

Regulations.AI

Overview of AI Regulations Globally

16 December 2025

Table of Contents

1. Argentina
2. Australia
3. Austria
4. Bangladesh
5. Belgium
6. Brazil
7. Bulgaria
8. Canada
9. Chile
10. China
11. Colombia
12. Costa Rica
13. Croatia
14. Cyprus
15. Czech Republic
16. Denmark
17. Ecuador
18. Egypt
19. Estonia
20. Ethiopia
21. European Union
22. Finland
23. France
24. Germany
25. Ghana
26. Greece
27. Hong Kong
28. Hungary
29. Iceland
30. India
31. Indonesia
32. Iran
33. Iraq
34. Ireland
35. Israel
36. Italy
37. Japan
38. Kazakhstan
39. Kenya
40. Latvia
41. Lithuania
42. Luxembourg
43. Malaysia
44. Maldives
45. Malta
46. Mexico
47. Morocco
48. Netherlands
49. New Zealand
50. Nigeria
51. Norway
52. Pakistan
53. Panama
54. Peru
55. Philippines
56. Poland
57. Portugal
58. Qatar
59. Romania
60. Russia
61. Rwanda
62. Saudi Arabia
63. Senegal
64. Serbia
65. Singapore
66. Slovakia
67. Slovenia
68. South Africa
69. South Korea
70. Spain
71. Sweden
72. Switzerland
73. Taiwan
74. Thailand
75. Tunisia
76. Turkey
77. Ukraine
78. United Arab Emirates
79. United Kingdom
80. United States
81. Uruguay
82. Uzbekistan
83. Vietnam

Argentina — AI Regulatory Landscape Summary

Overview

Argentina's AI regulatory landscape as of November 18, 2025, is characterised by a layered approach that combines national strategic planning, agency-level guidance, provincial protocols and multiple legislative proposals. The primary strategic anchors are [Agenda Digital 2030](#) and the [Plan Nacional de Inteligencia Artificial \("ArgenIA"\)](#), which set ambitions for digital transformation, capacity-building and ethical considerations in public policy. Operationalisation has occurred through administrative acts and agency resolutions focused on transparency, data protection and the public sector's adoption of AI. Meanwhile several bills introduced in the national legislature aim to create binding legal regimes, criminal prohibitions and sectoral rules.

Regulatory Instruments

- [Agenda Digital 2030 \(Digital Agenda 2030\)](#) - Strategic national digital transformation roadmap (Enacted/Published; strategic plan).
- [Plan Nacional de Inteligencia Artificial \("ArgenIA"\)](#) - National AI plan focused on research, capacity-building, ethics and public adoption (Enacted/Published; strategic plan).
- [Resolución 90/2021 – Programa de Inteligencia Artificial](#) - Administrative program to coordinate AI initiatives across public agencies (Enacted/Published; resolution).
- [Presentación del Centro Argentino Multidisciplinario de Inteligencia Artificial \(CAMIA\)](#) - Launch/presentation of a multidisciplinary AI center to foster research and collaboration (Enacted/Published; institutional initiative).
- [Expediente 1472-D-2023 – Modificaciones a la Ley 25467](#) - Proposed amendments to the Science, Technology & Innovation law to cover AI explicitly (Proposed; bill).
- [Expediente 2504-D-2023 – Uso de la Inteligencia Artificial en la Educación](#) - Bill proposing rules for AI use in education, including safeguards for minors and curricula (Proposed; bill).
- [Expediente 2505-D-2023 – Investigación, desarrollo y uso de la Inteligencia Artificial](#) - Bill addressing R&D governance, funding and ethical oversight (Proposed; bill).
- [Disposición 2/2023 – "Recomendaciones para una Inteligencia Artificial Fiable"](#) - Practical recommendations for trustworthy AI aimed at public agencies (Enacted/Published; disposition/guidelines).
- [Resolución 161/2023 – Programa de Transparencia y Protección de Datos Personales en el uso de la Inteligencia Artificial \(AAIP\)](#) - AAIP program linking AI use with transparency and data-protection obligations (Enacted/Published; resolution).
- [Senado Expediente 1747/23](#) - Senate project to regulate AI systems; legislative effort that reached debate but did not immediately produce binding law (Ended; legislative project).
- [Decisión Administrativa 750/2023 – Mesa Interministerial sobre Inteligencia Artificial](#) - Administrative decision creating an interministerial coordination table for AI policy (Enacted/Published; administrative decision).
- [Expediente 7225-D-2024 – Incorporación de artículos 128 bis y 131 bis al Código Penal](#) - Proposed criminal-code amendments to penalize dissemination of sexual images generated by AI (Proposed; bill).
- [Resolución 16/2024 – Creación del Comité de Innovación sobre Inteligencia Artificial \(Dirección General de Aduanas\)](#) - Agency-level innovation committee to explore AI in customs and trade operations (Enacted/Published; resolution).

- [Expediente 3003-D-2024 – Régimen jurídico aplicable para el uso responsable de la Inteligencia Artificial](#) - Broad bill proposing a legal regime for responsible AI use (Proposed; bill).
- [Expediente 3900-D-2024 – Creación del Observatorio Federal sobre Inteligencia Artificial](#) - Proposed federal observatory to monitor AI deployment and impacts (Proposed; bill).
- [Resolución 710/2024 – Creación de la Unidad de Inteligencia Artificial Aplicada a la Seguridad \(UIAAS\)](#) - Creation of a unit to govern AI use in security contexts (Enacted/Published; resolution).
- [Decreto 2726/2025 – Protocolo para la Adopción y Uso de Tecnologías de Inteligencia Artificial Generativa en la Administración Pública \(Provincia de Santa Fe\)](#) - Provincial decree setting protocols for generative-AI adoption in Santa Fe public administration (Enacted/Published; decree).
- [Resolución 4/2025 – Directrices de uso de Inteligencia Artificial Generativa en la Administración Pública \(Provincia de Buenos Aires\)](#) - Provincial guidelines for generative AI use by Buenos Aires provincial agencies (Enacted/Published; resolution).
- [Resolución de Presidencia 206/2025 – Guía de Recomendaciones y Directrices para el Uso de Sistemas de Inteligencia Artificial en el Poder Judicial de la Ciudad Autónoma de Buenos Aires](#) - Judicial guidance for AI systems in the CABA judiciary (Enacted/Published; resolution).
- [Resolución PGN 14/25 – Creación del Programa de Inteligencia Artificial del Ministerio Público Fiscal](#) - Creation of an AI program within the national prosecution service (Enacted/Published; resolution).
- [Resolución 1486/2025 – Implementación de un Asistente Virtual con Inteligencia Artificial en el Portal de Gestión de Causas \(Poder Judicial de la Nación / Consejo de la Magistratura\)](#) - Implementation resolution for an AI virtual assistant in the national court case management portal (Enacted/Published; resolution).

Key Themes and Priorities

Several common themes run across Argentina's instruments: prioritizing trustworthy AI (ethics, fairness, human oversight), strengthening transparency and data protection (AAIP programs), enabling public-sector modernization (procurement rules, pilot frameworks and virtual assistants), and addressing harms through sectoral or criminal rules (deepfakes/sexual image dissemination). Capacity-building and research promotion (ArgenIA, CAMIA, proposed science-law amendments) aim to anchor long-term capability. Security-focused governance (UIAAS) signals attention to law enforcement and public-safety uses, raising policy trade-offs between effectiveness and rights protection.

Governance Structure

Governance is multi-institutional and federated. Key national actors include the Ministerio de Ciencia, Tecnología e Innovación; the Agencia de Acceso a la Información Pública (AAIP); the interministerial AI Mesa (created by Decisión Administrativa 750/2023); sectoral ministries (Education, Security, Justice, Customs); and the judiciary and prosecution services, which have issued their own directives. Provincial governments (notably Santa Fe and Buenos Aires) exercise autonomous competence over internal administration and have issued binding protocols. Proposed observatories and dedicated units (CAMIA, UIAAS, proposed Federal Observatory) are intended to provide technical expertise, oversight and monitoring capacity.

Implementation Status

Most strategic documents and administrative resolutions are enacted and in force, serving as immediate guidance. Bills remain under consideration in the legislature and would be required to create comprehensive, binding national rules. Implementation gaps include resource allocation, consistent enforcement mechanisms, harmonisation across provinces and clear liability rules for private-sector actors. The pace of provincial and judicial adoption indicates demand for operational rules, while the national legislature continues to debate higher-level statutory approaches.

Future Developments

Expect continued legislative activity to codify obligations on transparency, data protection and liability; potential criminal-law amendments specifically targeting harms caused by AI-generated sexual imagery; and further institutional consolidation (observatory, standards, certification or audit regimes). Argentina is likely to continue aligning policy language with international principles (OECD, UNESCO), while pursuing regionally tailored solutions.

International Context

Argentina's trajectory reflects global trends: emphasis on trustworthy AI, sector-specific rules, and a combination of soft law and emerging statutory proposals. Practitioners should track international instruments and consider interoperability with GDPR-style data regimes and international standards. For further information consult official portals such as [Argentina.gob.ar](https://www.argentina.gob.ar) and agency pages like the [Agencia de Acceso a la Información Pública \(AAIP\)](https://www.aaip.gob.ar).

Australia — AI Regulatory Landscape Summary

Overview

Australia's AI regulatory landscape blends national principles, capability-building and action plans with state-level operational mandates and sectoral guidance. The approach is pragmatic and risk-based: national instruments such as the AI Ethics Framework and the National AI Action Plan establish overarching principles and strategic priorities, while agencies and states (notably NSW, Queensland and Victoria) have developed mandatory operational frameworks, assurance processes and procurement controls for public sector use. The Commonwealth has also published discussion materials and an interim response under the "Safe and Responsible AI in Australia" program and advanced a National Framework for the Assurance of Artificial Intelligence in Government to govern federal deployments.

Regulatory Instruments

- [AI Ethics Framework \(Australia\) / Australia's AI Ethics Principles](#) – Foundational voluntary principles for developers and users of AI emphasising fairness, transparency, human-centred values and accountability. (Status: Enacted/Published; Type: Principles / Framework)
- [National AI Action Plan \(AI Action Plan\)](#) – Strategic national plan to build capability, accelerate adoption, and align research, industry and government investments. (Status: Enacted/Published; Type: Strategy / Action Plan)
- [National Artificial Intelligence Centre \(NAIC\) — CSIRO Data61](#) – Dedicated centre to coordinate government research, capability building and standards work across AI. (Status: Enacted/Published; Type: Institutional / Centre)
- [Safe and Responsible AI in Australia — Discussion Paper](#) – Commonwealth consultation paper exploring potential regulatory reforms and options for mandatory protections in high-risk settings. (Status: Enacted/Published; Type: Discussion Paper / Consultation)
- [Safe and Responsible AI in Australia — Government Interim Response to Consultation](#) – Interim policy response summarising Commonwealth positions and next steps following consultation. (Status: Enacted/Published; Type: Policy Response / Roadmap)
- [National Framework for the Assurance of Artificial Intelligence in Government](#) – A procedural framework setting assurance artefacts, governance roles and processes for federal government AI deployments. (Status: Enacted/Published; Type: Framework / Assurance)
- [NSW Artificial Intelligence Assessment Framework \(AIAF\)](#) – Operational risk and assessment framework for NSW public sector AI use; includes templates and mandatory assessment steps. (Status: In force; Type: Assessment Framework / Mandatory for NSW agencies)
- [DCS-2024-04 – Use of Artificial Intelligence by NSW Government Agencies \(NSW circular making AI Ethics Policy and AIAF mandatory\)](#) – Administrative circular requiring NSW agencies to adopt an AI Ethics Policy and apply the AIAF. (Status: In force; Type: Circular / Administrative Mandate)
- [Standard for AI transparency statements](#) – Template/standard requiring standardised transparency statements for AI systems (used in procurement and deployment). (Status: In force; Type: Standard / Transparency)
- [Proposals Paper for Introducing Mandatory Guardrails for AI in High-Risk Settings](#) – Paper proposing targeted mandatory requirements where AI poses significant public risk. (Status: Enacted/Published; Type: Policy Proposal / Consultation)

- [Artificial intelligence governance policy \(Queensland Government\)](#) – Queensland’s mandatory governance policy setting expectations for AI use across state agencies. (Status: In force; Type: Policy / Mandatory for QLD agencies)
- [Foundational Artificial Intelligence Risk Assessment \(FAIRA\) guideline \(Queensland Government\)](#) – Practical guideline and risk-assessment methodology for Queensland agencies to assess AI risk and mitigation. (Status: In force; Type: Guideline / Risk Assessment)
- [Policy for the responsible use of AI in government](#) – Cross-jurisdictional policy instrument setting minimum expectations for responsible AI use by public agencies. (Status: In force; Type: Policy)
- [Standard for accountable officials \(Policy for responsible use of AI in government\)](#) – Companion standard that defines roles, responsibilities and accountability obligations for named officials overseeing AI systems. (Status: In force; Type: Standard / Accountability)
- [Voluntary AI Safety Standard \(VAISS\)](#) – A voluntary technical safety standard intended to guide industry best practice on robustness and risk controls. (Status: Enacted/Published; Type: Voluntary Technical Standard)
- [Administrative Guideline for the safe and responsible use of Generative Artificial Intelligence in the Victorian Public Sector](#) – Operational guidance for Victorian agencies addressing generative AI risks, controls and procurement. (Status: In force; Type: Guideline / Administrative)
- [DTA AI Policy Update - Impact Assessment Tool and Procurement Guidance](#) – Updated tools and procurement guidance from the Digital Transformation Agency to operationalise impact assessments and supplier requirements. (Status: In force; Type: Policy Tools / Procurement Guidance)
- [Australia National AI Plan 2025](#) – National plan aligning capability, regulatory priorities and investments through 2025. (Status: In force; Type: Strategy / National Plan)

Key Themes and Priorities

Several clear priorities run across instruments:

- Risk-based regulation: most instruments adopt a risk-proportionate approach, with more stringent processes for high-impact or high-risk uses (health, social services, law enforcement and safety-critical systems).
- Assurance and documentation: the National Framework for Assurance, NSW AIAF, FAIRA (Queensland) and DTA tools emphasise consistent assessment artefacts, logging, testing and evidence trails to support governance and auditability.
- Accountability and governance: policies mandate accountable officials and governance structures inside agencies, while standards and templates clarify roles and responsibilities.
- Transparency and consumer protection: the Standard for AI transparency statements and related guidance require public-facing explanations, recordkeeping and procurement-level transparency obligations.
- Procurement and supplier controls: DTA procurement guidance and state frameworks require contractual obligations on suppliers to support assurance, testing and incident response.
- Voluntary technical workstreams: VAISS and NAIC-led initiatives support industry adoption of robustness, safety and testing best practices while preserving flexibility.

Governance Structure

The architecture is multi-layered and collaborative. Key national bodies include the Department of Industry (policy leadership), the [CSIRO Data61 / National Artificial Intelligence Centre \(NAIC\)](#) (capability, research and standards development), the [Digital Transformation Agency \(DTA\)](#) (federal policy tools, procurement and impact assessment), and the [Office of the Australian Information Commissioner \(OAIC\)](#) (privacy and data protection oversight). States maintain their own digital/IT governance teams and central agencies (for example [NSW](#)

[Government](#), [Queensland Government](#) and [Victorian Government](#)) which operationalise mandatory frameworks and circulars for their public sectors. Standards Australia and other technical forums contribute to voluntary standard development (e.g., VAISS).

