



INTIC

Instituto Nacional de Tecnologias de Informação e Comunicação

ICT Regulatory Authority

Fostering the AI Economy: Legal Frameworks for Data, Innovation and Digital Infrastructure

Data • Innovation • Digital Infrastructure



Prof. Dr. Eng. Lourino Alberto Chemane

Chairman of the Board of Directors of INTIC, IP

Maputo, 09 September 2026





- I.** Introduction
- II.** Legal and Regulatory Framework
- III.** Digital Infrastructure for the AI Economy
- IV.** Innovation and the AI Economy
- V.** Building Trust through Cybersecurity
- VI.** From Frameworks to Economic Value
- VII.** Conclusion



To present how **data, infrastructure, innovation and trust** drive Mozambique's AI economy.

I. Introduction



The AI Economy requires more than AI.

AI does not develop only through algorithms. It requires a comprehensive legal, institutional, technological and economic ecosystem.

The AI Economy =



Mozambique is progressively building the foundations for an **AI-ready ecosystem** through a sequential and integrated approach:



A trusted and inclusive AI economy for a more prosperous Mozambique.

II. Legal and Regulatory Framework



Mozambique's Evolving ICT Legal and Regulatory Framework



Electronic Transactions Law (ETL) – Law No. 3/17 of 9 January

The Law establishes the principles, general rules and legal framework for electronic transactions in general, electronic commerce and electronic government in particular, with the aim of ensuring protection in the use of Information and Communication Technologies.



Decree No. 67/2017, of 1 December

Approves the Electronic Government Interoperability Framework.



Resolution No. 45/2019, of 20 June

Ratifies the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).



Resolution No. 51/2017, of 21 June

Approves the Policy for the Information Society.



Resolution No. 59/2019, of 16 October

Approves the Strategic Plan for the Information Society.



Decree No. 82/2020, of 10 September

Approves the Regulation on the Use of the .mz Domain.



Resolution No. 69/2021, of 31 December

Approves the National Cybersecurity Policy and its Implementation Strategy.



Decree No. 42/2024, of 18 June

Approves the Regulation of the National Scientific Repository of Mozambique.



Decree No. 59/2023, of 27 October

Approves the Regulation on the Registration and Licensing of Providers of Electronic Services Intermediaries and Digital Platform Operators.



Resolution No. 39/2024, of 23 July

National Science, Technology and Innovation Policy and Strategy.



Cybercrime Law – Law No. 14/2026, of 1 July

Establishes the legal framework for cybercrime, investigation and the collection of evidence in electronic form.



Cybersecurity Law – Law No. 13/2026, of 1 July

Establishes the legal framework for cybersecurity and the protection of information systems and critical infrastructures.



Proposed Personal Data Protection Law

Proposal for a Personal Data Protection Law — approved by the Executive and awaiting approval by the Assembly of the Republic. Establishes the legal framework for the protection of personal data.



Data Centre Regulation – Decree No. 71/2025, of 31 December

Establishes the legal framework applicable to the creation, operation and management of data centres, defining technical, security, energy-efficiency and service-continuity requirements.



Cloud Computing Regulation – Decree No. 72/2025, of 31 December

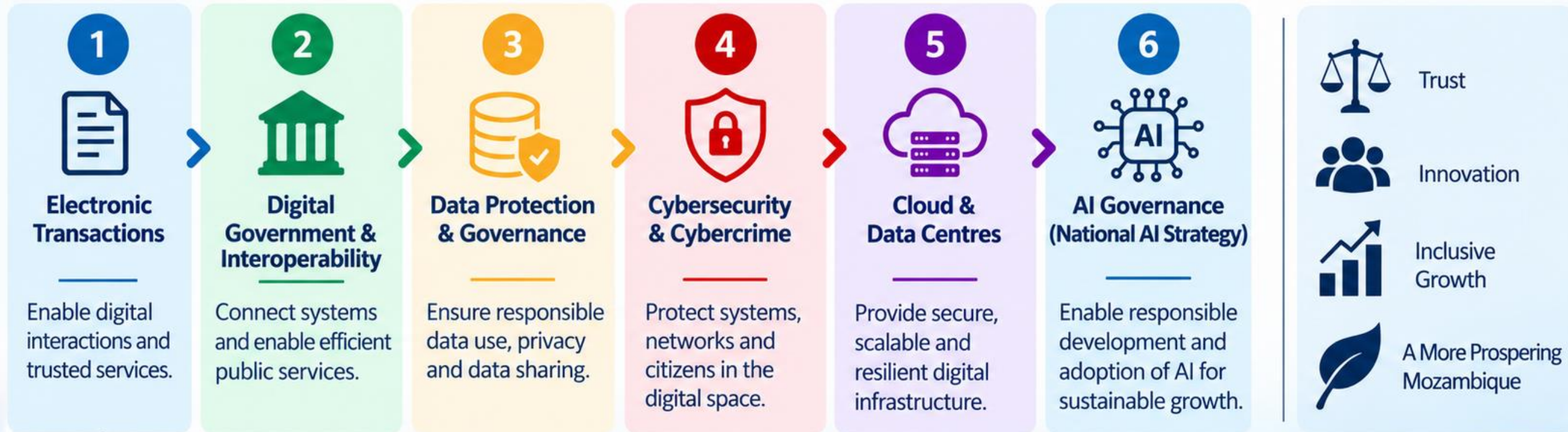
Establishes the legal framework applicable to the provision of cloud computing services, including requirements for security, privacy, data localisation, interoperability and service continuity.



