws and regulations that impose obligations on digital payment service providers to combat money laundering and financing of terrorism and proliferation in digital payments.

Article 18

Transfer and Protection of Personal Data

1. Pursuant to Article 20 of the Protocol, State Parties shall allow cross-border transfer of data, including personal data necessary to facilitate digital payments with appropriate regulatory oversight.

2. Notwithstanding paragraph 1 of this Article, State Parties may restrict the transfer of data, including personal data by electronic means, to protect personal data, privacy, and the confidentiality of individual records and accounts, including in accordance with its laws and regulations. However, such restrictions shall not be used as a means of avoiding the commitments or obligations of State Parties under this Annex or the Protocol.

3. The provisions of Articles 20 and 21 of the Protocol and the provisions of Articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 21 of the Annex on Cross-Border Data Transfers to the Protocol shall apply *mutatis mutandis* to this Annex.

Article 19

Deceptive and Fraudulent Practices

1. Each State Party shall adopt or maintain laws and regulations to prevent deceptive and fraudulent practices or to deal with the effects of a default on digital payments taking into account relevant international best practices and standards.

2. State Parties shall:

a. adopt or maintain laws and regulations that impose obligations on digital payment service providers to protect against deceptive and fraudulent practices in digital payments.

b. facilitate the adoption and use of emerging and advanced technologies to prevent deceptive and fraudulent practices in digital payments, subject to the Annex on Emerging and Advanced Technologies to the Protocol.

Article 20

Consumer Protection

State Parties shall:

a. ensure that consumers engaged in digital trade have easy access to clear, comprehensive, and readily available information on fees and charges, exchange rates, and dispute resolution mechanisms for cross-border digital payments;
b. establish effective mechanisms for resolving disputes arising from cross-border digital payments;
c. cooperate to address consumer complaints or concerns related to cross-border digital payments.

Article 21

Responding to Emergencies in Cross-Border Digital Payments

1. State Parties shall:
   a. establish or designate national or sectoral emergency response teams to administer the provisions covered in Articles 16, 17, 19, and 20 of this Annex; and
   b. through their national emergency response teams, cooperate and collaborate to address incidents covered in Articles 16, 17, 19, and 20 of this Annex.

2. State Parties may mandate the national or sectoral emergency response teams to establish a registry or database in their respective jurisdictions for the collection, collation, and analysis of incidents covered in Articles 16, 17, 19, and 20 of this Annex.

Article 22

Cooperation

1. State Parties shall:
   a. cooperate through the exchange of information, knowledge and expertise, research and development, training activities, peer learning, technical assistance, public-private sector collaboration, capacity building, and sharing experiences and best practices relating to cross-border digital payments;

   b. where necessary, collaborate with relevant regional, continental, and international bodies in the implementation of this Annex.

2. State Parties may establish a continental Forum of central banks, policymakers, financial technology enterprises, continental and regional payment and settlement systems, mobile financial service providers, banks, and other relevant stakeholders to foster cooperation and collaboration on cross-border digital payment and settlement systems.

3. State Parties shall cooperate closely with each other, consistent with their respective national legal and administrative systems, to combat or prevent matters covered in Articles 16, 17, and 19 of this Annex, through, among others:
   b. exchange of information and best practices;

c. mutual legal assistance;
d. public awareness campaigns; and
e. training and capacity building for law enforcement and judicial authorities and other relevant stakeholders.

Article 23

Harmonisation of Safety and Security Regulations

1. State Parties shall harmonise their laws and regulations or measures referred to in Articles 16, 17, 18, and 19 of this Annex.
2. States Parties shall ensure that :
    a. their digital payment service providers comply at all times with the applicable relevant laws and regulations or measures referred to in Articles 16, 17, 18, and 19 of this Annex; and
    b. laws and regulations or measures referred to in Articles 16, 17, 18, and 19 of this Annex are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between financial institutions, digital payments or State Parties, or a disguised restriction to cross-border digital payments or digital trade.

PART V

FINAL PROVISIONS

Article 24

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex in order to facilitate its effective implementation and enforcement.

Article 25

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 26

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 27

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.

ANNEX ON

FINANCIAL TECHNOLOGY

PART I

GENERAL PROVISIONS

Article 1

Definitions

For the purpose of this Annex:

a. **"Annex"** means the Annex on Financial Technology to the Protocol;
b. **"Financial Technology"** means technologies that transform the provision of financial services, spurring the development of new business models, applications, processes, and products. For greater certainty, these include, but are not limited to:
    i. start-ups and scaled-up enterprises specialised in technology-enabled financial innovation;
    ii. incumbent financial institutions using and transitioning to platform models; and
    iii. technology enterprises offering aggregation services to digital financial service providers.
c. **"Person of a State Party"** means a person of a State Party as defined in Article 1(p) of the Protocol.