Implementation Status

Implementation varies by instrument: foundational national principles and the NAIC are established and widely referenced; the National Framework for Assurance and DTA tools are published and being used across federal agencies; state frameworks in NSW, Queensland and Victoria are already in force and apply mandatory processes within those jurisdictions. The Commonwealth's discussion paper, interim response and proposals for guardrails indicate ongoing consultation and a likely trajectory toward targeted mandatory obligations for particularly hazardous or high-impact AI use-cases. Many federal and state agencies are actively updating procurement templates, training staff, and appointing accountable officials to meet the new expectations.

Future Developments

Near-term developments are likely to include: the potential introduction of targeted mandatory guardrails for identified high-risk domains, broader adoption of standardised transparency statements, consolidation of assurance artefacts across jurisdictions for interoperability, and continued development of voluntary technical standards (VAISS) into normative procurement criteria. Australia seeks to align with international norms (OECD, G20 and major trading partners) while retaining a pragmatic, implementable focus on government assurance and public sector deployments.

International Context

Australia's program positions the country as a collaborative middle-power aligning its principles and practical artefacts with OECD and other international AI governance workstreams. The preference for a risk-based, sectoral mix of voluntary standards plus targeted mandates mirrors approaches being adopted in other jurisdictions, facilitating cross-border interoperability while allowing domestic flexibility. Practitioners working across markets should monitor both Australian federal developments and state-level mandates that may impose additional obligations.

For more information and primary sources see the websites of the Department of Industry (<https://www.industry.gov.au>), CSIRO (<https://www.csiro.au>), the Digital Transformation Agency (<https://www.dta.gov.au>), the Office of the Australian Information Commissioner (<https://www.oaic.gov.au>) and the relevant state government portals (for example [NSW](#), [Queensland](#) and [Victoria](#)).

Austria — AI Regulatory Landscape Summary

Overview

Austria's AI policy framework combines a strategy-led approach with operational instruments and funding to encourage trustworthy, human-centred AI while preparing for EU-wide rules. The national AI strategy "Artificial Intelligence Mission Austria 2030 (AIM AT 2030)" provides the strategic backbone; it is implemented through sectoral measures, funding lines and operational services. This framework is embedded within broader digital governance tools such as the [Digital Austria](#) programme and Austria's National Roadmap for the Digital Decade. Austria has emphasised practical readiness for the EU Artificial Intelligence Act ([Regulation \(EU\) 2024/1689](#)) by building service capacity, preparing supervisory arrangements and aligning domestic transparency and data access initiatives.

Regulatory Instruments

- [AI for Green \(funding initiative to apply AI for climate and environmental challenges\)](#) - A targeted funding/programme stream (run via the FFG and related instruments) to promote AI applications for sustainability and environmental protection; status: In force; type: funding initiative/programme.
- [Artificial Intelligence Mission Austria 2030 \(AIM AT 2030\)](#) - Austria's national AI strategy (published 2021) setting principles, priority fields and measures through 2030; status: In force; type: national strategy/roadmap.
- [Digital Austria Act \(Digitales Arbeitsprogramm der Bundesregierung\)](#) - The federal digital programme with cross-ministerial measures for public administration digitalisation and AI governance; status: Passed/Active; type: executive programme/strategic act.
- [Nationaler strategischer Fahrplan für die Digitale Dekade Österreich \(Digital Decade Roadmap\)](#) - Austria's national roadmap aligning national digital targets to the EU Digital Decade (digital skills, infrastructure, data) through 2030; status: Enacted/Published; type: strategic roadmap.
- [Beirat für Künstliche Intelligenz \(AI Advisory Board / KI-Beirat\)](#) - A consultative advisory council that provides independent technical, ethical and societal advice to government and RTR; status: In force; type: advisory body.
- [Digital Skills Initiative \(Digitale Kompetenzoffensive\)](#) - Nationwide digital competence programme including AI literacy components (workshops, curricula); status: In force; type: national skills initiative.
- [KI-Maßnahmenpaket \(AI measures package\)](#) - A set of administrative and policy measures (preparing a labelling approach, servicelated architecture and monitoring activities) to increase transparency and preparedness for the AI Act; status: Enacted/Published; type: policy/implementation package.
- [KI-Servicestelle \(AI Service Office\) — establishment at RTR](#) - Operational helpdesk and information hub hosted at the RTR to assist stakeholders with AI questions and AI Act readiness; status: Passed/Operational; type: service office / preparatory body.
- [Datenstrategie für Österreich \(Data Strategy for Austria\)](#) - National data strategy and associated measures to enable trusted reuse of public and protected data; status: Enacted/Published; type: strategy / enabling framework.
- [Informationsfreiheitsgesetz \(Freedom of Information Act\)](#) - Establishes proactive publication duties and access to government-held information, strengthening transparency for AI deployments in the public sector; status: In force (phased implementation); type: statutory law.

- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(AI Act\)](#) - The EU-level risk-based AI regulation that sets obligations for providers, deployers and Member States; status: In force at EU level with phased applicability; type: EU Regulation.
- [Digital Austria Act 2.0 \(Digital Austria Act — 2.0 / Digital Austria Act: Digital Sovereignty measures\)](#) - An update extending the Digital Austria strategy with a stronger focus on digital sovereignty, administration AI projects and interoperability; status: Passed/Published; type: strategic update / policy package.
- [Strategy of the Federal Government for Artificial Intelligence – Implementation Plan 2024 \(KI-Umsetzungsplan 2024\)](#) - The government's 2024 implementation plan translating AIM AT 2030 measures into actionable short- and medium-term steps, including monitoring and priority projects; status: Enacted/Published; type: implementation plan.

Key Themes and Priorities

Across instruments Austria emphasises: (1) Trustworthy, human-centred AI and alignment with fundamental rights; (2) public-sector uptake and digital sovereignty (including administration-specific KI projects and an AI map of public deployments); (3) data access and re-use (Data Strategy & data governance); (4) skills and inclusion via the Digitale Kompetenzoffensive; and (5) practical readiness for the EU AI Act through services, monitoring and capacity-building. Sectoral priorities include climate/environment (AI for Green), health, transport and education.

Governance Structure

Coordination is led by the Bundeskanzleramt and the Digital Austria governance architecture, supported by inter-ministerial fora (AI Policy Forum) and advisory bodies (KI-Beirat). Operational tasks and early implementation support are delegated to agencies such as the RTR (KI-Serviceestelle), FFG (research funding), Statistik Austria and the Bundesrechenzentrum. The national supervisory and market surveillance responsibilities required by the EU AI Act are being prepared across ministries and agencies; RTR is a central node in the planned supervisory ecosystem.

Implementation Status

Implementation is active and pragmatic: many AIM AT measures have moved into execution (funding calls, pilots, skills programmes). The RTR KI-Serviceestelle is operational and publishes guidance and studies; the FFG runs AI funding strands including AI for Green. The Digital Austria Act and its 2.0 update steer public administration projects and digital sovereignty measures. The Informationsfreiheitsgesetz imposes proactive transparency obligations which intersect with AI accountability requirements. Austria coordinates implementation to align with the EU AI Act timelines and is creating the infrastructure (registries, service desks, supervisory capacity) necessary for compliance.

Future Developments

Near-term priorities include finalising national supervisory roles for the EU AI Act, deploying the planned AI-Landkarte (administrative AI map), advancing the administration-level language model pilot, consolidating the KI-Serviceestelle into supervisory processes, expanding AI-for-Green and other strategic funding calls, and deepening skills and literacy at population scale. The Digital Austria Act 2.0 will accelerate digital sovereignty measures in procurement and cloud/data infrastructure.

International Context

Austria places a strong emphasis on EU alignment: national instruments are explicitly designed to integrate the AI Act, the EU Data Strategy and the Digital Decade. Austria participates in EU coordination mechanisms and uses EU

funding and policy instruments to reinforce domestic initiatives. Official national materials and guidance are published via the national AI portal (ki-strategie.at), the Digital Austria hub (digitalaustria.gv.at) and operational guidance from RTR (rtr.at/ki-servicestelle).

For foundational documents consult the national AI portal ([AI Strategy / AIM AT 2030](#)), the Digital Austria central pages ([Digital Austria](#)), RTR's KI-Servicestelle ([RTR KI-Servicestelle](#)) and the EU text of the AI Act ([Regulation \(EU\) 2024/1689](#)).

Bangladesh — AI Regulatory Landscape Summary

Overview

Bangladesh's AI regulatory framework as of 2025 is best understood as a layered and transitional architecture that combines: (1) broad cyber and security-focused laws; (2) national strategies and policy documents that guide public-sector adoption and capacity building; and (3) draft and sectoral instruments intended to govern platforms, data protection and administrative oversight. The instruments listed here reflect that mixture: some are enacted laws with enforcement mechanisms, others are strategy/policy documents or drafts that indicate the government's intentions but are not yet binding law.

Regulatory Instruments

- [Digital Security Act, 2018 \(ডিজিটাল নিরাপত্তা আইন, ২০১৮\)](#) - Historically a central statute addressing online offences, content-related criminality and digital investigation powers. Status: Ended (per dataset). Type: Enacted (now terminated/replaced in practice by subsequent legislation or policy measures where indicated).
- [National Strategy for Artificial Intelligence: Bangladesh \(National Strategy for Artificial Intelligence Bangladesh\)](#) - Published national strategy providing objectives, priority use-cases (e.g., agriculture, healthcare, public services), capacity-building plans and institutional roles to promote AI adoption. Status: Enacted/Published. Type: Strategy / policy document.
- [Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms \(draft\)](#) - Draft sectoral regulation proposing new oversight and compliance rules for digital platforms, social media and over-the-top (OTT) services, likely including content moderation obligations, local representation and reporting duties. Status: Draft. Type: Sectoral regulation (telecommunications/platforms).
- [Draft Personal Data Protection Act / Draft Data Protection Act 2023](#) - Proposed comprehensive data protection law intended to define personal data rights, lawful bases for processing, controller/processor obligations, security measures and cross-border transfer rules. Status: Proposed. Type: Draft statute (data protection).
- [Agency to Innovate \(a2i\) Bill / Agency to Innovate Act 2023](#) - Legislation creating or strengthening the Agency for Innovation (a2i) to lead public-sector digitization, innovation programming and deployment of AI-enabled public services; confers administrative mandate, budgetary and programmatic authority. Status: Passed. Type: Enabling/organizational statute.
- [Cyber Security Act, 2023 \(সাইবার নিরাপত্তা আইন, ২০২৩\)](#) - Enacted statute addressing cyber threats, incident response, obligations on service providers and penalties for cyber offences; acts as a principal law for cyber incident management and enforcement. Status: Enacted/Published. Type: Statute (cybersecurity).
- [National Artificial Intelligence Policy 2024 \(Draft\)](#) - Draft policy document intended to complement the national strategy with concrete policy measures, standards, and governance recommendations for public procurement, ethics, and research support. Status: Draft. Type: Policy/Guidance.

Key Themes and Priorities

Several common themes appear across Bangladesh's regulatory instruments:

- State-led digital transformation: Centralization of AI adoption within public-sector modernization programs (a2i) and national strategy documents prioritizing economic development, service delivery and productivity gains.

- Security and order: Cyber- and content-focused laws reflect priorities on national security, public order and controlling online harms — shaping enforcement posture and investigative powers that will affect AI systems and platforms.
- Emerging data governance: The proposed Draft Personal Data Protection Act indicates movement toward rights-based data regulation which is a precondition for trustworthy, privacy-preserving AI.
- Platform accountability: The BTRC draft signals regulatory expansion into platform governance, which may impose operational duties on social media and OTT providers that host AI-enabled recommendation and moderation systems.
- Capacity and innovation: Strategy and draft policy emphasize capacity building, research funding, standards development and public–private collaboration to foster a local AI ecosystem.

Governance Structure

Key actors and roles include:

- Agency for Innovation (a2i): Operational lead for public-sector digitization and AI adoption; with the passage of the a2i Act (2023) it is positioned to coordinate pilots, set procurement criteria and issue practical guidance for government AI projects. More information about a2i's programs is public on the Agency's website, e.g. <https://a2i.gov.bd>.
- Bangladesh Telecommunication Regulatory Commission (BTRC): Sector regulator likely to enforce draft rules for digital, social media and OTT services and manage obligations for intermediaries; homepage: <https://www.btrc.gov.bd>.
- Ministry of Posts, Telecommunications and Information Technology (or relevant ICT ministry): Policy coordination, legislative sponsorship and alignment of national strategy and AI policy.
- Law enforcement and national cyber authorities: Implement and enforce the Cyber Security Act and related measures; handle incident response and investigative activities under enacted laws.
- Other stakeholders: Bangladesh Computer Council (BCC), universities and research centres, private sector AI firms, civil-society organizations and international partners providing technical assistance.

Implementation Status

Implementation varies by instrument: the Cyber Security Act (2023) and the a2i Act (2023) are enacted and provide tangible legal and institutional change. The National Strategy for Artificial Intelligence (published) already informs budgetary and programmatic priorities. Draft instruments — the BTRC regulation, the Draft Personal Data Protection Act (2023) and the National AI Policy 2024 — remain subject to consultation and revision. Until the Draft Data Protection Act is finalized and enacted, private- and public-sector actors face legal uncertainty on data rights and compliance obligations; similarly, the BTRC draft could materially shift platform obligations if adopted in final form.

Future Developments

Key near-term developments to track include: the legislative fate of the Draft Personal Data Protection Act (will it be adopted in whole, amended or deferred); finalization of the National AI Policy (2024 draft) and the practical standards it recommends; adoption or modification of the BTRC platform regulation draft; and secondary guidance from a2i and sectoral regulators implementing elements of the national strategy (procurement rules, pilot standards, data-sharing frameworks). International engagement (technical cooperation, standards harmonization) will influence these domestic steps, particularly around data transfers and AI safety standards.

International Context

Bangladesh's emerging framework shows parallels with other jurisdictions that pair cybersecurity and platform rules with later-stage data protection and AI policy work. The sequence — security statutes first, then strategy and administrative reform (a2i), and subsequently data protection and sectoral platform regulation — reflects a pragmatic, state-led model of digital governance. International comparators and partnership opportunities include data-protection frameworks, interoperable standards for AI safety and transparency, and capacity-building programs from multilateral partners. Implementing internationally recognized good practices (risk-based regulation, transparency, data protection aligned with global norms) will increase interoperability for trade and research collaborations.

For more information about relevant agencies and to monitor primary sources, consult the Agency for Innovation (a2i): <https://a2i.gov.bd> and the Bangladesh Telecommunication Regulatory Commission: <https://www.btrc.gov.bd>. Official government portals and ministry pages publish bills, gazettes and consultation drafts as they become public.