II. Legal and Regulatory Framework

From ICT Laws and Regulations to AI-Ready Regulation

A progressive and integrated approach to build a trusted and enabling environment for the AI economy.



Mozambique is progressively building the foundations of an AI-ready regulatory environment.

II. Legal and Regulatory Framework



Guiding, Legal and Regulatory Instruments

Approved, **under Review**, **under Development** and **Planned**.

INTIC, IP
National Institute of Information
and Communication Technologies



- ❖ Personal Data Protection Law; and
- ❖ Regulation on Access and Use of the Centralized Government E-mail System.



- ❖ **Regulation of the Electronic Government Interoperability Framework.**



- ❖ **National Data Governance Policy and corresponding Strategy** – African Union Commission, European Union, GIZ and UNECA;
- ❖ **National Digital Transformation Strategy** – Project “Establishing the foundations for a Digital Mozambique”, a joint initiative of the International Telecommunication Union (ITU) and the European Union Delegation in Mozambique;
- ❖ **Digital Government Strategy** – World Bank, EDGE Project;
- ❖ **National Artificial Intelligence Strategy** – UNESCO;
- ❖ **National Cybersecurity Strategy (2026–2030)** – Finland;
- ❖ **Development Standards for Information Systems for Public Administration** – World Bank, EDGE Project; and
- ❖ **E-commerce Regulation** – VODACOM Mozambique.



- ❖ **Online Copyright Law;**
- ❖ **Artificial Intelligence Law;**
- ❖ **Open Data Regulation; and**
- ❖ **Digital Identity Regulation.**



II. Legal and Regulatory Framework

Data Governance as a Foundation of the AI Economy



The National Data Governance Policy and Strategy adopts principles aligned with the strategic frameworks of the African Union (AU) and SADC, ensuring coherence with regional priorities in data governance.



II. Legal and Regulatory Framework

Data Protection, Privacy and Trust

DATA PROTECTION PROCESSING AGENTS – ART. 38SS



Data Controller

A natural or legal person under public or private law that determines how the data is handled.

- Personal data
- Sensitive data
- Anonymized data



Data Processor

Makes decisions related to the processing of personal data on behalf of the data controller throughout the life cycle of the data and to achieve the purposes and the processing means.



Data Operator

Carries out the processing of personal data on behalf of the data controller but does not have the power to make decisions.



Data Protection Officer (DPO)

Acts as the communication channel between the controller, the data subjects and the Data Protection Authority (DPA). The DPO is appointed by the controller and processor and must not have decision-making power.



Data Processing

Any operation performed on personal data. Examples: collection, production, classification, use, access, reproduction, transmission, distribution, control, storage, deletion, evaluation, modification.



Legal Basis

Any processing of personal data must be based on a legal basis.



Data Protection Authority

It is the public administration body that supervises compliance with the law.

It has powers to issue guidelines and minimum technical standards to ensure the applicable data security and privacy.

Compliance and Good Practices



Any entity that processes personal data must comply with data security requirements throughout the data processing lifecycle.



Processing agents must adopt appropriate technical and administrative security measures.



Measures must be observed from the product design stage.



Infringements are subject to applicable sanctions by the DPA.

III. Digital Infrastructure for the AI Economy



Digital Infrastructure as an Enabler of AI



Connectivity

Reliable, secure and affordable connectivity to enable access, inclusion and AI-driven services.