Article 2

Objectives

1. The objectives of this Annex are to:
    a. give effect to Article 35(2) of the Protocol;
    b. leverage financial technology to promote cross-border digital payments and boost intra-African trade;
    c. encourage cooperation among State Parties in promoting responsible innovation and regulation of financial technology;
    d. promote collaboration between State Parties, financial technology enterprises, and industry bodies, consistent with the respective laws and regulations of the State Parties; and
    e. establish predictable and transparent harmonised rules, and common principles and standards, to facilitate the seamless operation of financial technology enterprises in Africa.

Article 3

Scope of Application

1. This Annex shall apply to financial technology deployed and used in digital trade by persons of State Parties.

2. This Annex shall not derogate from or modify the rights and obligations of the State Parties under the Protocol on Trade in Services. For greater certainty, in the event of any conflict or inconsistency between this Annex and the Protocol on Trade in Services, the provisions of the Protocol on Trade in Services shall prevail to the extent of the conflict or inconsistency.

PART II

REGULATIONS AND STANDARDS

Article 4

Non-Discrimination

1. A State Party shall accord no less favourable treatment to financial technology licensed or registered in other State Parties than it accords to like financial technology in its territory.

2. A State Party shall accord no less favourable treatment to financial technology licensed or registered in another State Party than it accords to like financial technology licensed or registered in other State Parties or Third Parties.

Article 5

Registration and Licensing

1. State Parties shall register and license financial technology enterprises to provide or facilitate financial products and services in accordance with their national laws and regulations to facilitate intra-African trade.

2. State Parties shall adopt or maintain legal and regulatory frameworks that allow financial technology enterprises to provide financial products and services.

3. State Parties may, in their legal and regulatory frameworks, allow financial technology enterprises to provide financial products and services directly and independently without the requirement to partner with a financial institution.

4. State Parties shall, subject to their laws and regulations, promote license passporting of financial technology enterprises to provide digital payments or financial services across multiple State Parties.

5. State Parties shall harmonise their laws and regulations pertaining to the registration and licensing of financial technology enterprises.

Article 6

Interoperability

State Parties shall promote cross-border interoperability between financial technology, financial institutions, and other digital payment service providers to facilitate digital payment services through, among others:

a. adopting relevant regional, continental, and international standards;
b. facilitating access to and use of open application programming interfaces and platforms;
c. eliminating unnecessary regulatory and technical barriers to the interoperability of digital payments; and
d. collaborating with digital payment providers, payment aggregators, regulators, and industry associations on common standards and technical solutions.

Article 7

Open Finance

State Parties shall, as appropriate, adopt or maintain laws and regulations for open finance that:

a. allow for secure and efficient financial services data exchange between financial institutions and authorised financial technology enterprises through application programming interfaces; and

b. enable financial technology enterprises to develop innovative financial products and services that leverage customer-consented data, and that promote the achievement of potential benefits, such as increased competition and enhanced value for customers.

Article 8

Regulatory Sandboxes

1. State Parties shall endeavour to establish regulatory sandboxes at the national level to facilitate the development and testing of financial technology innovations under regulatory oversight, while protecting consumers, managing risk, and preserving financial system stability.

2. State Parties shall ensure that the regulatory sandboxes:
    a. provide a controlled environment that fosters innovation and facilitates the development, testing, and validation of use cases of financial technology for a limited time before their deployment and use in digital trade or entry into the AfCFTA digital market; and
    b. enable, where appropriate, the testing of financial technologies in real-world conditions for a limited period, subject to compliance with consumer protection, financial stability, data protection, and cybersecurity laws and regulations.

3. State Parties shall endeavour to establish regulatory sandboxes at continental or regional levels to facilitate the development and testing of financial technology by persons of State Parties including African-owned enterprises.

4. The regulatory sandboxes referred to in this Article shall focus on financial technology innovations in areas including, but not limited to, digital payments, blockchain technology, and regulatory technology.

Article 9

Competition and Innovation

State Parties shall promote competition and innovation in financial technology through:

a. adopting policies and laws that encourage responsible innovation and fair competition between financial technology enterprises, and between financial technology enterprises and financial institutions;
b. adopting relevant regional, continental, and international standards for financial technology, ensuring a harmonised regulatory environment that supports innovation while protecting consumer interests and financial stability;
c. promoting research and development in financial technology;
d. encouraging their financial technology enterprises to use facilities and assistance, where available, in other State Parties' territories to explore new business opportunities;
e. fostering collaboration, dialogue, partnership, and technology transfer among their financial technology enterprises;

f. adopting measures to facilitate the entry, scalability, and sustainability of financial technologies, including, but not limited to, cross-border incubation programmes, funding opportunities, and regulatory guidance;
g. establishing innovation facilities, including but not limited to, innovation hubs that promote collaboration and knowledge sharing between financial technology enterprises, relevant industry, academia, and regulators; and
h. promoting financial technology literacy and awareness among African micro, small and medium-sized enterprises, women, youth, indigenous persons, rural and local communities, and persons with disabilities and other underrepresented groups in order to increase adoption and use of financial technology.