Belgium — AI Regulatory Landscape Summary

Overview

Belgium's AI policy and regulatory architecture is the product of its federated political system and strong multistakeholder engagement. The landscape combines: (a) a national coalition and coordination mechanism (AI4Belgium) that produces roadmaps, guidance and practical tools; (b) regionally owned programmes and research initiatives (the Vlaams Onderzoeksprogramma / AI Vlaanderen in Flanders, DigitalWallonia4.AI in Wallonia) that fund and coordinate research, skills and adoption; (c) a Brussels-based institute (FARI) that provides research, testbeds and public-sector experimentation for the capital region; and (d) direct applicability of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which is the binding legal framework for many AI uses in Belgium. These elements act in complementary ways: regional initiatives mobilise research and industrial adoption; the national coalition concentrates on coordination and community-building; the EU Act sets mandatory legal standards which national and regional actors help stakeholders meet. ([altai.ai4belgium.be](https://altai.ai4belgium.be/?utm_source=openai))

Regulatory Instruments

- [AI4Belgium \(Belgian national AI coalition / roadmap\)](#) - A national, multi-stakeholder coalition and roadmap that coordinates federal guidance, produces practical assessment tools (for example an ALTAI-based assessment instance), organises working groups and supports public-private collaboration. Status: In force. Type: National coalition / policy roadmap / implementation support tool. ([altai.ai4belgium.be](https://altai.ai4belgium.be/?utm_source=openai))
- [Vlaams Onderzoeksprogramma Artificiële Intelligentie \(Flemish AI Research Programme / AI Vlaanderen\)](#) - A regionally financed strategic research programme and policy package in Flanders that links universities, research centres and industry to fund basic and applied AI research, demonstrators and adoption supports; it is paired with implementation measures, a Flemish AI Expertisecentrum and a skills agenda. Status: In force. Type: Regional research programme & policy plan. ([imec.be](https://www.imec.be/nl/vlaamse-innovatiemotor/samenwerking/vlaamse-onderzoeksprogrammas/vlaams-ai-onderzoeksprogramma?utm_source=openai))
- [DigitalWallonia4.AI \(Walloon AI programme / Digital Wallonia AI\)](#) - A Walloon digital strategy programme to accelerate AI adoption and ecosystem development across four axes (society, businesses, training, partnerships/research). It funds adoption schemes, cluster initiatives (Start IA), and a regional research fund (ARIAC / TRAIL). Status: In force. Type: Regional programme / ecosystem & adoption support. ([digitalwallonia.be](https://www.digitalwallonia.be/en/posts/digitalwallonia4-ai-artificial-intelligence-at-the-service-of-citizens-and-companies-in-wallonia/?utm_source=openai))
- [FARI – Artificial Intelligence for the Common Good Institute \(Brussels AI institute / roadmap\)](#) - A university-led institute (VUB & ULB) with an AI Test & Experience hub, an AI Academy and research hubs focused on urban and public-interest AI projects; it supports regional pilots, public-sector experiments, training and civic engagement. Status: In force. Type: Regional research institute & testbed. ([fari.brussels](https://www.fari.brussels/?utm_source=openai))
- [Artificial Intelligence Act \(Regulation \(EU\) 2024/1689\) — applicable in Belgium as EU regulation](#) - The EU's risk-based regulatory framework for AI systems; it establishes prohibitions, obligations for high-risk systems, transparency rules for certain AI, conformity assessment regimes, market surveillance and enforcement. Status: In force (EU regulation directly applicable). Type: Supranational binding regulation. ([op.europa.eu]

(https://op.europa.eu/en/publication-detail/-/publication/dc8116a1-3fe6-11ef-865a-01aa75ed71a1/language-en?utm_source=openai)

Key Themes and Priorities

Across Belgium's instruments, common themes are prominent: human-centred and trustworthy AI (fundamental rights, non-discrimination, explainability); skills, education and workforce transition (regional academies, training streams and SME support); support for innovation and adoption (grants, Start IA diagnostics, research consortia); testing and experimentation (regional testbeds and FARI's experience hub); and alignment with EU standards and conformity requirements (preparing actors for obligations under Regulation (EU) 2024/1689). Regional economic development and support for SMEs is consistently prioritized alongside ethical and legal safeguards. For practical resources, AI4Belgium hosts assessment tools (ALTAI-based) and community platforms; Flanders hosts a research programme and a public AI Expertisecentrum; Wallonia operates DigitalWallonia4.AI and ARIAC/TRAIL research instruments; Brussels operates FARI as an applied hub. ([altai.ai4belgium.be])(https://altai.ai4belgium.be/?utm_source=openai)

Governance Structure

Governance is distributed: federal public services (eg. BOSA / Strategy & Support at federal level) participate in national coordination and in EU fora; regional departments (Flanders: Departement Economie, Wetenschap en Innovatie (EWI), VLAIO; Wallonia: Agence du Numérique, SPW) lead regional programmes and funding; Brussels (Innoviris, BRIC) funds and hosts FARI projects. Universities and research centres (imec, VIB, VITO, public universities) are central implementers for research and testing. Public-private clusters (Agoria, Infopôle, Réseau IA) and civil-society stakeholders participate in steering committees. This multi-actor governance supports policy alignment, but requires active coordination to translate EU legal obligations into operational procedures (procurement rules, conformity assessments, public sector AI governance). ([[vlaanderen.be](https://www.vlaanderen.be/digitaal-vlaanderen/onze-diensten-en-platformen/ai-expertisecentrum?utm_source=openai)])(https://www.vlaanderen.be/digitaal-vlaanderen/onze-diensten-en-platformen/ai-expertisecentrum?utm_source=openai)

Implementation Status

As of late 2025: the EU AI Act (Regulation (EU) 2024/1689) is in force and authoritative; Belgian regional programmes and AI4Belgium are operational, providing funding, training, testbeds and assessment instruments. Implementation work focuses on: enabling compliance (guidance and tools for documentation, risk assessments and conformity routes); aligning research/testbeds with standardisation work; scaling SME support; and maturing governance and enforcement arrangements. Challenges include the operationalisation of conformity assessment for many AI products, establishing market surveillance responsibilities across levels of government, and ensuring interoperability between regional initiatives and EU technical standards. Practical supports (ALTAI-based assessment, regional testbeds and academy courses) are being used to prepare public and private actors for compliance and responsible deployment. ([op.europa.eu])(https://op.europa.eu/en/publication-detail/-/publication/dc8116a1-3fe6-11ef-865a-01aa75ed71a1/language-en?utm_source=openai)

Future Developments

Expect continued emphasis on: (a) implementing EU technical standards and conformity procedures in Belgium; (b) expanding testbeds and certification pilots to support conformity assessments; (c) further integration of regional training and public-sector procurement guidance with EU obligations; and (d) iterative updates to national/regional roadmaps to reflect standardisation outputs and Commission/EU guidance documents. Public bodies will need to upgrade procurement practices, documentation and monitoring to meet high-risk obligations; industry will need to scale up documentation, data governance and risk-management practices. Continued cross-level coordination (federal-regional-EU) will be crucial.

International Context

Belgium's model—regional research & adoption hubs plus a national coalition—is consistent with other multilevel EU states that combine local experimentation with EU-wide legal harmonisation. Belgian initiatives actively link to European networks, standardisation activities and EU policy instruments; regional programmes contribute to the EU coordinated plan on AI and to international research collaborations. Belgian testbeds and academic institutes (eg. FARI) position Brussels as a practical laboratory for EU urban policy experimentation, while national tools such as AI4Belgium's assessment platforms help small and medium organisations align with EU expectations. For more information, visit the official programme portals: [AI4Belgium / ALTAI tool](#), [AI Vlaanderen / Flanders AI](#), [DigitalWallonia4.AI](#), [FARI](#), and the official EU publication of the Artificial Intelligence Act: [Regulation \(EU\) 2024/1689 \(Artificial Intelligence Act\)](#). ([altai.ai4belgium.be](https://altai.ai4belgium.be/?utm_source=openai))

Brazil — AI Regulatory Landscape Summary

Overview

Brazil's AI regulatory framework is a hybrid architecture composed of strategic national documents, administrative ordinances that operationalize those strategies, sectoral resolutions (notably by the judiciary) and a pending comprehensive legislative proposal. Since early parliamentary initiatives in 2019, the Brazilian approach has gravitated toward coordinating policy tools and building institutional capacity prior to finalizing sweeping statutory obligations. The *Estratégia Brasileira de Inteligência Artificial* (EBIA, 2021) and the *Plano Brasileiro de Inteligência Artificial 2024–2028* (PBIA) are the backbone of public policy, while Decree nº 12.308/2024 and 2025 CITDIGITAL resolutions created governance structures to manage plan delivery. Simultaneously, *Projeto de Lei nº 2.338/2023* seeks to create a national legal framework but remains under review; its progress will determine the transition from a largely strategy-driven system to one with clearer legal obligations for private- and public-sector AI deployments.

Regulatory Instruments

- [Projeto de Lei nº 5.051/2019 \(Principles for the use of Artificial Intelligence in Brazil\)](#) - Early parliamentary proposal to set principles for AI. Status: Ended. Type: Legislative proposal (not enacted).
- [Projeto de Lei nº 5.691/2019 \(Institui a Política Nacional de Inteligência Artificial — National AI Policy\)](#) - Proposed to institute a National AI Policy; influenced subsequent strategy debates. Status: Ended. Type: Legislative proposal (not enacted).
- [Projeto de Lei nº 21/2020 \(Foundations, principles and guidelines for development and application of AI in Brazil\)](#) - Legislative text that has been altered in its parliamentary course; contributed to legislative drafting practice. Status: Changed. Type: Legislative proposal (amended during consideration).
- [Estratégia Brasileira de Inteligência Artificial \(Brazilian Strategy for Artificial Intelligence\)](#) - Core national strategy defining priorities: research, capacity building, public adoption, and ethical guidelines. Status: Enacted/Published. Type: Strategic policy document.
- [Portaria MCTI nº 4.617, de 6 de abril de 2021 \(Ordinance instituting the Brazilian Strategy for Artificial Intelligence\)](#) - Administrative ordinance that formally instituted EBIA within the Ministry of Science and Technology. Status: Enacted/Published. Type: Executive/administrative act.
- [Portaria MCTI nº 4.979, de 13 de julho de 2021 \(Ordinance amending the EBIA annexes\)](#) - Amendment to EBIA annexes (adjusting programs and actions). Status: Enacted/Published. Type: Executive/administrative amendment.
- [Projeto de Lei nº 2.338/2023 \(Marco Legal da Inteligência Artificial — Draft national AI regulatory framework\)](#) - Central draft bill proposing baseline obligations, risk classifications, transparency requirements and oversight mechanisms. Status: Under review. Type: Legislative proposal (pending).
- [Decreto nº 12.308/2024 \(Decree instituting the Interministerial Committee for Digital Transformation / Comitê Interministerial para a Transformação Digital\)](#) - Established an interministerial committee to coordinate digital transformation and AI policy implementation across ministries. Status: Enacted/Published. Type: Executive decree.
- [Plano Brasileiro de Inteligência Artificial 2024-2028 \(Brazilian Plan for Artificial Intelligence, PBIA\)](#) - The operational plan for AI policy with prioritized programs, targets and timelines. Status: Enacted/Published. Type: Strategic/operational plan.

- [Resolução CNJ nº 615/2025 \(CNJ Resolution establishing guidelines for development, use and governance of AI solutions in the Judiciary\)](#) - Judiciary-specific rules setting standards for transparency, testing, accountability and protections for due process. Status: In force. Type: Sectoral regulatory resolution.
- [Resolução CITDIGITAL nº 1/2025 \(Regimento Interno do Comitê Executivo do Comitê Interministerial para a Transformação Digital\)](#) - Internal rules for the executive committee responsible for digital transformation. Status: Enacted/Published. Type: Administrative regulation.
- [Resolução CITDIGITAL nº 2/2025 \(Resolution establishing the Group of Work to manage the Brazilian Plan for Artificial Intelligence - PBIA\)](#) - Formal creation of the working group tasked with PBIA delivery. Status: Enacted/Published. Type: Administrative resolution.
- [Portaria nº 8/2025 \(Portaria establishing the composition of the Group of Work to manage the PBIA\)](#) - Specifies members and roles within the PBIA working group. Status: Enacted/Published. Type: Administrative order.
- [Portaria CNJ nº 270/2025 \(Portaria designating the members of the National Committee on Artificial Intelligence of the Judiciary - Comitê Nacional de Inteligência Artificial do Judiciário\)](#) - Designation of committee members to oversee judiciary AI initiatives. Status: Enacted/Published. Type: Administrative order (judiciary).

Key Themes and Priorities

Common themes across Brazil's AI governance include: (1) coordination and institutional capacity through interministerial bodies and working groups; (2) a risk-based, sector-sensitive posture that favors sectoral rules before blanket prohibitions; (3) promotion of innovation, research, and public-sector adoption to spur economic and social benefits; (4) emphasis on privacy, data protection and transparency, with the ANPD and LGPD central to oversight where personal data are processed; and (5) development of governance safeguards—documentation, impact assessment, human oversight—particularly for high-impact or high-risk uses.

Governance Structure

Primary governance actors include the Ministry of Science, Technology and Innovation (MCTI), the Interministerial Committee for Digital Transformation/CITDIGITAL (established under Decree nº 12.308/2024), technical working groups managing PBIA, and sectoral authorities such as the National Council of Justice for the judiciary. The Autoridade Nacional de Proteção de Dados (ANPD) plays a pivotal role when AI processing involves personal data under the LGPD. The architecture is intentionally multi-stakeholder: government, judiciary, academia and private sector actors are expected to engage through consultations and formal PBIA working groups.

Implementation Status

Implementation is active but uneven. EBIA and PBIA have been published and resourced with governance bodies; CBIA operational annexes were adjusted by MCTI portarias. Working groups and committee membership have been designated under 2024–2025 instruments (Decree nº 12.308/2024, Resoluções CITDIGITAL nº 1/2025 and nº 2/2025, Portaria nº 8/2025). The judiciary has enforceable AI governance through Resolução CNJ nº 615/2025 and Portaria CNJ nº 270/2025. The congressional process on PL 2.338/2023 remains the main outstanding statutory step and will materially affect obligations, enforcement powers, and compliance timelines when/if enacted.

Future Developments

Key items to monitor: final text and parliamentary fate of Projeto de Lei nº 2.338/2023; ANPD guidance or normative acts addressing AI-specific data protection nuances; development of conformity assessment, certification or audit mechanisms; emergence of sectoral rules for high-risk applications; and Brazil's international regulatory alignment (e.g., with the EU AI Act, OECD Guidelines, UNESCO Recommendation). Stakeholders should

prepare governance artefacts—impact assessments, logging and transparency reports, human oversight mechanisms—to align with both current soft-law expectations and potential statutory obligations.

International Context

Brazil positions its AI policy to be interoperable with international standards and principles while protecting national innovation. EBIA and PBIA reference international frameworks and seek dialogue in multilateral fora. The LGPD and the ANPD provide a domestic data-protection backbone closely watched by international partners and investors. Brazil's mix of strategy-driven deployment, sectoral regulation (exemplified by CNJ) and a pending national statute reflects a pragmatic route toward governance that balances innovation, rights protection and international alignment.