Cloud and Data Centres

Modern and resilient cloud infrastructure and data centres to store, process and manage growing volumes of data.



Computing Capacity

High-performance computing infrastructure, including GPUs and cloud resources, to support AI development and deployment.



Storage

Scalable, secure and cost-effective storage solutions for data, models and applications.



Digital Platforms

Interoperable digital platforms and services to enable innovation, collaboration and delivery of AI solutions.

No AI economy is possible without adequate digital infrastructure.



III. Digital Infrastructure for the AI Economy

Data Centers: Building National Computing Capacity

Decree No. 71/2025, of 31 December

1

OBJECTIVE AND SCOPE

WHAT DOES IT REGULATE?



- Legal regime applicable to data center operators.
- Covers registration, licensing and operation.
- Applies to operators and data centers that develop activities within the national territory.

2

REGULATORY MODEL

HOW IS IT IMPLEMENTED?



Regulatory Authority: registers data center operators and centers.



Procedures, obligations and notifications: carried out through the New Technologies Operator Portal.



Registration of operators: public and free on the Portal.



Foreign operators: must appoint a legal representative established in Mozambique.

3

CATEGORIES OF DATA CENTERS

CLASSIFICATION BASED ON RESILIENCE AND REDUNDANCY

ADVANCED

Multiple independent circuits and redundant systems; supports operations without impact from failures.

STANDARD

Redundant components and multiple circuits; allows operation with limited impact on the environment.

LIMITED

Redundancy of main components, a single circuit; maintenance may cause service interruption.

BASIC

No redundancy of components/circuits; susceptible to interruptions due to failure or maintenance.

4

LICENSING AND INSTALLATION

MAIN REQUIREMENTS



Exploration/management: only for licensed operators.



Installation and operation: depends on a data center operating license.



Construction: comply with the Urban Land Regulation and the EIA, where applicable.



Location: consider natural risks, distance from roads/industries and fiber optic connections.



Continuous maintenance of air conditioning and refrigeration.