Article 10

Transparency and Notification

1. Each State Party shall promptly:
    a. publish or make publicly available, including through electronic means, its laws, regulations, policies, procedures, and administrative rulings of general application affecting financial technology; and
    b. notify, through the Secretariat, the other State Parties of the introduction of any new laws and regulations, amendments to existing laws and regulations, or any measures pertaining to or affecting financial technology.

2. Nothing in this Article shall be construed to require any State Party to disclose or allow access to confidential information and data, the disclosure of which would impede law enforcement or prejudice legitimate commercial and strategic interests of particular enterprises or institutions, whether public or private, or would otherwise be contrary to its public or essential security interests.

PART III

SAFETY AND SECURITY

Article 11

Cybersecurity

1. Pursuant to Article 25 of the Protocol, State Parties shall adopt or maintain measures to combat cybercrime and cyberthreats in financial technology, taking into account relevant regional and international best practices and standards.

2. State Parties shall adopt laws and regulations that impose obligations on financial technology enterprises to ensure early detection and response to and protect against cybercrime and cyberthreats.

Article 12

Anti-Money Laundering and Financing of Terrorism and Proliferation

1. Each State Party shall adopt or maintain laws and regulations to combat money laundering and financing of terrorism and proliferation in financial technology taking into account relevant international best practices and standards.

2. State Parties shall adopt or maintain laws and regulations that impose obligations on financial technology enterprises to combat money laundering and financing of terrorism and proliferation in financial technology.

Article 13

Transfer and Protection of Personal Data

1. State Parties shall adopt laws and regulations that impose obligations on financial technology enterprises to protect personal data.

2. State Parties shall not adopt or maintain measures that prevent transfers of data, including personal data by electronic means, necessary for providing or facilitating digital financial services by a person of a State Party.

3. State Parties shall, in adopting or maintaining measures referred to in paragraph 2 of this Article, enable secure cross-border transfer of data for all financial technology enterprises with appropriate regulatory oversight. The provisions of Articles 20 and 21 of the Protocol and the provisions of Articles 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 21 of the Annex on Cross-Border Data Transfers to the Protocol shall apply *mutatis mutandis* to this Annex.

4. Notwithstanding paragraph 2 of this Article, State Parties may restrict the transfer of data, including personal data, by electronic means to protect personal data, personal privacy, and the confidentiality of individual records and accounts, including in accordance with its laws and regulations. However, such restrictions shall not be used as a means of avoiding a State Parties' commitments or obligations under this Annex.

Article 14

Deceptive and Fraudulent Practices

1. Each State Party shall adopt or maintain laws and regulations to prevent deceptive and fraudulent practices or to deal with the effects of a default on financial technology, taking into account relevant international best practices and standards.

2. State Parties shall adopt or maintain laws and regulations that impose obligations on financial technology enterprises to protect against deceptive and fraudulent practices.

Article 15

Consumer Protection

State Parties shall:

a. adopt or maintain laws and regulations on financial technology for the protection of consumers;
b. adopt or maintain laws and regulations that impose obligations on financial technology enterprises to protect consumers; and
c. cooperate to address and provide redress for consumer complaints or concerns on financial technology.

Article 16

Responding to Emergencies in Financial Technology

The provisions of Article 21 of the Annex on Cross-Border Digital Payments to the Protocol shall apply *mutatis mutandis* to Articles 11, 12, 14, and 15 of this Annex.

Article 17

Harmonisation of Safety and Security Regulations

The provisions of Article 23 of the Annex on Cross-Border Digital Payments to the Protocol shall apply *mutatis mutandis* to Articles 11, 12, 14, and 15 of this Annex.

Article 18
Cooperation

1. State Parties shall cooperate through the exchange of information, knowledge and expertise, research and development, training activities, peer learning, technical assistance, public-private sector collaboration, capacity building, and sharing experiences and best practices relating to financial technology.

2. State Parties may collaborate in the creation of regional or continental certification bodies on the use of financial technologies.

3. State Parties shall, where necessary, collaborate with relevant regional, continental, and international bodies in the implementation of this Annex.

4. State Parties shall cooperate closely with each other, consistent with their respective national legal and administrative systems, to combat and prevent matters covered in Articles 11, 12, and 14 of this Annex, through, among others:

    a. exchange of information and best practices;
    b. mutual legal assistance;
    c. public awareness campaigns; and
    d. training and capacity building for law enforcement and judicial authorities and other relevant stakeholders.

PART IV

FINAL PROVISIONS

Article 19

Regulations and Guidelines

State Parties may develop continental regulations or guidelines on any of the aspects of this Annex to facilitate its effective implementation and enforcement.

Article 20

Dispute Settlement

Any dispute between the State Parties arising out of or relating to the interpretation or application of any provision of this Annex shall be settled in accordance with the Protocol on Rules and Procedures on the Settlement of Disputes.

Article 21

Review and Amendment

This Annex shall be subject to review and amendment in accordance with Articles 28 and 29 of the AfCFTA Agreement, respectively.

Article 22

Authentic Texts

This Annex is drawn up in six (6) original texts in the Arabic, English, French, Kiswahili, Portuguese, and Spanish languages, all of which are equally authentic.