Source (official portal): [https://\[government AI portal\]](https://[government AI portal])

Bulgaria — AI Regulatory Landscape Summary

Overview

Bulgaria's artificial intelligence policy architecture in 2025 combines enacted national strategic documents, EU-level legally binding obligations, and a set of draft or proposed national instruments. The principal enacted strategic instruments set long-term priorities for AI development to 2030 and situate AI within the country's broader digital transformation agenda. EU instruments — notably the [EU AI Act](#) (Regulation (EU)) and the [EU Coordinated Plan on Artificial Intelligence](#) — apply directly and shape priorities and legal obligations. In parallel, several drafts from academic, ministerial and political sources signal ongoing national-level legislative and sectoral development (including education and proposed national AI law).

Regulatory Instruments

- [Concept for the Development of Artificial Intelligence in Bulgaria until 2030 \(National AI Strategy\)](#) - A national strategic framework setting priorities for AI research, innovation, public sector adoption, skills and ethics. Status: Enacted/Published. Type: National strategy.
- [National strategy for the development of Artificial Intelligence in Bulgaria \(Bulgarian Academy of Sciences draft\)](#) - A research- and science-led draft emphasizing basic research, capacity building in BAS and ecosystem links. Status: Draft. Type: Academic draft strategy.
- [Digital Transformation of Bulgaria for the period 2020–2030 \(National strategic document\)](#) - A broad digital transformation plan that frames AI as an enabling technology for e-government, industry digitalization and infrastructure. Status: Enacted/Published. Type: National strategic document.
- [National Programme 'Digital Bulgaria 2025'](#) - A time-bound programme focusing on digital public services, infrastructure, skills and adoption measures. Status: Enacted/Published. Type: National programme.
- [Coordinated Plan on Artificial Intelligence \(EU, 2021 review\)](#) - EU-level strategic coordination instrument with recommendations for Member States on R&D, skills, data and innovation. Status: Enacted/Published (applies to Bulgaria as EU Member State). Type: EU coordinated plan.
- [Regulation \(EU\) — AI Act \(Regulation on Artificial Intelligence\)](#) - The EU's risk-based regulatory framework imposing obligations on providers and deployers of AI systems, prohibitions and obligations for high-risk AI. Status: In force (directly applicable in Bulgaria). Type: EU regulation.
- [Draft National Strategy for Artificial Intelligence \(presented by Ministry of Electronic Governance / Ministry of Innovation, project up to 2030\)](#) - A government-level draft intended to harmonize ministerial responsibilities, detail implementation steps and align with the EU AI Act. Status: Proposed/Draft. Type: Government strategy draft.
- [Draft Strategy for the Development and Integration of Artificial Intelligence in Bulgarian Education](#) - Sectoral draft focused on curriculum integration, teacher training, and student skills for AI. Status: Proposed/Draft. Type: Sectoral strategy draft (education).
- [Draft AI Act presented by political party 'Da, Bulgaria' \(project bill for an AI law\)](#) - A political party-led draft that proposes a national AI law; it reflects parliamentary/political interest in codifying AI rules domestically. Status: Proposed/Draft. Type: Draft parliamentary bill.

Key Themes and Priorities

Common priorities across national and EU instruments include: (1) alignment with the EU AI Act and GDPR to ensure legal compliance and market access; (2) capacity-building for research, public administration and business; (3) ensuring trustworthy and ethical AI, including transparency and risk management for high-risk systems; (4) data governance and facilitating responsible access to public-sector data; (5) integration of AI into public services and targeted sectors (health, education, transport); and (6) skills and education initiatives aimed at both workforce reskilling and school curricula. Documents also emphasize private–public partnerships, research funding and European cooperation.

Governance Structure

Key actors referenced in national documents include the Ministry of Electronic Governance (or equivalent e-governance bodies), the Ministry of Innovation, the Bulgarian Academy of Sciences (BAS), the Electronic Government Agency and the Commission for Personal Data Protection (CPDP). The Council of Ministers and interministerial coordination bodies are the anticipated locus for cross-cutting policy decisions. Under the EU AI Act, Bulgaria must designate national competent authorities and a national contact point; national strategies anticipate assigning responsibility to existing ministries/agencies or establishing a focal coordination mechanism to meet EU obligations.

Implementation Status

Strategic instruments (Concept for AI until 2030, Digital Transformation 2020–2030, Digital Bulgaria 2025) are enacted and provide the policy scaffolding and funding priorities. The EU AI Act is in force and creates immediate legal obligations for covered systems. However, practical implementation in Bulgaria requires: (a) operational commitments (budget lines, procurement reform and agency mandates), (b) designation of national supervisory authorities and contact points, (c) development of guidance and standards for public-sector procurement of AI, and (d) capacity-building for regulators and businesses to meet compliance obligations. Draft strategies and proposed bills are still under consultation or parliamentary consideration and will shape the next legislative and operational steps once finalized.

Future Developments

Near-term developments to monitor include finalization of the government-led national AI strategy (Ministry of Electronic Governance/Ministry of Innovation), progress on the education sector AI strategy, any parliamentary movement on the "Da, Bulgaria" draft AI bill, and the concrete designation of national authorities and enforcement resources to implement the EU AI Act. Additionally, implementation instruments such as public procurement rules, national standards for high-risk AI, certification schemes and funding calls for AI R&D and skills will determine the pace of adoption. Bulgaria's 2030 horizon indicates sustained policy attention, but success will depend on implementation capacity and cross-sector coordination.

International Context

Bulgaria's policies are explicitly designed to align with EU frameworks: the EU Coordinated Plan provides strategic priorities while the EU AI Act imposes binding rules that shape compliance and market conditions. Bulgaria participates in EU-level coordination, and national strategies reference European research programmes, Horizon Europe funding channels and cross-border cooperation. For international businesses and researchers, compliance with the EU AI Act and GDPR remains the primary legal requirement; national strategies primarily provide funding, partnership and procurement direction rather than changing EU-level legal duties.

For further reference: official EU materials on the EU AI Act and the Coordinated Plan are published on the European Commission's websites: [EU AI Act information \(European Commission\)](#) and [Coordinated Plan on Artificial Intelligence \(EC\)](#). National documents and drafts are commonly published via Bulgarian government

portals and ministry pages; consult the national e-governance and ministry sites for the latest official texts and consultation materials.

Canada — AI Regulatory Landscape Summary

Overview

Canada's AI regulatory landscape in 2025 is characterized by a layered, risk-based approach that mixes federal strategy, administrative rules for public-sector automated decision-making, voluntary industry codes, technical standards, and provincial initiatives addressing specific domains such as employment. The federal framework emphasizes responsible innovation, capacity-building, risk management and international cooperation. Although a high-profile legislative package (Bill C-27) containing the Artificial Intelligence and Data Act (AIDA) and the Consumer Privacy Protection Act (CPPA) ended in its last introduced form, its proposals continue to inform policy, and multiple federal agencies have published practical instruments and guidance to operationalize responsible AI principles.

Regulatory Instruments

- [Pan-Canadian Artificial Intelligence Strategy \(PCAIS\)](#) - Federal research and capacity-building strategy focused on sustaining AI research leadership, talent and responsible development; Type: Strategy/Program; Status: In force.
- [Algorithmic Impact Assessment \(AIA\) tool \(Treasury Board of Canada Secretariat\)](#) - Practical, risk-based assessment instrument required for federal procurement and deployment of automated decision systems to identify harms, mitigation and governance controls; Type: Administrative tool; Status: In force.
- [Directive on Automated Decision-Making \(Treasury Board of Canada Secretariat\)](#) - Binding Treasury Board directive for federal institutions that sets mandatory requirements around classification, testing, monitoring, human oversight and transparency for ADM systems; Type: Directive (administrative/mandatory for federal public sector); Status: In force.
- [Artificial Intelligence and Data Act \(AIDA\) \(proposed, part of Bill C-27\)](#) - Proposed federal legislation to create risk-based obligations for certain AI systems (now ended in the form presented in Bill C-27); Type: Proposed statute (ended); Status: Ended.
- [Digital Charter Implementation Act \(Bill C-27\)](#) — An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act - Comprehensive bill linking privacy reform and AIDA; Type: Bill/Legislative package (ended); Status: Ended.
- [Consumer Privacy Protection Act \(CPPA\) \(proposed, part of Bill C-27\)](#) - Proposed modernization of federal private-sector privacy law; Type: Proposed statute (ended); Status: Ended.
- [Personal Information and Data Protection Tribunal Act \(PIDPTA\) \(proposed, part of Bill C-27\)](#) - Proposed administrative tribunal mechanism tied to CPPA enforcement; Type: Proposed statute (ended); Status: Ended.
- [Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems](#) - Industry-focused, non-binding code setting expectations for risk management, safety testing, disclosure, and incident reporting for advanced generative AI systems; Type: Voluntary code; Status: Enacted/Published.
- [Canadian Artificial Intelligence Safety Institute \(CAISI\)](#) - Federally supported institute for safety research, standards development and cross-sector coordination on high-risk AI; Type: Institution/initiative; Status: Enacted/Published.
- [Guide on the use of generative AI \(Treasury Board of Canada Secretariat\)](#) - Practical guidance for public servants on procurement, responsible use, sensitive data handling and vendor management when using

generative AI; Type: Guidance; Status: Enacted/Published.

- [Working for Workers Four Act, 2023 \(Bill 149\) — amendments creating Part III.1 re: use of AI in hiring \(Ontario\)](#) - Provincial law introducing obligations and transparency requirements for employers using automated hiring tools; Type: Provincial statute (employment); Status: Passed.
- [Énoncé de principes pour une utilisation responsable de l'intelligence artificielle par les organismes publics \(Québec Ministry of Cybersecurity and Digital Affairs\)](#) - Québec's principles for public-sector use of AI emphasizing rights protection, transparency and accountability; Type: Principles/Guidance (provincial); Status: Enacted/Published.
- [CAN-ASC-6.2 Accessible and Equitable Artificial Intelligence Standard](#) - National standard addressing accessibility, equity and inclusive design in AI systems; Type: Standard; Status: In force.
- [Canada-EU Memorandum of Understanding on Artificial Intelligence](#) - International cooperation agreement to promote regulatory alignment, information sharing and joint research; Type: International MOU; Status: In force.
- [Implementation Guide for Managers of Artificial Intelligence Systems \(Innovation, Science and Economic Development Canada\)](#) - Manager-focused, operational guidance for lifecycle governance, risk assessment and compliance practices for AI systems; Type: Guidance; Status: Enacted/Published.
- [Guideline E-23 — Model Risk Management \(Office of the Superintendent of Financial Institutions\) \(final\)](#) - Final OSFI guideline setting model risk management expectations for federally regulated financial institutions, including AI/ML models; Type: Regulator guideline; Status: Enacted/Published.

Key Themes and Priorities

Several consistent themes run across Canada's instruments: risk-based governance (prioritizing oversight for higher-impact systems); transparency and explainability (impact assessments, documentation and disclosures for affected individuals); privacy and data protection; fairness, accessibility and equity (standards and provincial principles); model and lifecycle risk management (OSFI and manager guides); and international alignment (EU MOU and cooperative initiatives). The federal approach places strong emphasis on public-sector accountability and procurement controls, while industry-facing measures are primarily voluntary or standards-based pending future statutory action.

Governance Structure

Multiple federal bodies share responsibilities: the Treasury Board of Canada Secretariat administers directives and tools for federal institutions ([Treasury Board](#)); Innovation, Science and Economic Development Canada (ISED) leads on industrial strategy and guidance ([ISED](#)); the Office of the Privacy Commissioner provides privacy enforcement and interpretation on personal data practices ([OPC](#)); the Office of the Superintendent of Financial Institutions (OSFI) oversees model risk in the financial sector ([OSFI](#)); and CAISI provides research, standards and safety coordination. Provincial authorities (e.g., Ontario and Québec ministries) regulate in areas under provincial jurisdiction such as employment and public services. International cooperation is coordinated through trade and diplomacy channels and technical collaboration with partners like the EU.

Implementation Status

Implementation is heterogeneous: federal public-sector directives and the AIA tool are operational and mandatory in federal organizations, while voluntary codes, standards and guidance documents have been published and are being adopted by some private entities. The OSFI E-23 guideline is final and informs financial sector governance. Bill C-27 and its contained AIDA/CPPA/PIDPTA package ended in its introduced form, leaving statutory AI-specific obligations for the private sector unimplemented at the federal level as of this snapshot,

though many agencies and stakeholders continue to work on implementing its policy intent through non-statutory means.

Future Developments

Key future developments to watch include any renewed federal legislative efforts to codify AI risk-based obligations, wider uptake and possible formalization of voluntary codes into contractual or sectoral expectations, the maturation of technical standards into compliance baselines (e.g., CAN-ASC-6.2), continued OSFI engagement on AI in finance, and evolving provincial measures that may create a patchwork for certain economic sectors. International alignment efforts, including the Canada-EU MOU, are likely to shape interoperability and cross-border data and compliance expectations.

International Context

Canada's approach deliberately seeks alignment with international partners to enable trade and shared safety practices. The Canada-EU Memorandum of Understanding on Artificial Intelligence and participation in multilateral AI forums support regulatory interoperability. Canada emphasizes standards, research collaboration and adherence to norms that promote safety, human rights and accountable innovation. For more on federal strategy and published guidance see the Government of Canada portal at <https://www.canada.ca>, Treasury Board resources at <https://www.canada.ca/en/treasury-board-secretariat.html>, and Innovation, Science and Economic Development at <https://ised-isde.canada.ca>.

Summary prepared based on enacted directives, published guidance, standards and the list of instruments provided. Stakeholders should monitor parliamentary activity for renewed legislative proposals, departmental notices for implementation timelines, and sector-specific regulators for evolving supervisory expectations.

Chile — AI Regulatory Landscape Summary

Overview

Chile's artificial intelligence regulatory landscape (as of December 1, 2025) is a multi-layered ecosystem combining strategic national policy, sectoral guidance, rights- and consumer-focused instruments, cybersecurity and data-protection statutes, and an active parliamentary docket proposing AI-specific laws and criminal-law amendments. The national policy and its Action Plan provide direction and priorities: responsible innovation, respect for human rights, transparency, capacity building and public-sector risk management. Operationally binding instruments exist for the public sector, cybersecurity and procurement, while multiple bills under review seek to establish comprehensive regulatory and criminal frameworks.