5

REGULATION STRUCTURE

MAIN COMPONENTS



General provisions



Rights and obligations of operators



Essential services and classified information



Procedures and fees



Supervision and sanctions



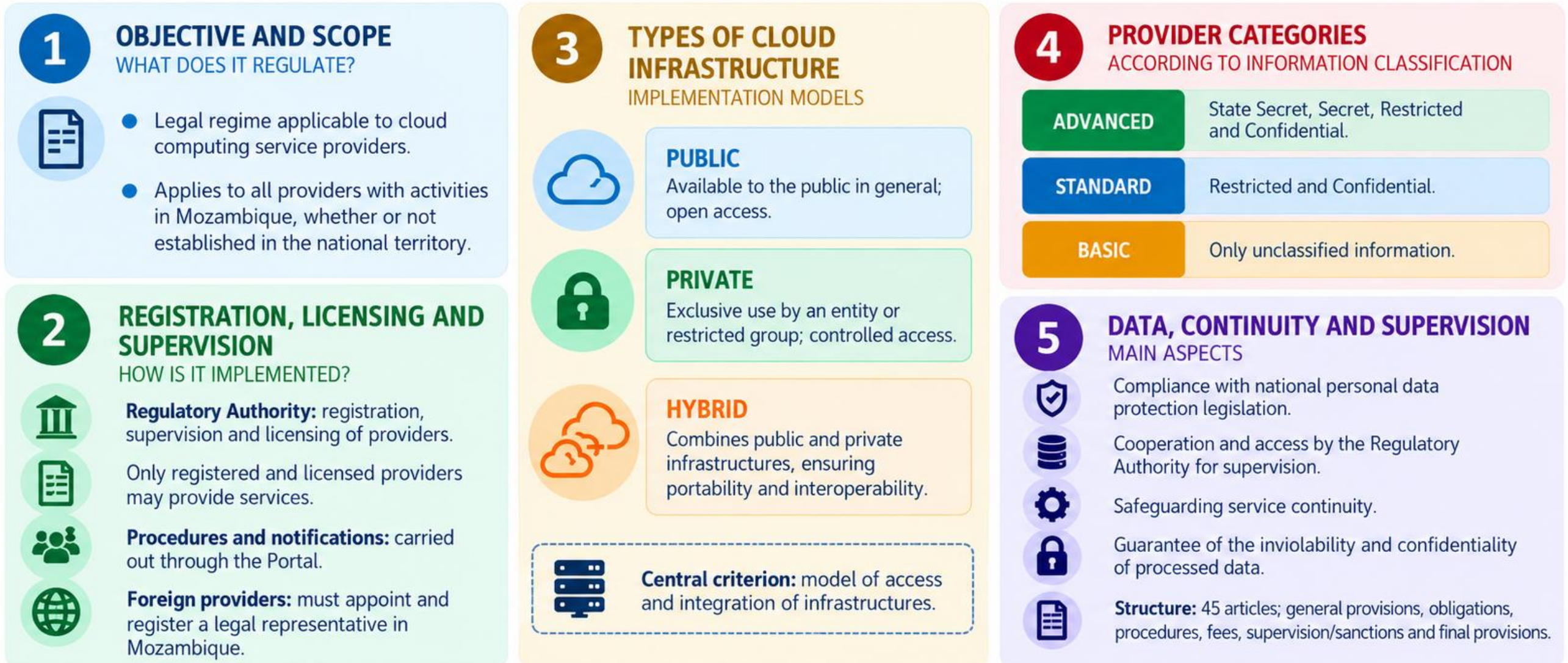
Final and transitional provisions



III. Digital Infrastructure for the AI Economy

Cloud Computing: Enabling Scalable AI

Decree No. 72/2025, of 31 December

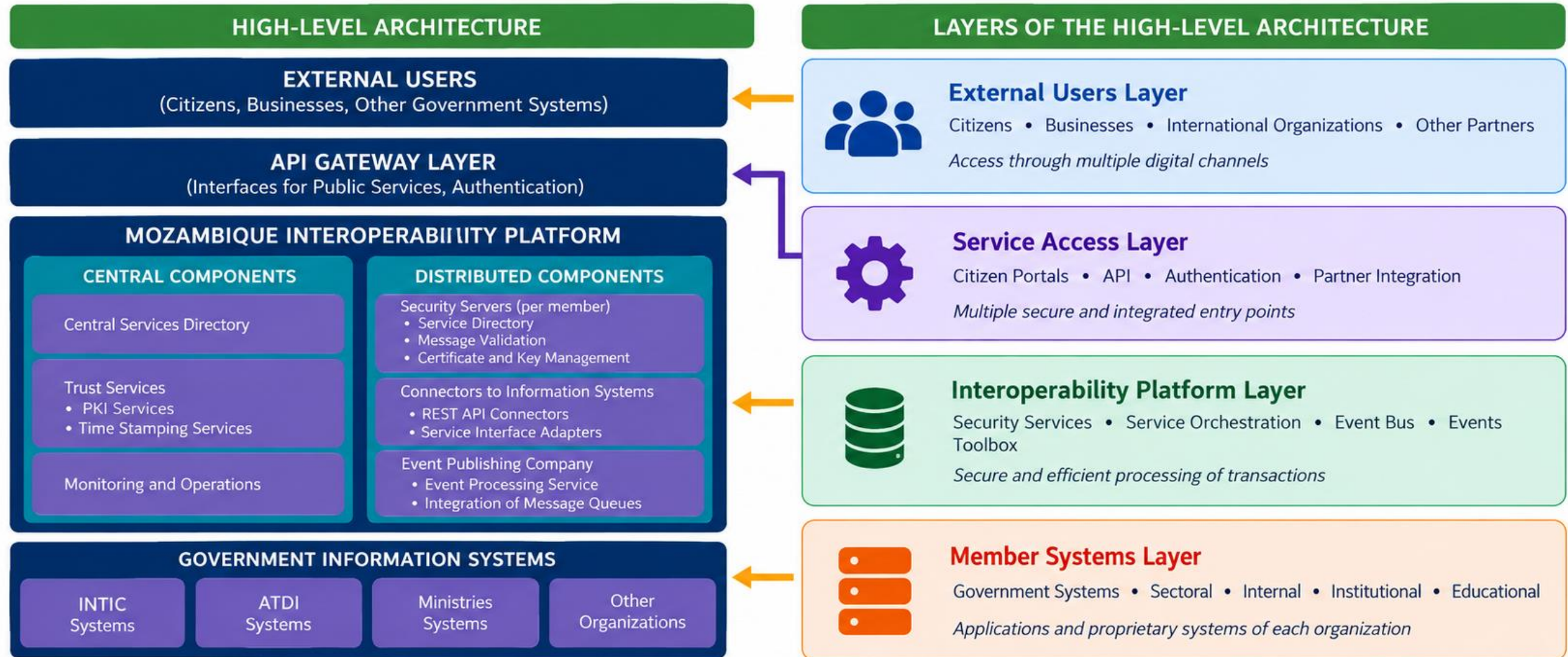




III. Digital Infrastructure for the AI Economy

Interoperability: Connecting the Digital State

Proposed Architecture





III. Digital Infrastructure for the AI Economy

Cybersecurity and Digital Resilience

Critical Infrastructure and Essential Services — Law No. 13/2026 — Cybersecurity and Law No. 14/2026 — Cybercrimes



