SEPTEMBER 11, 2025

CODESA SAFEGUARDS, COMPLIANCE AND LEGAL INTERFACES

GSIA'S PLATFORM FOR PUBLIC/PRIVATE PARTNERSHIPS

CREATED BY
EUSL AB
Care to Change the World

CODESA Safeguards, Compliance, and Legal Interfaces

Environmental and Social Safeguards Framework (ESSF)

Purpose: To establish a coherent system for identifying, assessing, and managing environmental, social, and governance (ESG) risks associated with CODESA-financed programs, particularly digital and infrastructure initiatives, in alignment with regional and international standards.

Chapter 1 – Screening and Categorization

1.1 Risk Classification

All CODESA-financed activities shall undergo ESG screening to determine their risk category: **High, Substantial, Moderate, or Low**, consistent with AfDB ISS and World Bank ESF taxonomy.

1.2 Proportionality Principle

The scope and depth of safeguards instruments shall be proportionate to the risk classification. High-risk projects require full Environmental and Social Impact Assessment (ESIA), while low-risk projects may require only basic screening and mitigation measures.

1.3 Documentation

Screening results and risk classifications shall be documented in the allocation file and disclosed publicly in accordance with the Open Contracting Data Standard (OCDS).

Chapter 2 – Impact Assessment and Management Plans

2.1 Required Instruments

Depending on the risk category, the following instruments may be required:

- **ESIA** – Environmental and Social Impact Assessment
- **ESMP** – Environmental and Social Management Plan
- **SEP** – Stakeholder Engagement Plan
- **LMP** – Labour Management Procedures
- **RAP** – Resettlement Action Plan (where applicable)

2.2 Climate and Digital Risk Screening

All projects shall undergo climate-risk screening and, for digital initiatives, cybersecurity and data-protection risk assessments aligned with NIST CSF 2.0 and ISO/IEC 27001:2022.

2.3 Approval and Disclosure

Safeguards instruments must be cleared by the CODESA Safeguards Unit prior to procurement and disclosed in machine-readable formats.

Chapter 3 – Stakeholder Engagement and Grievance Redress

3.1 Engagement Principles

Stakeholder engagement shall be inclusive, gender-sensitive, and continuous throughout the project lifecycle.

3.2 Grievance Redress Mechanism (GRM)

Each project shall establish a GRM accessible to all stakeholders, with clear timelines for acknowledgment and resolution.

3.3 SEA/SH Protocols

Allegations of Sexual Exploitation and Abuse/Sexual Harassment (SEA/SH) shall be handled through survivor-centered protocols, with mandatory reporting within 48 hours to the Safeguards Unit and competent authorities.

Chapter 4 – Monitoring and Disclosure

4.1 Monitoring

The Secretariat shall maintain a consolidated safeguards risk register and track compliance through periodic audits and site visits.

4.2 Disclosure

All safeguards instruments, risk classifications, and monitoring reports shall be published on the CODESA website in OCDS-compliant formats.

4.3 Independent Verification

High-risk projects shall undergo third-party verification of safeguards compliance, with findings disclosed in the Annual Results Report.

References

- AfDB Integrated Safeguards System (ISS)
- World Bank Environmental and Social Framework (ESF)
- Open Contracting Data Standard (OCDS)
- NIST Cybersecurity Framework 2.0
- ISO/IEC 27001:2022

Data Protection, Cybersecurity, and Digital Sovereignty Policy

Purpose: To safeguard personal data, digital systems, and networks across COMESA Member States, ensuring compliance with regional digital strategies, e-commerce aspirations, and international best practices.

Chapter 1 – Data Protection Principles and Roles

1.1 Core Principles

(a) **Lawfulness and Fairness** – All personal data shall be processed lawfully, fairly, and transparently;
(b) **Purpose Limitation** – Data shall be collected for specified, explicit, and legitimate purposes;
(c) **Data Minimization** – Only data necessary for the stated purpose shall be processed;
(d) **Accuracy and Integrity** – Data shall be accurate and kept up to date;
(e) **Storage Limitation** – Data shall not be retained longer than necessary;
(f) **Accountability** – CODESA and implementing entities shall demonstrate compliance with these principles.

1.2 Roles and Responsibilities

(a) Each implementing entity shall designate a **Data Protection Officer (DPO)**;
(b) The CODESA Secretariat shall maintain a central compliance registry and provide oversight;
(c) Data subjects shall have enforceable rights, including access, rectification, and erasure.

Chapter 2 – Cybersecurity Controls and Incident Response

2.1 Security Baseline

(a) All systems shall implement controls aligned with the NIST Cybersecurity Framework 2.0 and maintain an ISO/IEC 27001:2022 roadmap;

(b) Multi-factor authentication, encryption, and network segmentation shall be mandatory for critical systems.

2.2 Incident Response

(a) All entities shall maintain an incident response plan, including detection, containment, eradication, and recovery procedures;

(b) Serious incidents (including data breaches) shall be reported to the CODESA Cybersecurity Unit and relevant authorities within 48 hours;

(c) Coordination with national Computer Emergency Response Teams (CERTs) is mandatory.

Chapter 3 – Cross-Border Data Flows and Localization

3.1 Data Transfer Rules

(a) Cross-border transfers of personal data shall be permitted only where adequate protection measures are in place, consistent with the **AU Malabo Convention** and COMESA digital trade protocols;
(b) Transfers to jurisdictions lacking adequate safeguards shall require contractual clauses or binding corporate rules approved by CODESA.

3.2 Data Localization

(a) Critical government and financial data shall be hosted within COMESA Member States unless otherwise authorized by the Donor Committee;

(b) Cloud service providers shall comply with sovereignty and security requirements set by CODESA.