Regulatory Instruments

- [Plan de Acción para la Política Nacional de Inteligencia Artificial \(Action Plan of the National AI Policy\)](#) - Strategic implementation roadmap derived from the National AI Policy that prioritizes capacity building, pilot projects, public-private coordination and regulatory experimentation. (Status: Enacted/Published; Type: Policy/Action Plan)
- [Política Nacional de Inteligencia Artificial \(National Policy on Artificial Intelligence\)](#) - Foundational national policy establishing Chile's objectives for AI governance and ethical principles. (Status: Enacted/Published; Type: National Policy). External reference: [bcn.cl](#).
- [Circular Interpretativa SERNAC — Protección de los consumidores frente al uso de sistemas de inteligencia artificial en las relaciones de consumo](#) - SERNAC guidance applying consumer protection rules to businesses using AI in consumer interactions, emphasizing transparency, information duties and remedies. (Status: Enacted/Published; Type: Interpretative Circular/Consumer Guidance)
- [Oficio Circular N° 711 — Lineamientos para el uso de herramientas de inteligencia artificial en el sector público](#) - Ministry-level guidelines requiring risk assessments, documentation, oversight and transparency when public entities employ AI. (Status: In force; Type: Administrative Circular). Source: [actualidadjuridica.doe.cl](#).
- [Proyecto de Ley \(Boletín 15869-19\) — Regula los sistemas de inteligencia artificial, la robótica y tecnologías conexas](#) - Draft bill proposing a comprehensive regime for AI systems and related technologies, including obligations for developers and deployers. (Status: Under review; Type: Draft Law)
- [Proyecto de Ley \(Boletín 15935-07\) — Modifica el Código Penal para sancionar el mal uso de la inteligencia artificial](#) - Draft amendment to create criminal sanctions for malicious or negligent misuse of AI. (Status: Under review; Type: Penal Amendment)
- [Proyecto de Ley \(Boletín 16021-07\) — Modifica el Código Penal para incorporar como circunstancia agravante el uso de inteligencia artificial en la comisión de delitos](#) - Draft proposing that using AI in committing crimes be considered an aggravating circumstance. (Status: Under review; Type: Penal Amendment)
- [Proyecto de Ley \(Boletín 16112-07\) — Modifica el Código Penal en lo relativo al delito de usurpación de identidad en contexto de uso de IA](#) - Draft focused on identity usurpation facilitated by AI-generated content and deepfakes. (Status: Under review; Type: Penal Amendment)
- [Instructivo del Ministerio de Ciencia sobre uso de IA en el Estado](#) - Operational instructive from MinCiencia detailing internal procedures, evaluation criteria and oversight for government AI projects. (Status: In force; Type: Ministry Instructive)

- [Ley N° 21.719 — Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales](#) - Comprehensive data protection law establishing a dedicated supervisory authority; central to AI governance due to data-processing rules. (Status: Not yet in force; Type: Statute). External reference: [bcn.cl](#).
- [Decreto \(No. 12\) Aprueba actualización de la Política Nacional de Inteligencia Artificial](#) - Formal update to the National AI Policy that refines priorities and aligns public-sector responsibilities. (Status: Enacted/Published; Type: Executive Decree). External reference: [scribd.com](#).
- [Ley N° 21.663 — Ley Marco de Ciberseguridad](#) - Framework law on cybersecurity and critical information infrastructure that imposes incident-reporting, protection and operational requirements on vital operators. (Status: In force; Type: Statute)
- [Proyecto de Ley que regula los Sistemas de Inteligencia Artificial](#) - Government bill to regulate AI systems; reflects executive priorities for a risk-based regulatory framework. (Status: Under review; Type: Draft Law). External reference: [iapp.org](#).
- [Resolución Exenta N° 372 — Recomendaciones del Consejo para la Transparencia sobre transparencia algorítmica](#) - Non-binding recommendations for algorithmic transparency and explainability applicable to public administration. (Status: Enacted/Published; Type: Advisory Resolution)
- [Proyecto de Ley \(Boletín 17112-19\) — Establece límites al desarrollo de la inteligencia artificial en resguardo de los derechos humanos fundamentales](#) - Draft proposing substantive limits on certain AI development activities to protect human rights. (Status: Under review; Type: Draft Law)
- [Directiva N° 45 \(Dirección de Compras y Contratación Pública\) — Recomendaciones sobre el tratamiento de datos personales en procedimientos de compras públicas](#) - Guidance for procurement processes involving personal data and AI-related goods/services. (Status: Enacted/Published; Type: Procurement Directive)
- [Decreto Supremo N° 285 \(Reglamento\) — Procedimiento de calificación de Operadores de Importancia Vital en el marco de la Ley Marco de Ciberseguridad](#) - Regulatory procedures to identify and qualify operators of vital importance under the cybersecurity law. (Status: Enacted/Published; Type: Regulation)
- [Decreto N° 662/2025 — Reglamento que regula los Modelos de Prevención de Infracciones](#) - Draft regulation implementing prevention model requirements tied to the new data-protection regime (Ley 21.719). (Status: Under review; Type: Regulation)
- [Instrucción General N°1 \(Agencia Nacional de Ciberseguridad, ANCI\) — Inscripción de prestadores de servicios esenciales en la Plataforma de Reporte de Incidentes](#) - Administrative instruction for incident reporting and registration of essential service providers. (Status: In force; Type: Administrative Instruction)

Key Themes and Priorities

Common themes across Chilean instruments include: protection of fundamental rights and privacy; transparency and explainability (particularly for public-sector AI); consumer protection in commercial AI uses; cybersecurity resilience for critical infrastructure employing AI; accountability and oversight for public deployments; and promoting innovation through policies and pilot programs. Risk-based thinking and sectoral responsibility allocation appear repeatedly: instruments combine high-level principles with practical checklists, procurement criteria and incident-reporting obligations.

Governance Structure

Governance is distributed. MinCiencia leads policy coordination and state adoption guidelines. ANCI enforces cybersecurity obligations for vital operators, while SERNAC handles consumer protection issues. The Consejo para la Transparencia issues recommendations for public transparency. ChileCompra governs procurement norms. The future Agencia de Protección de Datos Personales (created by Ley 21.719) will be pivotal for oversight of data-driven AI. Effective inter-agency coordination and clear enforcement roles remain crucial implementation tasks.

Implementation Status

Several foundational policies and administrative instruments are already in force (national policy updates, action plan, Oficio Circular N° 711, MinCiencia instructive, ANCI instruction, cybersecurity law and implementing decrees). SERNAC guidance and Consejo para la Transparencia recommendations are published and being applied. The new data protection statute exists but is not yet fully in force and its implementing regulations (including Decreto N° 662/2025) are pending, which delays full operationalization of data governance for AI. Multiple AI-specific bills remain under parliamentary review and will determine the ultimate statutory contours.

Future Developments

Watch for: enactment and coming-into-force steps for Ley 21.719 and related regulations; parliamentary outcomes for the various AI and penal-code bills (which could introduce new sanctions and a statutory risk-based AI regime); and further executive guidance integrating data-protection obligations into public-sector AI procurement and deployment. International alignment and participation in multilateral AI governance initiatives will also shape Chile's regulatory trajectory.

International Context

Chile's framework is broadly consistent with international trends towards a risk-based approach, emphasis on human rights and data protection, and layered governance combining sectoral regulation with horizontal statutes. The country has designed policies to be interoperable with international norms while pursuing domestic legislative clarity. The pending bills will determine the degree to which Chile's regime mirrors more prescriptive models in other jurisdictions or emphasizes flexible, principle-driven governance.

China — AI Regulatory Landscape Summary

Overview

China's AI regulatory framework is a deliberate combination of strategic industrial guidance and legally binding controls designed to maximize the country's technological development while limiting risks to national security, public order, and personal data privacy. The framework operates across several layers: (1) high-level development plans and governance principles that set strategic priorities and responsible-AI norms; (2) foundational laws that govern cybersecurity, data security, and personal information protection; and (3) targeted administrative measures addressing algorithmic recommendation, deep synthesis, generative AI services, outbound data transfers, network data management, and AIGC labeling and identification. Operationally, the framework emphasizes platform accountability, data traceability, security assessment, and explicit content labeling.

Regulatory Instruments

- [Cybersecurity Law of the People's Republic of China](#) - Comprehensive law governing network security, critical information infrastructure protection, data localization and obligations of network operators. Status: In force; Type: National law.
- [Notice of the State Council on Issuing the Development Plan for the New Generation of Artificial Intelligence \(New Generation Artificial Intelligence Development Plan\)](#) - High-level strategic roadmap to build China into an AI innovation center; sets targets for R&D, industry ecosystems, and standards. Status: Enacted/Published; Type: Policy/State Council notice.
- [Promoting the Development of the New Generation of Artificial Intelligence Industry: Three-Year Action Plan \(2018–2020\)](#) - Tactical implementation plan focusing on capability-building, pilot projects, and ecosystem incentives. Status: Enacted/Published; Type: Action plan.
- [Governance Principles for the New Generation of Artificial Intelligence \(Developing Responsible Artificial Intelligence\)](#) - Non-binding principles recommending values such as fairness, transparency, robustness, and human oversight. Status: Enacted/Published; Type: Governance principles.
- [Guidance on the Construction of National New Generation Artificial Intelligence Open Innovation Platforms](#) - Guidance promoting shared platforms, public datasets, and testing infrastructure to support industry growth. Status: Enacted/Published; Type: Guidance.
- [Guidance on Building the National New Generation Artificial Intelligence Standardization System](#) - Framework for national technical standards, benchmarks, and certification processes. Status: Enacted/Published; Type: Standardization guidance.
- [Data Security Law of the People's Republic of China](#) - Establishes duties for data processors, data classification (including 'important data'), and safeguards tied to national security. Status: In force; Type: National law.
- [Provisions on the Administration of Algorithmic Recommendation in Internet Information Services](#) - Regulatory obligations for algorithmic platforms: registration, record-keeping, content controls, transparency and user choice mechanisms. Status: In force; Type: Administrative provisions.
- [Personal Information Protection Law of the People's Republic of China \(PIPL\)](#) - Comprehensive personal data protection regime imposing legal bases for processing, individual rights, DPIA-like obligations, and strict rules for cross-border transfers. Status: In force; Type: National law.
- [Provisions on the Administration of Deep Synthesis of Internet-based Information Services](#) - Rules for deep synthesis (deepfakes and similar technologies): consent, labeling, platform responsibilities, and safeguards

against misuse. Status: In force; Type: Administrative provisions.

- [Security Assessment Measures for Outbound Data Transfers \(Measures for the Security Assessment of Outbound Data Transfers\)](#) - Procedures and thresholds for security reviews of outbound data transfers, including those tied to model training and cloud services. Status: In force; Type: Administrative measures.
- [Interim Measures for the Administration of Generative AI Services \(Generative AI Services Management Interim Measures\)](#) - Operational duties for generative AI providers: safety testing, training-data compliance, content management, labeling, and age-appropriate protections. Status: In force; Type: Interim administrative measures.
- [Regulations on Network Data Security Management \(网络安全安全管理条例\)](#) - Further elaboration on network data duties, incident reporting, and enforcement mechanisms at the network-data layer. Status: In force; Type: Administrative regulation.
- [Measures for the Identification of AI-Generated \(Synthetic\) Content \(人工智能生成合成内容标识办法\)](#) - Detailed measures requiring explicit marking/identification of AI-generated content (AIGC) and related obligations for providers. Status: In force; Type: Administrative measures.

Key Themes and Priorities

Several cross-cutting themes recur across these instruments: (1) data governance and sovereignty: rigorous classification, protection, and review of cross-border transfers; (2) platform accountability and algorithmic governance: registration, transparency, opt-out and audit obligations; (3) content integrity and social stability: labeling of synthetic content and requirements to prevent disinformation and unlawful outputs; (4) individual rights and privacy under PIPL: lawful basis, consent, purpose limitation, and data-subject rights; (5) standardization and industrial policy: promoting domestic infrastructure, benchmarks, and certification to accelerate safe deployment; and (6) national security: security assessment and powers to restrict activities that pose risks to state security.

Governance Structure

Multiple central bodies lead and implement the framework. The State Council provides high-level coordination and policy direction. The Cyberspace Administration of China (CAC) is the primary regulator for internet information services, algorithms, and content-related measures. The Ministry of Industry and Information Technology (MIIT) and the National Development and Reform Commission (NDRC) play key roles in industrial policy, standards, and platform governance. Other agencies involved include the Ministry of Public Security (for criminal enforcement), the Ministry of Science and Technology (policy and R&D), standardization bodies (for technical standards), and provincial regulators who implement and inspect compliance locally.

Implementation Status

Most foundational laws (Cybersecurity Law, Data Security Law, PIPL) are in force and form the legal backbone. Administrative measures targeting algorithms, deep synthesis, data export review processes, generative AI, and AIGC labeling have been promulgated and are operational. Enforcement has become more active: regulatory reviews, publicized enforcement actions against major platforms, mandatory security assessments for certain cross-border transfers, and administrative penalties have been used to compel compliance. Private companies and foreign firms face a combination of compliance burdens (data governance, documentation, model testing, labeling) and commercial incentives to localize or partner with domestic infrastructure providers.

Future Developments

Short- and medium-term developments are likely to include more sector-specific standards (finance, healthcare, critical infrastructure), expanded certification and audit regimes for high-risk models, clearer operational rules for

cross-border R&D collaboration, and further integration of AI standards into procurement and public-sector use. Expect continued policy support for domestic AI champions alongside tightening operational controls in areas intersecting with national security and public discourse.

International Context

China's approach contrasts with the EU's risk-based regulation and the U.S.'s sectoral, market-oriented tendencies. However, there is convergence on topics such as robustness, testing, and transparency at the technical level. China actively pursues international standardization and technical cooperation while maintaining distinct priorities around data sovereignty and content governance. Stakeholders engaging with China should plan for bilateral regulatory compliance strategies, active regulator engagement, and alignment with both domestic standards and relevant international norms.

Official central portals and regulator websites for reference include the State Council at <https://www.gov.cn>, the Cyberspace Administration of China at <https://www.cac.gov.cn>, the Ministry of Industry and Information Technology at <https://www.miit.gov.cn>, and the National Development and Reform Commission at <https://www.ndrc.gov.cn>. These sources publish laws, administrative measures, guidelines and implementation notices.

Colombia — AI Regulatory Landscape Summary

Overview

Colombia's AI regulatory framework as of November 22, 2025 combines national policy instruments, ministerial roadmaps and a suite of legislative proposals with varying fates. The state has chosen to lead with policy (CONPES 4144; Estrategia Nacional Digital 2023-2026; MinCiencias Hoja de Ruta) that define priorities, governance principles and implementation pathways. At the same time, Congress and the executive have advanced bills that attempt to establish binding duties — from a general statute to sectoral and procedural rules — reflecting a period of active legislative experimentation and public debate.

Regulatory Instruments

- [Proyecto 91/23: Mediante la cual se establece el deber de información para el uso responsable de la Inteligencia Artificial \(Duty of information for responsible AI\)](#) - Brief description: Sets an obligation of notice and information to individuals affected by automated decision-making and AI systems. Status & type: Ended (legislative proposal focused on transparency obligations).
- [Proyecto 130/23: Armonización de la inteligencia artificial con el derecho al trabajo \(AI and labor-rights harmonization\)](#) - Brief description: Seeks to align AI deployment with labor protections, collective bargaining and anti-discrimination in employment contexts. Status & type: Ended (labor-protection focused bill).
- [Por medio de la cual se define y regula la inteligencia artificial \(Proyecto 200/23\)](#) - Brief description: Early effort to provide a general-definition and baseline regulatory structure for AI, including risk categorization. Status & type: Ended (general AI law proposal).
- [Estrategia Nacional Digital 2023-2026 \(National Digital Strategy 2023-2026\)](#) - Brief description: Executive strategy establishing priorities for digital transformation, skills, infrastructure and responsible AI adoption across sectors. Status & type: Enacted/Published (national strategy document).
- [Hoja de Ruta para la adopción ética y sostenible de la Inteligencia Artificial \(MinCiencias\)](#) - Brief description: Roadmap from the Ministry of Science articulating ethical principles, capacity building, research priorities and pilot programs to guide safe AI adoption. Status & type: Enacted/Published (ministerial roadmap).
- [Proyecto 255/24: Lineamientos de uso de IA para la disminución de siniestros viales](#) - Brief description: Sectoral guidelines and possible obligations for AI systems aimed at reducing traffic accidents, including safety requirements and data-sharing protocols. Status & type: Under review (sectoral regulation proposal).
- [Proyecto 05/24: Ley de inteligencia artificial ética y sostenible para el bienestar social](#) - Brief description: Broad legislative proposal emphasizing ethical use, sustainability and social welfare objectives for AI systems. Status & type: Ended (general AI bill focused on ethics and social welfare).
- [Proyecto de Ley Estatutaria No.154 de 2024: Por la cual se define y regula la Inteligencia Artificial](#) - Brief description: Statutory bill aiming to create binding legal definitions and a comprehensive regulatory structure for AI, with an elevated legal status as an estatutaria if enacted. Status & type: Under review (statutory bill).
- [Proyecto 417/25: Regula e implementa el uso de IA en la gestión de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias \(PQRSD\) en entidades públicas](#) - Brief description: Proposal to regulate AI deployment in public administrative complaint-handling channels, emphasizing transparency, audit trails and appeal rights. Status & type: Proposed (public-administration/operational bill).
- [Política Nacional de Inteligencia Artificial \(CONPES 4144 - National Policy for Artificial Intelligence\)](#) - Brief description: National policy document setting strategic objectives, institutional roles and steps for coordinated

AI governance and implementation. Status & type: Enacted/Published (CONPES policy).