LAW NO. 13/2026 — CYBERSECURITY

Art. 3.º

Defines critical infrastructures, sets out the scope of the essential services covered and establishes the general principles for ensuring their cybersecurity and resilience, as well as the supervision regime.

Arts. 16.º–17.º

Establishes obligations for operators of critical infrastructures and essential services, including minimum cybersecurity requirements and incident reporting.

ANNEX II — LIST OF ESSENTIAL SERVICES

No.	SECTOR	SUBSECTORS / COVERED ENTITIES
1	 Energy	Electricity; petroleum & gas.
2	 Water	Water supply/distribution; wastewater collection and treatment; water retention systems.
3	 Transport	Airport, land and maritime transport operators; railway and traffic control systems; passenger transport.
4	 Finance	Banks; insurance; securities.
5	 Financial market infrastructure	Clearinghouses.
6	 Health	Health service and care provision facilities; health system providers; medical device manufacturers.
7	 Telecommunications infrastructure	Telecommunications operators.
8	 Internet infrastructure	Domain name registries; IXPs; DNS providers; IP registry.



LAW NO. 14/2026 — CYBERCRIMES

Establishes enhanced criminal protection for critical infrastructures and essential services, criminalizing conduct that compromises them.

Art. 11.º

Corporate network intrusion with compromise of critical infrastructures and essential services

Criminalizes invasion of corporate networks or information systems of public or private entities when such action results in compromising critical infrastructures and essential services.



Art. 12.º

Attacks intended to affect critical infrastructures

Criminalizes, among other conduct, attacks intended to destroy, alter, damage, deteriorate, alter or disable critical infrastructures, or systems or information essential for the operation of such services.



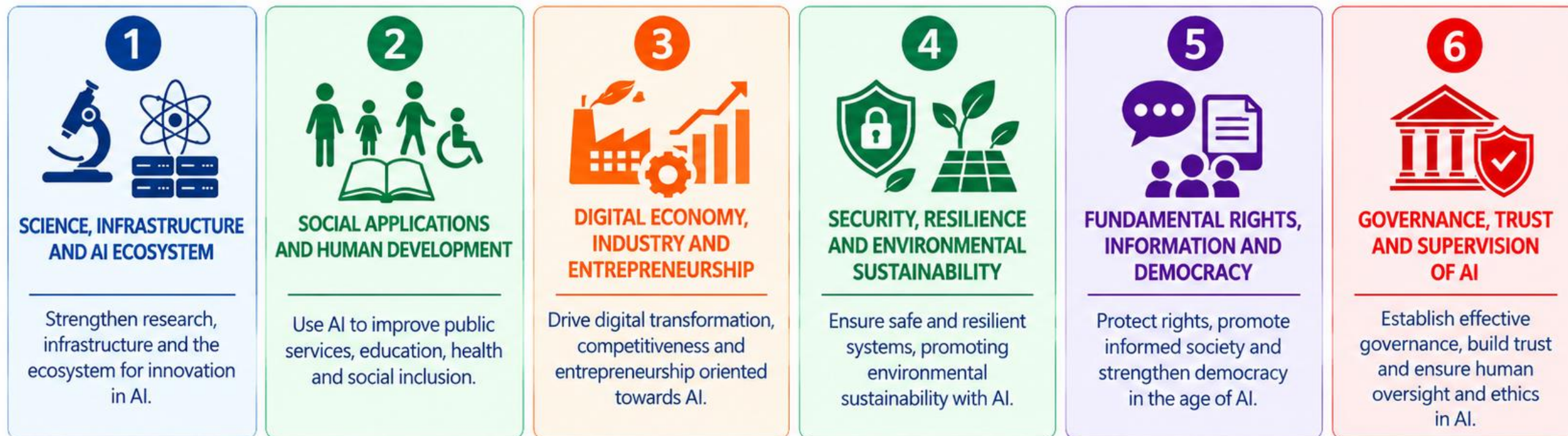
Thus, Law No. 14/2026 ensures total criminal protection for critical infrastructures and essential services defined in Annex II, as referred to in Law No. 13/2026.