Chapter 4 – Audits and Breach Notification

4.1 Security Audits

(a) Periodic cybersecurity audits shall be conducted by independent auditors, with findings reported to the CODESA Audit & Risk Subcommittee;

(b) Vulnerability assessments and penetration tests shall be performed at least annually.

4.2 Breach Notification

(a) Data breaches involving personal data or critical systems shall be notified to:

- The CODESA Secretariat within **48 hours**;
- Affected data subjects without undue delay;
- Relevant national regulators and donors as required by law or financing agreements. (b) Notifications shall include the nature of the breach, affected data, mitigation measures, and remedial actions.

References

- AU Malabo Convention on Cybersecurity and Personal Data Protection
- NIST Cybersecurity Framework 2.0

- ISO/IEC 27001:2022
- COMESA Digital Strategy (reference page)

Legal Operations Manual and Standard Form Contracts

Purpose: To provide a unified legal framework and standardized templates for agreements executed under CODESA, ensuring consistency, enforceability, and compliance with COMESA Treaty provisions, donor requirements, and international best practices.

Chapter 1 – Contract Typologies

1.1 Grant Agreements
Used for financial support provided to implementing partners without expectation of repayment, subject to fiduciary and safeguards obligations.

1.2 Service Contracts
For consultancy and technical services, including advisory, capacity building, and IT development.

1.3 Goods and Works Contracts
For procurement of equipment, infrastructure works, and related services under CODESA-financed projects.

1.4 Framework Agreements
For recurring procurement needs, enabling efficiency and economies of scale.

1.5 Non-Disclosure Agreements (NDAs)
To protect confidential information exchanged during negotiations or project implementation.

1.6 Intellectual Property (IP) Licenses
For software, digital platforms, and proprietary technologies deployed under CODESA programs.

Chapter 2 – Mandatory Clauses

All standard contracts shall include the following clauses:
(a) **Intellectual Property Rights (IPR)** – Allocation of ownership and licensing terms for deliverables;
(b) **Data Protection and Confidentiality** – Compliance with the Data Protection, Cybersecurity, and Digital Sovereignty Policy;
(c) **Liability and Indemnity** – Allocation of risk and remedies for breach;
(d) **Force Majeure** – Definition of events beyond control and associated relief measures;
(e) **Termination** – Grounds for termination, including breach, insolvency, and force majeure;
(f) **Anti-Corruption and AML Compliance** – Prohibition of prohibited practices and sanctions for violations.

Chapter 3 – Governing Law and Venue

(a) All contracts shall specify **COMESA law** as the governing law, supplemented by general principles of international commercial law where applicable;
(b) Venue for dispute resolution shall be Lusaka, Zambia, unless otherwise agreed in writing.

Chapter 4 – Arbitration and Mediation Options

(a) Disputes arising under contracts shall be resolved through a tiered mechanism:

- **Negotiation → Mediation under UNCITRAL Mediation Rules → Arbitration under UNCITRAL Arbitration Rules (2013)** or **ICC Rules**, as specified in the contract;
(b) Arbitration awards shall be enforceable under the New York Convention (1958);

(c) For contracts involving COMESA Member States, reference may be made to the COMESA Court of Justice for matters within its jurisdiction.

References

- UNCITRAL Arbitration Rules (2013)
- UNCITRAL Mediation Rules (2021)
- New York Convention (1958)

Dispute Resolution Protocol

Purpose: To establish a coherent, tiered mechanism for resolving disputes arising under CODESA's governance framework, financing agreements, and contracts, ensuring consistency with the COMESA Treaty and international arbitration standards.

Chapter 1 – Internal Escalation

1.1 Notification and Good Faith Negotiation

Any dispute (hereinafter "Dispute") shall first be notified in writing to the CODESA Secretariat and escalated to the Executive Director for good-faith negotiations.

1.2 Governing Board Review

If unresolved within thirty (30) days, the matter shall be referred to the CODESA Governing Board for determination. The Board shall convene within fifteen (15) days of referral and issue a written decision within thirty (30) days thereafter.

Chapter 2 – Mediation/Conciliation

2.1 Mediation Framework

If internal escalation fails, the Parties shall submit the Dispute to mediation under the **UNCITRAL Mediation Rules (2021)**, administered by a mediator jointly appointed by the Parties or, failing agreement, by an appointing authority acceptable to both.

2.2 Timelines and Confidentiality

Mediation shall commence within thirty (30) days of the request and conclude within forty-five (45) days unless extended by mutual agreement. Mediation communications shall remain confidential.

Chapter 3 – Arbitration (UNCITRAL/ICC)

3.1 Scope

Any Dispute concerning financing obligations, fiduciary covenants, or contractual rights not resolved by mediation shall be finally settled by arbitration under:

(a) **UNCITRAL Arbitration Rules (2013)**, or

(b) **ICC Arbitration Rules**, if expressly agreed in the relevant contract.

3.2 Seat and Language

The seat of arbitration shall be **Lusaka, Zambia**, unless otherwise agreed. The language of arbitration shall be English.

3.3 Tribunal and Enforcement

The tribunal shall comprise three arbitrators unless the Parties agree to a sole arbitrator. Awards shall be final and binding and enforceable under the New York Convention (1958).

Chapter 4 – Referral to National Courts or COMESA Mechanisms

4.1 COMESA Court of Justice

Disputes involving interpretation of the COMESA Treaty or obligations of Member States may be referred to the COMESA Court of Justice in accordance with its Statute.

4.2 National Courts

Operational disputes not subject to arbitration may be referred to competent national courts, provided such referral does not conflict with the COMESA legal order or donor covenants.

References

- UNCITRAL Mediation Rules (2021)
- UNCITRAL Arbitration Rules (2013)
- New York Convention (1958)