- [Por medio de la cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético y responsable \(Government bill, Senate 442/25\)](#) - Brief description: Government-sponsored bill addressing ethical, transparency and accountability measures for AI; included legislative debate and was marked as Ended in this dataset. Status & type: Ended (government bill).

Key Themes and Priorities

Several cross-cutting themes run through Colombia's instruments: (1) Transparency and information duties (notice, documentation and rights to explanation); (2) risk-based approaches that prioritize safety for high-impact applications (e.g., mobility, public administration); (3) protection of fundamental rights, including non-discrimination and privacy; (4) labor protections and the impact of AI on employment; (5) capacity building, public procurement, and R&D promotion to ensure competitive and responsible adoption; and (6) sectoral tailoring—illustrated by road-safety and PQRSD proposals that specify operational controls for public-interest use cases.

Governance Structure

Leadership and coordination are distributed. MinCiencias drives research, ethics guidance and the Hoja de Ruta. The Departamento Nacional de Planeación (DNP) coordinates national policy through CONPES 4144. MinTIC and sectoral ministries (transport, labor, justice, health) are responsible for operationalizing rules in their domains. Enforcement of rights linked to data protection and consumer protection is overseen by the Superintendencia de Industria y Comercio and other supervisory bodies; sectoral regulators will play enforcement roles where sectoral statutes are adopted. Legislative oversight remains with the Congreso de la República when statutory instruments are proposed.

Implementation Status

Published instruments (CONPES 4144; Estrategia Nacional Digital 2023-2026; Hoja de Ruta MinCiencias) provide an active policy framework and implementation roadmap with pilot programs, coordination mechanisms and capacity-building lines. Multiple legislative proposals indicate sustained momentum but also political negotiation: several bills are listed as Ended in the dataset (showing that not all proposals reached enactment), while other significant statutory efforts are still under review. Administrative guidance currently carries more immediate compliance force than the draft statutes that have not been enacted.

Future Developments

Near-term developments to watch include the progress of Proyecto 255/24 (road-safety) and Proyecto Estatutaria No.154 de 2024 (statutory attempt), possible new CONPES implementation actions, and sectoral regulations or technical standards produced by MinTIC, MinCiencias and sectoral regulators. Private-sector actors and public entities should monitor regulations affecting procurement, public-administration deployments (PQRSD) and labor impacts.

International Context

Colombia's policy instruments explicitly aim to align with international frameworks and best practices to promote interoperability and investment while upholding rights. The hybrid policy-plus-legislation path mirrors approaches in other jurisdictions that combine national strategies, sectoral guidance and selective statutory protections rather than a single monolithic statute immediately replacing all sectoral rules.

Sources & further reading: [government AI portal](#), [official sources](#).

Costa Rica — AI Regulatory Landscape Summary

Overview

Costa Rica has emerged as a pioneer in AI governance in Central America and the Caribbean, becoming the first country in the region to adopt a comprehensive National Artificial Intelligence Strategy (ENIA 2024-2027). The country's regulatory approach combines strategic policy frameworks with pending legislation to create an ecosystem that promotes responsible AI development while protecting fundamental rights. The [Ministry of Science, Innovation, Technology and Telecommunications \(MICITT\)](#) leads AI policy coordination, with the [Legislative Assembly](#) advancing comprehensive AI legislation. Costa Rica's framework reflects international best practices while adapting to national context, positioning the country as a regional model for balanced AI governance.

Regulatory Instruments

- [National Artificial Intelligence Strategy \(ENIA\) 2024-2027](#) - Comprehensive strategic framework launched in October 2024, establishing Costa Rica's vision for ethical, safe, and responsible AI development with emphasis on bias auditing, human oversight, and protection of fundamental rights.
- [Artificial Intelligence Regulation Bill \(Legislative Assembly\)](#) - Draft legislation introduced in May 2023 proposing establishment of a regulatory authority for AI oversight, with requirements for accountability, explainability, and bias prevention. Notable for being drafted with ChatGPT-4 assistance.

Key Themes and Priorities

- **Ethical AI Development:** Strong focus on ensuring AI systems respect human dignity, fundamental rights, and democratic values throughout their lifecycle.
- **Algorithmic Transparency:** Requirements for AI systems to provide understandable explanations of decision-making processes to affected individuals.
- **Bias Prevention and Fairness:** Mandatory regular bias audits including gender assessments during development and deployment phases.
- **Human Oversight:** Mechanisms for human intervention and control over AI decisions, particularly in high-stakes contexts.
- **Innovation Promotion:** Support for AI research, development, and entrepreneurship while maintaining ethical guardrails.
- **High-Risk AI Governance:** Enhanced requirements for AI in critical sectors including healthcare, education, and justice.
- **International Alignment:** Coordination with global frameworks including EU AI Act, OECD Principles, and UNESCO ethics recommendations.

Governance Structure

- [Ministry of Science, Innovation, Technology and Telecommunications \(MICITT\)](#): Lead coordinating body for ENIA implementation and overall AI policy development.
- **Proposed Competent Authority for AI:** Independent regulatory body proposed in the AI Regulation Bill with powers for oversight, supervision, auditing, and enforcement.

- [Legislative Assembly](#): Considering AI regulation bills and providing legislative oversight of AI governance.
- **Inter-institutional Commission**: Coordinates AI policy across government ministries and agencies under ENIA framework.

Implementation Status

The National AI Strategy (ENIA) 2024-2027 is in active implementation following its October 2024 launch. Initial phases focus on establishing governance structures, developing detailed guidelines, and building institutional capacity. Pilot programs are planned for priority sectors including healthcare and education. The AI Regulation Bill remains under consideration in the Legislative Assembly since its May 2023 introduction, with committee review and public consultation ongoing. Costa Rica's comprehensive approach combines immediate strategic guidance through ENIA with longer-term legislative development. The framework continues to evolve as implementation experience informs policy refinement.

Future Developments

Costa Rica's AI governance framework will continue developing along multiple tracks. The Legislative Assembly may advance the AI Regulation Bill toward passage, potentially establishing the proposed competent authority for AI oversight. ENIA implementation will progress through its phases, with scaling of pilot initiatives and ecosystem consolidation by 2027. Additional AI-related legislation may address specific sectors or applications. Updates to align with evolving international standards are anticipated. The successor framework to ENIA will be developed as the 2027 end date approaches. Costa Rica is likely to expand regional cooperation on AI governance with Central American and Caribbean partners.

International Context

Costa Rica's AI governance approach demonstrates strong alignment with international frameworks. The [EU AI Act](#) significantly influenced both ENIA's risk-based approach and the proposed legislation's regulatory structure. The [OECD AI Principles](#) inform emphasis on accountability, transparency, and human-centered values. The [UNESCO Recommendation on the Ethics of AI](#) guides ethical provisions. Costa Rica participated in European Union technical cooperation that supported ENIA development. The country engages with regional AI governance initiatives through the Organization of American States and Latin American networks. Costa Rica's pioneering position in Central America and the Caribbean makes it a potential model for neighboring countries developing AI frameworks.

Croatia — AI Regulatory Landscape Summary

Overview

Croatia's AI policy and regulatory environment in 2025 is structured around strategic national plans, investment-oriented delivery instruments, draft AI-specific roadmaps, and an active process to transpose the EU Artificial Intelligence Act. The national approach privileges coordination across ministries, alignment with EU law and programmes, support for research and innovation through smart specialisation (S3), and operational delivery via the National Recovery and Resilience Plan (NRRP). While core strategic documents are enacted, AI-specific plans remain in draft form and the EU AI Act transposition process is underway at the national level. The aim across instruments is to enable safe, trustworthy and economically productive AI adoption while safeguarding rights and strengthening skills and infrastructure.

Regulatory Instruments

- [Strategija digitalne Hrvatske za razdoblje do 2032. godine \(Digital Croatia Strategy for the period to 2032\)](#) - National digital strategy that embeds AI as a cross-cutting enabler. Status: Enacted/Published. Type: National strategy (long-term).
- [Nacionalna razvojna strategija Republike Hrvatske do 2030. godine \(National Development Strategy of the Republic of Croatia to 2030\)](#) - High-level development strategy aligning economic, social and technological priorities; references digitalisation and innovation including AI. Status: Enacted/Published. Type: National development strategy.
- [Nacionalni plan oporavka i otpornosti 2021–2026 \(National Recovery and Resilience Plan\)](#) - Financing and implementation instrument that allocates investments for digital transformation, research infrastructure and public administration digital projects linked to AI uptake. Status: Enacted/Published. Type: Recovery & resilience implementation plan.
- [Draft: Nacionalni plan za razvoj umjetne inteligencije 2021–2025 \(Draft National Plan for the Development of Artificial Intelligence 2021–2025\)](#) - Early draft AI roadmap setting priority areas (research, skills, ethics, public-sector adoption). Status: Draft. Type: National AI plan (draft).
- [Nacionalni plan za razvoj umjetne inteligencije \(plan and action plan for period up to 2032; action plan 2026–2028\) \(National Plan for the Development of Artificial Intelligence to 2032\)](#) - Expanded long-term AI plan with a short-term action plan (2026–2028) to operationalise priorities and coordinate cross-sector activity. Status: Draft. Type: National AI plan with action plan.
- [National transposition process / working group for the EU Artificial Intelligence Act \(transposition of the EU AI Act\)](#) - National process to prepare implementing measures, identify competent authorities and align domestic legal frameworks with the EU AI Act requirements. Status: Under review. Type: Transposition / regulatory implementation process.
- [Strategija pametne specijalizacije \(S3\) – S3 2029 \(Smart Specialisation Strategy, S3 2029 revision\) — includes AI as a priority technology](#) - S3 revision that designates AI as a priority enabling technology, linking AI investments to sectoral specialisation and EU cohesion funding. Status: Enacted/Published. Type: Innovation & industrial policy strategy.

Key Themes and Priorities

Across Croatia's strategic and draft instruments several consistent priorities and themes appear: (1) strengthening digital infrastructure and data availability (secure data spaces, interoperability, research datasets); (2) boosting research, innovation and compute capacity (universities, centres of excellence, testbeds); (3) developing human capital and workforce retraining in AI-relevant skills; (4) accelerating public-sector digital transformation and introducing AI in public services with governance safeguards; (5) ensuring fundamental rights protection, privacy and non-discrimination when AI is designed and deployed; (6) promoting business adoption through targeted support under S3 and NRRP; and (7) aligning national rules with EU-level regulation (notably the EU AI Act) and international standards.

Governance Structure

Implementation is organised across ministries and national bodies. Ministries typically involved include those responsible for digital transformation, economy and sustainable development, science & education, and public administration. The National Recovery and Resilience Plan is implemented through designated programme bodies and managing authorities tied to EU funding. Data protection oversight is exercised by the national data protection authority (Agencija za zaštitu osobnih podataka - AZOP). A cross-cutting transposition working group has been established to coordinate EU AI Act implementation and to define national competent authorities for high-risk AI systems. Additional stakeholders include regional authorities, innovation agencies, academic research centres, and industry associations involved via the S3 process.

Implementation Status

As of the retrieval date, core strategic documents such as Digital Croatia 2032, the National Development Strategy 2030 and the S3 2029 revision are enacted and form the strategic backbone. The NRRP 2021–2026 is active and funds concrete projects that support AI uptake. AI-specific planning exists in draft formats: the 2021–2025 draft served as an initial sectoral roadmap and was followed by a longer-term draft plan to 2032 with an action plan for 2026–2028; these remain subject to formal adoption and will require coordination with EU transposition work. The national transposition process for the EU AI Act is underway and under review; its outputs (designation of competent authorities, national implementing legislation, enforcement arrangements, guidance documents) will define regulatory compliance obligations for the private and public sectors.

Future Developments

Priority near-term developments include: (1) formal adoption of the National Plan for the Development of Artificial Intelligence to 2032 and its 2026–2028 action plan (subject to national procedures); (2) completion of the transposition process for the EU AI Act and publication of national implementing measures and guidance; (3) deployment of NRRP-funded digital and AI projects with measurable deliverables; and (4) S3-driven programming that channels cohesion and research funding into targeted AI clusters and testbeds. Stakeholders should monitor publication of implementing decrees, guidance from the transposition working group, and calls for proposals under NRRP and S3 programmes.

International Context

Croatia positions its AI policy within the EU policy and regulatory ecosystem. Alignment with the EU AI Act is the principal international dimension of regulation. National strategies and plans are also shaped by participation in EU R&I programmes (e.g., Horizon Europe), cohesion policy instruments, and regional smart-specialisation networks. Croatia's approach therefore combines national priorities with EU regulatory obligations and funding opportunities, which together determine the shape and pace of domestic AI policy and market incentives.

For additional information, see the national portal: <https://gov.hr> and the European Commission AI policy pages: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/artificial-intelligence_en.

Cyprus — AI Regulatory Landscape Summary

Overview

This document provides a detailed, practical account of Cyprus's AI regulatory framework as it stands in 2025. Cyprus manages AI policy through a combination of strategic documents, capacity-building action plans and a formal governance framework to implement Regulation (EU) 2024/1689 at the national level. The approach is to sustain research and innovation while ensuring that safety, fundamental rights and accountability required by EU law are implementable in national practice. Key components of the current landscape are the national strategies (some concluded, some enacted or under review) and the Governance Framework for EU AI Regulation implementation.