IV. Innovation and the AI Economy



Six Strategic Pillars of the National AI Strategy

PILLARS OF THE NATIONAL ARTIFICIAL INTELLIGENCE STRATEGY



ETHICS • INCLUSION • SECURITY • SOVEREIGNTY • INNOVATION • COLLABORATION • SOCIAL IMPACT

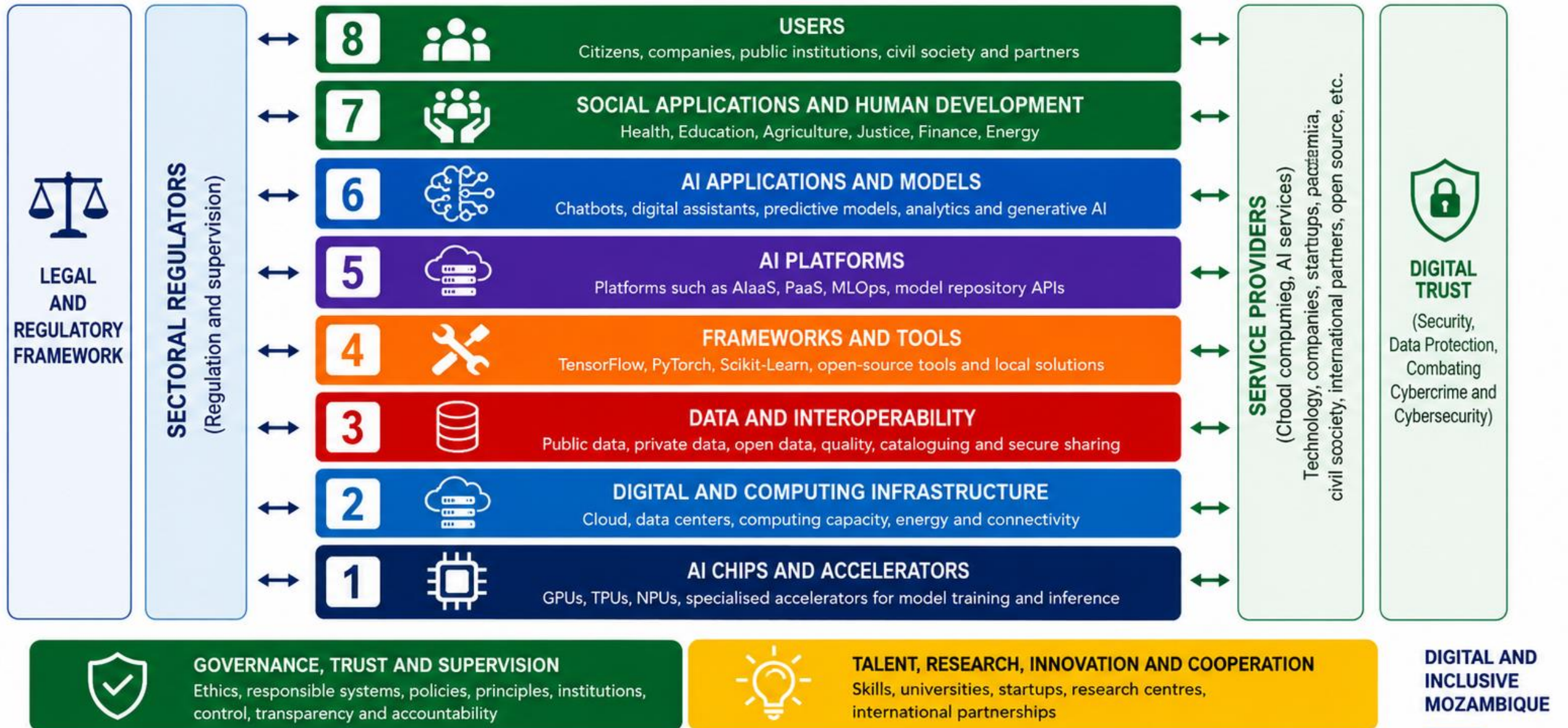
A DIGITAL AND INCLUSIVE MOZAMBIQUE

The Proposal for the National Artificial Intelligence Strategy (ENIA) presents these six pillars and places data, computing, **health**, security, rights and governance within an integrated architecture.