Regulatory Instruments

- [National Artificial Intelligence Strategy: Actions for the Leverage and Development of AI in Cyprus](#) - Status: Under review. Type: National strategy / policy roadmap. Brief description: A comprehensive strategic document intended to set national priorities for AI adoption, ethics, procurement, public-sector deployment, skills and R&D alignment; currently in review to ensure alignment with the EU AI Regulation and the newly enacted R&I strategy.
- [Digital Strategy for Cyprus 2020-2025](#) - Status: Ended. Type: National digital strategy. Brief description: The 2020–2025 Digital Strategy established mid-term objectives in digital infrastructure, e-government, cybersecurity and digital inclusion. Its completed programmes and lessons inform subsequent policy cycles but the instrument itself is no longer active.
- [National Action Plan for Digital Skills 2021-2025 \(e-skills Action Plan\)](#) - Status: Ended. Type: Action plan (skills development). Brief description: A targeted plan to raise workforce digital skills and support retraining/upskilling initiatives to accompany digital transformation in the public and private sectors; many of its initiatives are being mainstreamed into ongoing R&I and education policies.
- [National Strategy for Research and Innovation 2024-2026](#) - Status: Enacted/Published. Type: Strategy / programme for R&I. Brief description: Enacted in 2024, this strategy sets immediate priorities for research funding, innovation clusters, university–industry collaboration and AI-related research themes for 2024–2026, and functions as the primary vehicle for steering public R&D investment and capacity-building.
- [Governance Framework for the Implementation of Regulation \(EU\) 2024/1689 on Artificial Intelligence in Cyprus](#) - Status: Enacted/Published. Type: Governance framework / national implementation instrument. Brief description: The formal instrument that defines roles, competencies, enforcement procedures and coordination mechanisms necessary for implementing the EU AI Regulation in Cyprus, including the designation of competent authorities, reporting lines and modalities for cross-border cooperation.

Key Themes and Priorities

Across instruments, common themes include: (1) workforce development and digital skills to enable adoption and mitigate impacts on employment; (2) bolstering research, innovation and university–industry linkages in AI and adjacent fields; (3) modernising public services through data-driven applications while safeguarding privacy and rights; (4) aligning national governance with EU regulation and standards; and (5) fostering international cooperation, notably with EU institutions.

Governance Structure

The Governance Framework provides the legal and organisational basis for domestic enforcement of Regulation (EU) 2024/1689. Implementation is coordinated across ministries responsible for digital policy and research & innovation, national research funding bodies, sectoral regulators and the national data protection authority. The framework describes how national competent authorities will supervise compliance, how market surveillance will be conducted, and how Cyprus will cooperate with the EU AI Board and other Member States.

Implementation Status

Practically, the Governance Framework is the operative regulatory instrument for AI compliance: it sets the procedures for risk classification, the duties of providers and deployers, conformity assessment procedures and incident reporting aligned with EU obligations. The Digital Strategy 2020–2025 and the e-skills action plan have reached their scheduled end and their remaining actions have been prioritised for absorption into the Research & Innovation Strategy and the forthcoming National AI Strategy. The Research & Innovation Strategy 2024–2026 is already in force and provides funding priorities that feed into national AI research and pilot programmes.

Future Developments

Key near-term developments to watch include the finalisation and publication of the National Artificial Intelligence Strategy (the document is currently under review) and the issuance of concrete implementing guidance and technical specifications by the national competent authorities designated under the Governance Framework. Further steps will include operationalising registries, staffing and resourcing supervisory bodies, publishing sectoral guidance for regulated industries, and rolling out targeted funding calls under the R&I strategy for AI projects.

International Context

Cyprus's AI policy is explicitly designed to operate within the EU's regulatory architecture; the Governance Framework institutionalises that alignment with Regulation (EU) 2024/1689. The national research and skills instruments aim to leverage EU programmes and to align domestic priorities with EU-level initiatives on trustworthy AI, standards and cross-border cooperation. For reference and liaison with EU-level material see the European Union legal resources and the national government portal such as [Cyprus Government Portal](#) and broader EU legal portals (for texts of Regulation (EU) 2024/1689, see [EUR-Lex](#)).

For implementers and stakeholders, the practical recommendation is to: (1) monitor the publication of the final National AI Strategy and subsequent secondary guidance from national competent authorities; (2) map existing or planned AI systems against the EU risk-based classification as operationalised by the Governance Framework; (3) ensure documentation, conformity procedures and data governance practices are consistent with the national framework; and (4) pursue funding and collaboration opportunities under the National Strategy for Research and Innovation 2024–2026.

Sources and primary references are the enactments and strategy documents listed in the Regulatory Instruments section and the national government portals and ministry publications linked above. Stakeholders should consult the official notices, legal texts and designated authorities' guidance for operational details and authoritative instructions.

Czech Republic — AI Regulatory Landscape Summary

Overview

The Czech Republic's AI regulatory landscape is a layered mix of national strategy, implementation planning, sectoral legislation, EU-level regulation and cross-government coordination mechanisms. This structure is anchored by two generations of national strategy documents (the original 2019 strategy and the more recent National Artificial Intelligence Strategy 2030), an action plan for 2025, a draft national Adaptation Act to operationalize the EU Artificial Intelligence Act domestically, an updated Act on Cybersecurity (No. 264/2025 Sb.) that addresses technical and incident-response risks for critical ICT and AI-enabled systems, and a governmental *Committee for Artificial Intelligence* (Výbor pro umělou inteligenci) within the Ministry of Industry and Trade (MPO) that coordinates policy implementation.

Regulatory Instruments

- [National Artificial Intelligence Strategy of the Czech Republic \(2019\)](#) - The first national roadmap for AI: strategic priorities for research, human capital, ethics and early public-sector piloting. Status: Changed (superseded in part but remains historically important). Type: Strategy / policy document.
- [National Artificial Intelligence Strategy of the Czech Republic 2030](#) - The medium-term strategy updating national priorities through 2030, emphasizing competitiveness, data infrastructure, public administration AI adoption, skills and ethical safeguards. Status: Enacted/Published. Type: Strategy / national policy framework.
- [Action Plan of the National Artificial Intelligence Strategy 2030 \(NAIS\) for 2025 \(Implementační plán programu Digitální Česko / Akční plán NAIS 2025\)](#) - Implementation-oriented plan that sets concrete projects, timelines, budget lines and responsible ministries/agencies for 2025. Status: Enacted/Published. Type: Action/implementation plan.
- [Draft Adaptation Act to Implement the EU Artificial Intelligence Act \(Adaptační návrh zákona o umělé inteligenci\)](#) — draft national AI law - A draft national law intended to provide procedural and institutional arrangements required by the EU AI Act (designation of competent authorities, sanctions framework, market surveillance rules and national procedural details). Status: Draft. Type: Draft implementing legislation.
- [Act on Cybersecurity \(Zákon o kybernetické bezpečnosti\), No. 264/2025 Sb.](#) - National cybersecurity law that imposes obligations on operators of essential services, digital service providers and maintains incident-reporting, risk management and technical-security requirements. Status: In force. Type: Sectoral statute (cybersecurity).
- [European Union Regulation on Artificial Intelligence \(AI Act\) — as applicable in the Czech Republic](#) - The EU-wide regulation establishing a risk-based legal framework for AI systems (prohibited practices, high-risk systems rules, transparency requirements, conformity assessment and market surveillance). Status: In force (EU Regulation). Type: Supranational directly-applicable regulation.
- [Committee for Artificial Intelligence \(Výbor pro umělou inteligenci\) — governmental coordinating body \(MPO\)](#) - Cross-ministerial coordination body hosted by the Ministry of Industry and Trade responsible for policy coordination, monitoring NAIS implementation and stakeholder engagement. Status: In force. Type: Government committee / coordination mechanism.

Key Themes and Priorities

Across documents, common themes include: (1) alignment with the EU risk-based approach (prohibition of certain AI uses and strict requirements for high-risk systems); (2) promotion of AI research, innovation and industrial competitiveness; (3) investment in data infrastructure, public-sector pilots and skills development; (4) cybersecurity, resilience and incident preparedness for AI-driven systems; (5) ethical safeguards and human-centric AI principles; and (6) institutional coordination so that ministries, regulators and market surveillance mechanisms implement EU rules consistently. NAIS 2030 and the 2025 Action Plan emphasize practical pilots, capacity building, and measurable outputs, while the Cybersecurity Act addresses technical resilience obligations that interact with AI safety requirements.

Governance Structure

Governance centers on the Ministry of Industry and Trade (MPO) through the Committee for Artificial Intelligence, which coordinates the cross-government response and oversees NAIS 2030 implementation. The Draft Adaptation Act is expected to set out national competent authorities and enforcement roles required by the EU AI Act; until it is adopted, responsibilities are being coordinated politically through the Committee and relevant ministries (industry, interior, justice, health, labour, digital agenda). The Cybersecurity Act designates national cybersecurity authorities and incident-reporting mechanisms that apply to critical AI systems overlapping with essential services.

Implementation Status

As of 2025: the EU AI Act functions as the binding legal baseline for AI systems in the Czech Republic; the National AI Strategy 2030 and the NAIS Action Plan 2025 are published and being operationalized; the Cybersecurity Act No. 264/2025 Sb. is in force and applied to ICT and AI systems where statutory thresholds apply; and the Adaptation Act to implement the EU AI Act remains in draft and must be enacted to finalize domestic administrative, sanctioning and procedural details. Practical implementation activities include funding calls, public-sector pilots, preparatory guidance for companies on conformity paths and initial coordination for market surveillance.

Future Developments

Key near-term developments to watch include: parliamentary or governmental adoption of the Draft Adaptation Act (which will determine national enforcement structures and sanctions), publication of implementing guidance and technical standards to operationalize EU conformity requirements, continued funding and pilot projects under NAIS 2030 and the 2025 Action Plan, and regulatory coordination between the national cybersecurity authority and designated AI supervisory bodies. Continued alignment with EU-level guidance, standardisation bodies and cross-border enforcement cooperation is expected.

International Context

The Czech Republic's AI regulatory regime is explicitly designed to align with EU law and the EU AI Act in particular, while its national strategies emphasize competitiveness and collaboration within the EU single market. The government participates in EU-level standardization and regulatory dialogues and seeks to combine adherence to EU obligations with measures that support domestic innovation and public-sector modernization. For central EU-level materials, see the EU Regulation pages (example external resource: [European Union law portal \(EUR-Lex\)](#)) and national materials on government portals (example: [Czech government AI portal](#)).

Stakeholders should monitor the official government portal and the Ministry of Industry and Trade for updated guidance and text of the Draft Adaptation Act, and should align compliance, procurement and cybersecurity practices now to accommodate the EU AI Act and applicable national cybersecurity obligations.

Denmark — AI Regulatory Landscape Summary

Overview

Denmark's AI regulatory framework in 2025 is structured around binding EU legislation, national implementing legislation, strategic policy documents and practical guidance and testing mechanisms. The centerpiece is Regulation (EU) 2024/1689 (the EU Artificial Intelligence Act), which applies directly in Denmark and establishes a risk-based regulatory regime for AI systems. Denmark has complemented the EU framework with a national Act that contains supplementary provisions, while ministries and agencies have produced strategies, guides and operational tools that prioritize responsible innovation, public-sector transparency and alignment with data protection rules.

Regulatory Instruments

- [National Strategy for Artificial Intelligence \(National strategi for kunstig intelligens\)](#) - A strategic roadmap setting national objectives for research, skills, public-sector transformation and ethical use. Status: Enacted/Published. Type: National strategy.
- [Strategy for Denmark's Digital Growth \(Strategi for Danmarks digitale vækst\)](#) - Broad digital economic policy including measures to foster AI-enabled growth, digital skills and business adoption. Status: Enacted/Published. Type: National strategy.
- [Strategic Approach for Artificial Intelligence \(Strategisk indsats for kunstig intelligens\)](#) - A coordinated, updated governmental approach emphasizing responsible public-sector deployment, innovation ecosystems and risk management. Status: Enacted/Published. Type: Policy strategy.
- [Regulation \(EU\) 2024/1689 - Artificial Intelligence Act \(EU AI Act\) \(applies in Denmark\)](#) - The EU's primary binding legal instrument defining risk categories, obligations for providers and deployers, and cross-border enforcement mechanisms. Status: In force. Type: EU regulation (direct effect).
- [Act on Supplementary Provisions to the Regulation on Artificial Intelligence \(Lov om supplerende bestemmelser til forordningen om kunstig intelligens\)](#) - National legislation implementing Member State choices under the EU AI Act, clarifying enforcement powers, administrative measures and domestic procedures. Status: Enacted/Published. Type: National implementing Act.
- [Proposal for Parliamentary Resolution on Guidelines and Risk Assessments for the Use of Artificial Intelligence \(B 42\)](#) - Parliamentary proposal focused on formalizing risk assessment practices for public providers; recorded as ended. Status: Ended. Type: Parliamentary proposal/resolution.
- [Proposal for Parliamentary Resolution to Establish an Independent AI Supervisory Authority under the Data Protection Authority \(B 90\)](#) - Proposed creation of a dedicated supervisory body for AI under Datatilsynet; recorded as ended. Status: Ended. Type: Parliamentary proposal.
- [Proposal for Parliamentary Resolution to Ensure Transparency in Authorities' Use of Algorithms \(B 136\)](#) - Proposal seeking stronger transparency obligations for public-sector algorithmic systems; recorded as ended. Status: Ended. Type: Parliamentary proposal.
- [Proposal for Parliamentary Resolution on Better Data Security and Data Ethics \(B 149\)](#) - Parliamentary initiative highlighting data security and ethical data use; recorded as ended. Status: Ended. Type: Parliamentary proposal.
- [Datatilsynet Guidance: Public Authorities' Use of Artificial Intelligence – 'Before You Start' \(Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang\)](#) - Practical guidance for authorities on legal and

privacy considerations when planning AI projects; includes risk assessment and documentation best practices. Status: Enacted/Published. Type: Regulatory guidance by supervisory authority.

- [Digitaliseringsstyrelsen Guides for Responsible Use of Generative AI \(Guides til ansvarlig anvendelse af generativ kunstig intelligens\)](#) - Agency-level guidance addressing generative models, control measures, and recommended safeguards for public-sector and procurement contexts. Status: Enacted/Published. Type: Agency guidance.
- Regulatory Sandbox for Artificial Intelligence (Regulatorisk sandkasse for AI) – Datatilsynet & Digitaliseringsstyrelsen - A supervised testing environment that allows companies and authorities to trial AI systems with regulatory support and oversight to inform compliance and best practice. Status: Enacted/Published. Type: Operational/testing mechanism.
- [Digital Taskforce for Artificial Intelligence \(Digital Taskforce for kunstig intelligens\)](#) - Cross-government forum to coordinate AI policy, implementation and stakeholder engagement. Status: Enacted/Published. Type: Interagency coordination body.

Key Themes and Priorities

Across Denmark's regulatory instruments several recurring priorities are visible. First, harmonization with the EU AI Act and GDPR — ensuring AI systems respect privacy and fundamental rights — is core. Second, public-sector algorithmic transparency and accountability are emphasized; guidance targets documentation, impact assessment and procurement. Third, Denmark promotes responsible innovation through the regulatory sandbox and strategic support for research, startups and skills. Fourth, special attention is being given to generative AI and high-profile AI systems to address emergent harms, disinformation risks and output accountability.

Governance Structure

Operational governance relies on Datatilsynet (the Danish Data Protection Authority) for privacy and data-related oversight and Digitaliseringsstyrelsen (Agency for Digitisation) for guidance on public-sector use, procurement support and digital transformation. The supplementary national Act and the EU AI Act define the formal enforcement roles, including designation of national competent authorities and coordination mechanisms. The Digital Taskforce provides a policy coordination platform across ministries, while the regulatory sandbox serves as a joint operational tool for testing and iterative policy development.