IV. Innovation and the AI Economy

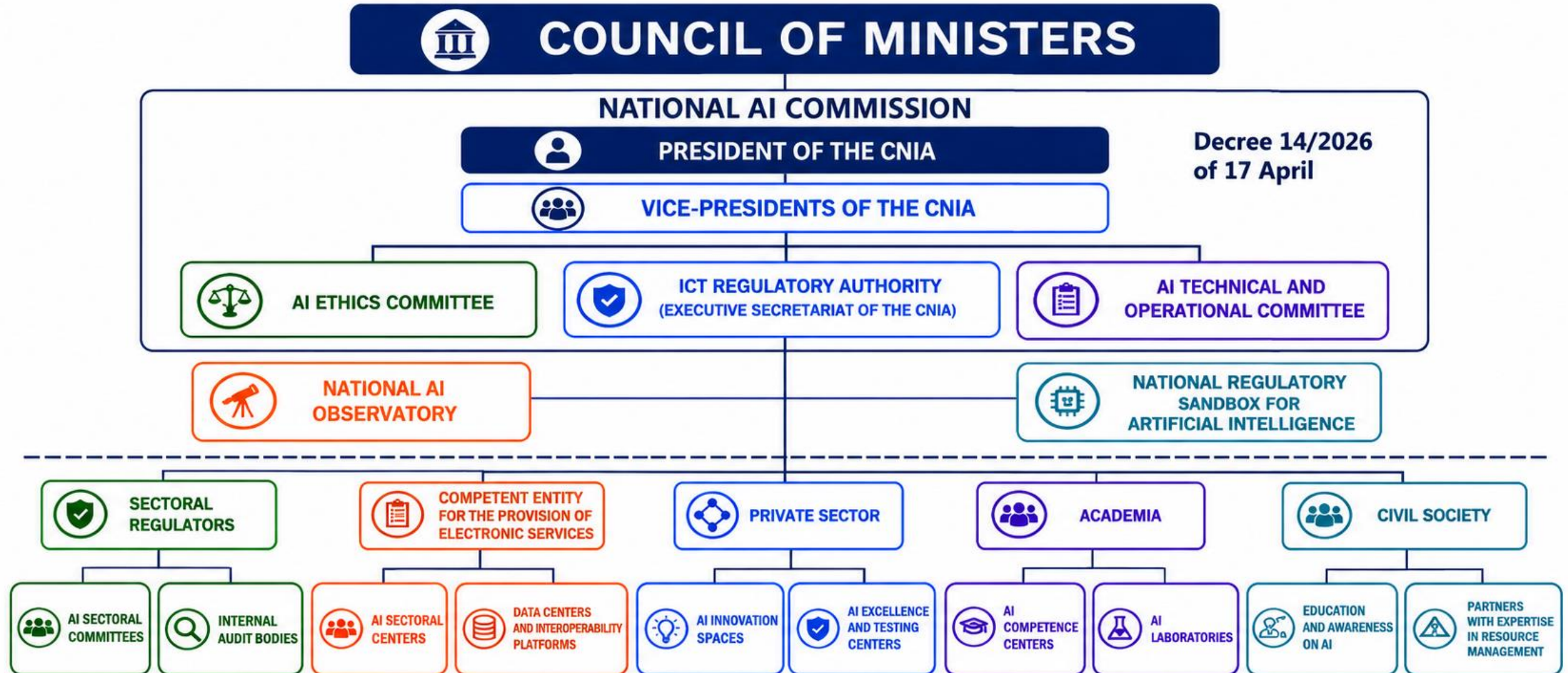
National Model of AI Layers





IV. Innovation and the AI Economy

AI Governance: Institutions, Oversight and Trust





IV. Innovation and the AI Economy

National Artificial Intelligence Commission

President: Minister of Communications and Digital Transformation

Vice-Presidents: Ministers of Education and of National Defence

Representatives from the sectors responsible for the following areas:

1.	Information and Communication Technologies
2.	Communications
3.	Health
4.	Energy
5.	Industry
6.	Trade
7.	Agriculture
8.	State Administration and Public Service
9.	National Defence
10.	Finance
11.	Education
12.	Labour

Representatives from the following entities:

13.	State Information and Security Service
14.	ICT Regulatory Authority
15.	Communications Regulatory Authority
16.	National Cybersecurity Council
17.	National Geo-Spatial Development Agency (ADE)
18.	Financial Sector Regulatory Authority
19.	Regulatory Authority for the Scientific Research Sector in Human Health
20.	National Council for Ethics in Scientific Research
21.	Supreme Court
22.	Public Prosecution Service
23.	Civil Society
24.	Private Sector



V. Building Trust through Cybersecurity

One Ecosystem: Data + Infrastructure + Innovation + Trust



Trust is the foundation for a resilient, inclusive and prosperous AI economy.

V. Building Trust through Cybersecurity

Proposal for the National Cybersecurity Strategy

Pillars

The 2026–2030 Strategy adopts a modern approach based on cybersecurity resilience, digital trust and digital sovereignty, structured around the following pillars:

- | | |
|---|---|
|  | 1 Governance, Leadership and National Coordination; |
|  | 2 Protection and Resilience of Critical Infrastructures; |
|  | 3 Prevention, Detection, Response and Incident Recovery; |
|  | 4 Human Capital, Skills and Cybersecurity Culture; |
|  | 5 Digital Trust, Digital Identity and Trust Services; |
|  | 6 Fight against Cybercrime and International Cooperation; |
|  | 7 Emerging Threats, Research and Innovation. |



*A safer, more resilient
and digitally sovereign Mozambique*



V. Building Trust through Cybersecurity

Policy and Regulatory Alignment

 Instrument	 Main Contribution to the AI Economy
 Data Governance Policy and Strategy	High-quality, trusted and well-governed data
 Digital Transformation Strategy	Digital government and public services
 National Artificial Intelligence Strategy	Innovation and AI adoption
 Cybersecurity Strategy	Trust and resilience in the digital ecosystem
 Data Protection Law	Privacy and fundamental rights
 Cloud Computing Regulation	Scalable and secure infrastructure
 Data Centre Regulation	Computing infrastructure and data sovereignty
 Interoperability Framework	Data exchange and integration across systems

□ VI. From Frameworks to Economic Value



What Does This Mean for Mozambique's AI Economy?



Government



Better public services



Evidence-based decision-making



More efficient and transparent government

A more responsive, effective and citizen-centric public sector.



Private Sector



Startups and innovation



New AI-enabled businesses



Increased productivity and competitiveness



New digital products and services

A more dynamic and competitive economy.



Academia & Research



Research and development



Skilled talent



Innovation and entrepreneurship



Technology transfer and collaboration with industry

Knowledge, talent and innovation for national development.



Society



Inclusion and equal opportunities



Better and more affordable services



Protection of rights and trust



Improved quality of life and sustainable development

A more inclusive, prosperous and trustworthy society.

Turning our frameworks into real impact for people, businesses and a more prosperous Mozambique.



VI. From Frameworks to Economic Value

Key Challenges and Priorities Ahead

	Limited computing capacity	Invest in scalable and cost-effective computing infrastructure.		Cybersecurity	Enhance cybersecurity capabilities and resilience.
	Availability and quality of data	Strengthen data governance, standards and data sharing.		Interoperability	Ensure interoperability across government systems and sectors.
	Skills and talent	Develop a skilled workforce and attract and retain talent.		Responsible AI	Promote ethical, transparent and human-centric AI.
	Investment	Mobilize public and private investment in digital and AI.		Private-sector adoption	Create an enabling environment for business innovation and AI adoption.
	Regulatory capacity	Strengthen institutional capacity for effective and agile regulation.		Sustainable digital infrastructure	Invest in resilient, inclusive and environmentally sustainable infrastructure.

From establishing frameworks to implementing them at scale.



VII. Conclusion

Mozambique is progressively building the foundations for a **trusted AI economy**, supported by an increasingly integrated ecosystem of data, digital infrastructure, innovation and cybersecurity. The effective governance, protection and responsible reuse of data, combined with secure, scalable and resilient digital infrastructure, are essential to creating the conditions for the development and adoption of AI.

At the same time, **innovation, research, startups, industry and skills** are critical to transforming these foundations into practical AI solutions and economic opportunities. **Cybersecurity, the protection of rights and accountability** are equally important to building the trust required for the sustainable adoption of AI across government, the private sector, academia and society.

Ultimately, the challenge is to move **from regulation to innovation, from data to value, and from infrastructure to an AI economy**. This requires not only establishing the necessary legal and regulatory frameworks, but also ensuring their effective implementation at scale, so that AI contributes to inclusive growth, improved public services, greater competitiveness and a more prosperous Mozambique.

By working together, we can turn these foundations into real and lasting impact for people, businesses and a more prosperous Mozambique.



Thank you very much
for your kind attention!