Implementation Status

Implementation is underway: the EU AI Act is in force and applied in Denmark; the national Supplementary Act has been published to clarify Member State-level provisions. Practical measures (guidance, sandbox, taskforce) are active and being used to shape how public authorities and companies interpret obligations — especially regarding high-risk systems, procurement and generative AI. Several parliamentary proposals were considered but ended, and many of their policy aims have been absorbed into the guidance and administrative measures rather than separate statutory instruments.

Future Developments

Key next steps include formal designation of national competent authorities for enforcement of specific AI Act obligations, deeper sectoral guidance (health, welfare, security), alignment of public procurement rules with AI compliance requirements, enhanced supervisory capacity and further detailed guidance for generative AI safety and resilience. Monitoring outcomes from the regulatory sandbox will inform iterative updates to guidance and enforcement practice.

International Context

Denmark's framework aligns closely with EU law and broader international AI governance trends (notably OECD AI principles and GDPR-driven privacy protections). The national approach emphasizes using EU-level baseline obligations as the legal foundation while leveraging domestic strategies, guidance, testing facilities and interagency coordination to promote competitiveness, public trust and rights protection. For official Danish resources see the [Government AI portal](#) and additional references at [official sources](#).

Ecuador — AI Regulatory Landscape Summary

Overview

Ecuador is actively developing a comprehensive AI regulatory framework through multiple complementary instruments at various stages of implementation. The country's approach balances innovation promotion with protection of fundamental rights, personal data privacy, and ethical AI deployment. Ecuador's AI governance journey began with the Organic Law on Personal Data Protection (LOPDP) enacted in May 2021, which established GDPR-inspired privacy protections applicable to AI systems processing personal data. The regulatory landscape advanced significantly in 2024-2025 with the introduction of the Draft Organic Law for AI Regulation (comprehensive 83-article framework under parliamentary review), adoption of the Code of Ethics for AI Use by the Superintendence of Economic Competition in June 2025 (the first such ethical framework by a public institution in Latin America), and the AI and Data Protection Regulation Bill promoted by the Superintendence of Personal Data Protection in September 2025 (currently in public consultation). This multi-layered approach demonstrates Ecuador's commitment to responsible AI governance while supporting digital transformation and economic development. Key government actors include the [Ministry of Technology and Digital Innovation](#), the [Superintendence of Personal Data Protection](#), [SENESCYT](#) (research and innovation), and sector-specific regulators. Ecuador draws inspiration from international frameworks including the [EU AI Act](#), [OECD AI Principles](#), and [UNESCO AI Ethics Recommendation](#) while adapting these to local context.

Regulatory Instruments

- [Organic Law on the Protection of Personal Data \(LOPDP\)](#) (In force, May 2021) - Ecuador's foundational data protection legislation modeled on GDPR, establishing comprehensive requirements for processing personal data including by AI systems, individual rights, and oversight by the Superintendence of Personal Data Protection.
- [Draft Organic Law for the Regulation and Promotion of Artificial Intelligence](#) (Under review, introduced August 2024) - Comprehensive 83-article framework establishing risk-based AI governance, classification systems, requirements for high-risk AI, algorithmic transparency, fundamental rights protection, and innovation incentives.
- [Code of Ethics for the Use of Artificial Intelligence](#) (In force, June 2025) - Groundbreaking ethical framework adopted by the Superintendence of Economic Competition, the first such code by a public institution in Ecuador and Latin America, establishing principles for responsible governmental AI use.
- [AI and Data Protection Regulation Bill](#) (Proposed, public consultation September 2025) - Targeted legislation addressing AI-specific data protection challenges, introducing requirements for algorithmic explainability, enhanced transparency, and strengthened individual rights in AI contexts.

Key Themes and Priorities

Several themes emerge across Ecuador's AI regulatory instruments: Risk-based Approach following the EU AI Act model, with stricter requirements for high-risk applications affecting fundamental rights, health, safety, or critical infrastructure; Data Protection and Privacy as foundational concerns, with multiple instruments addressing AI's unique privacy challenges through requirements for data minimization, security, transparency, and individual rights; Algorithmic Transparency and Explainability emphasized across frameworks, requiring AI systems to provide meaningful information about decision-making processes and enabling human understanding; Fundamental Rights Protection ensuring AI deployment respects constitutional guarantees of privacy, equality,

due process, and non-discrimination; Human Oversight and Control requiring meaningful human involvement in AI-assisted processes, particularly for high-stakes decisions; Innovation and Economic Development balanced with regulation through incentives for responsible AI research, development, and deployment serving public interest; Ethical AI Deployment based on principles of fairness, accountability, transparency, and societal benefit; International Alignment seeking consistency with global best practices while addressing Ecuador's specific development priorities and institutional capacities; Multi-stakeholder Governance involving government agencies, private sector, academia, and civil society in AI policy development and oversight; and Capacity Building through education, training, research support, and infrastructure development to build national AI expertise.

Governance Structure

Ecuador's AI governance involves multiple institutions with complementary roles. The [Ministry of Technology and Digital Innovation](#) serves as the lead coordinating ministry for AI policy, expected to oversee a proposed National AI Agency under the Draft AI Law. The [Superintendency of Personal Data Protection](#) enforces the LOPDP and would gain enhanced authority for AI-specific data protection under the proposed AI Data Protection Bill, including specialized AI and Algorithmic Systems Unit. [SENESCYT](#) (Secretary of Higher Education, Science, Technology and Innovation) coordinates AI research, capacity building, and innovation support. A proposed National AI Council would provide multi-stakeholder policy guidance and coordination across government. Sector-specific regulators oversee AI applications in healthcare, finance, education, and other domains. The [Superintendence of Economic Competition](#) demonstrates leadership through its AI Ethics Code governing institutional AI use. Provincial and municipal governments engage in local AI implementation, particularly smart city initiatives. This distributed governance model emphasizes coordination while allowing sectoral specialization. Multi-stakeholder participation includes private sector through consultations and advisory roles, academia and research institutions in standards development and capacity building, civil society in monitoring and advocacy, and international organizations providing technical assistance and best practice sharing.

Implementation Status

Ecuador's AI regulatory framework is at various implementation stages. Fully operational: The Organic Law on Personal Data Protection (LOPDP) is in full effect since May 2022, with the Superintendency of Personal Data Protection conducting enforcement, and the Code of Ethics for AI Use by the Superintendence of Economic Competition operational since June 2025. Under legislative review: The Draft Organic Law for AI Regulation is under parliamentary consideration with expert roundtables completed in 2024, stakeholder input incorporated, and final passage expected in 2025-2026. In public consultation: The AI and Data Protection Regulation Bill consultation period runs through approximately November 2025, gathering input before National Assembly consideration. Under development: Implementing regulations, technical standards, certification frameworks, and AI testing sandboxes are being developed to support forthcoming legislation. Early AI deployments occur in public administration digitalization, healthcare telemedicine and diagnostics, agricultural optimization, environmental monitoring, and educational technology, often as pilot projects testing governance approaches. International engagement includes participation in Latin American AI networks, collaboration with UNESCO and OECD, engagement with European partners on AI regulation, and contribution to global AI governance discussions with developing country perspectives.

Future Developments

Ecuador's AI regulatory landscape will continue evolving in coming years. Near-term (2025-2026) expectations include passage of the Draft Organic Law for AI Regulation, enactment of the AI and Data Protection Regulation Bill following consultation, establishment of the National AI Agency and governance structures, development of implementing regulations and technical standards, and launch of AI innovation sandboxes and support programs. Medium-term (2027-2028) developments may include sector-specific AI regulations for healthcare, finance, education, and critical infrastructure; additional legislation addressing emerging AI challenges such as deepfakes and disinformation; AI professional certification and standards programs; expanded AI deployment in public

services; and strengthened international cooperation and regional alignment. Long-term (2029-2030) vision encompasses a mature AI ecosystem with comprehensive regulatory framework, Ecuador positioned as regional leader in responsible AI, robust innovation ecosystem supporting AI research and development, widespread AI deployment serving public interest and economic growth, active participation in global AI governance, and ongoing evaluation and adaptation of regulations as AI technology evolves. Anticipated regulatory focus areas include generative AI governance (large language models, synthetic media), AI in critical sectors (healthcare diagnostics, autonomous systems, financial services), AI and labor (workplace automation, worker rights, skills transition), AI environmental impacts (energy consumption, sustainability), and cross-border AI governance (data flows, liability, enforcement cooperation).

International Context

Ecuador's AI framework draws heavily from and seeks alignment with international approaches. Primary influences include the [EU AI Act](#) providing the risk-based classification model, high-risk AI categories, prohibited uses framework, and transparency and conformity assessment requirements. The [OECD AI Principles](#) contribute emphasis on inclusive growth and sustainable development, human-centered values and fairness, transparency and explainability, robustness and safety, and accountability. The [UNESCO Recommendation on AI Ethics](#) informs proportionality and precaution, cultural and value diversity, solidarity and cooperation, and environmental sustainability. The EU [GDPR](#) serves as the model for Ecuador's data protection law and AI-specific privacy requirements. Regional cooperation occurs through the [Ibero-American Data Protection Network \(RIPD\)](#), Latin American AI networks, and potential harmonization efforts with neighboring countries. Ecuador contributes developing country perspectives to global AI governance, emphasizing ethical AI governance is achievable for all resource levels, AI regulation must support development objectives, global South participation is essential in AI standard-setting, and technology transfer and capacity building are critical for equitable AI benefits. Ecuador seeks adequacy determinations from GDPR jurisdictions for international data flows, participation in AI standards development bodies, bilateral cooperation with advanced AI economies, and influence on regional Latin American AI frameworks.

Egypt — AI Regulatory Landscape Summary

Overview

Egypt has established itself as a pioneer in AI governance in Africa and the Arab world, developing a comprehensive regulatory framework that balances innovation promotion with responsible AI development. The country became the first in both the Arab region and Africa to adhere to the [OECD AI Principles](#) in 2021, signaling its commitment to internationally recognized standards. Egypt's approach operates across three complementary layers: strategic planning through the [National AI Strategy](#) (now in its second edition), ethical guidance via the [Egyptian Charter for Responsible AI](#), and emerging binding requirements through the [Draft AI Law](#) currently under development. This layered approach enables Egypt to provide clear direction while maintaining flexibility as AI technology evolves.

Regulatory Instruments

- [Egypt National Artificial Intelligence Strategy \(First Edition\)](#) - The foundational 2021 strategy that established Egypt's AI vision, creating the NCAI governance structure and four pillars: AI for Human Resources, AI for Government, AI for Development, and International Cooperation. This strategy enabled Egypt's OECD adherence and launched major capacity building initiatives.
- [Egyptian Charter for Responsible Artificial Intelligence](#) - Adopted in April 2023, this non-binding ethical framework establishes five core principles (human-centered design, transparency, justice, accountability, security) through 13 general guidelines and 16 implementation guidelines. Government AI projects must comply under MCIT supervision.
- [Egypt National Artificial Intelligence Strategy \(Second Edition 2025-2030\)](#) - Launched by President El-Sisi in January 2025, this updated strategy expands to six pillars (Governance, Technology, Data, Infrastructure, Ecosystem, Talents) and sets ambitious KPIs including \$42.7 billion annual AI value and 30,000 AI professionals by 2030.
- [Egypt Draft Artificial Intelligence Law](#) - Currently under development through participatory consultations praised by the Inter-Parliamentary Union, this law will establish binding requirements, enforcement mechanisms, and penalties to complement existing voluntary frameworks.

Key Themes and Priorities

Egypt's AI governance framework reflects several consistent priorities across all regulatory instruments:

- **Inclusive AI Development:** Ensuring AI benefits all Egyptians across economic and social dimensions, with specific attention to vulnerable and marginalized groups.
- **Capacity Building:** Major investments in AI education and skills development, including the 'Our Future is Digital' program targeting 100,000 youth and goals to increase AI professionals to 30,000.
- **Regional Leadership:** Egypt leads both the Arab AI Group and the African AI Group within the African Union, contributing to unified regional AI visions.
- **Economic Transformation:** Leveraging AI to achieve 7.7% ICT sector GDP contribution and potentially adding 7-12% to overall GDP by 2030.
- **National Arabic Language Model:** A unique initiative to develop foundational Arabic AI capabilities for translation, sentiment analysis, and sector-specific applications.

- **Ethical AI Principles:** Consistent emphasis on human-centered design, transparency, fairness, accountability, and security across all instruments.
- **International Alignment:** Implementing OECD AI Principles while adapting global frameworks to Egyptian and regional contexts.
- **Public-Private Partnership:** Engaging private sector, academia, and civil society in AI development and governance.

Governance Structure

Egypt's AI governance operates through a coordinated institutional framework:

- **National Council for Artificial Intelligence (NCAI):** The apex governance body chaired by the Minister of Communications and Information Technology. NCAI develops and oversees strategy implementation, coordinates policy across ministries, and includes representatives from government, private sector, and independent experts.
- **Ministry of Communications and Information Technology (MCIT):** The lead implementing agency responsible for coordinating AI initiatives across government, supervising government AI projects for compliance with the Charter, and providing technical expertise for policy development.
- **Center for Responsible AI (Planned):** A new institution called for in the 2025-2030 Strategy to provide specialized ethical oversight, compliance guidance, and responsible AI certification.
- **Sector-Specific Coordination:** Ministries responsible for healthcare, agriculture, education, and other sectors implement AI applications within their domains under NCAI coordination.

Implementation Status

Egypt has made significant progress in implementing its AI governance framework. Since 2021, the country has advanced nearly 50 positions in global AI readiness rankings between 2020 and 2024. The 'Our Future is Digital' program has trained tens of thousands of young Egyptians in AI and digital skills. Partnerships with UNESCO for AI readiness assessment and with international technology companies support ongoing capacity building. Government digitization initiatives under the AI4G pillar have integrated AI into various public services. The Egyptian Charter for Responsible AI has been operational since April 2023, providing ethical guidance for AI development. The second edition of the National AI Strategy, launched in January 2025, is now being implemented across its six pillars. The Draft AI Law is progressing through stakeholder consultations, with enactment expected in the coming years. Key infrastructure investments are underway, including data centers and cloud services to support AI deployment.

Future Developments

Egypt's AI regulatory landscape continues to evolve with several key developments anticipated:

- **AI Law Enactment:** The Draft AI Law is expected to be finalized and enacted, establishing binding requirements and enforcement mechanisms.
- **Center for Responsible AI:** Establishment of this new institution for ethical oversight and compliance guidance.
- **National Arabic LLM:** Development of the foundational Arabic language model with subsequent domain-specific versions for healthcare, agriculture, and legal sectors.
- **2030 KPI Achievement:** Progress toward targets including \$42.7 billion annual AI value, 30,000 AI professionals, and 250+ AI companies.
- **Regional AI Hub:** Continued efforts to position Cairo as a global center for AI collaboration and innovation.

- **Charter Updates:** Annual reviews and updates to the Egyptian Charter for Responsible AI based on stakeholder feedback and evolving AI capabilities.

International Context

Egypt's AI governance framework demonstrates strong alignment with international standards while maintaining regional relevance. As the first Arab and African country to adopt the [OECD AI Principles](#) in 2021, Egypt has implemented these principles through the Egyptian Charter for Responsible AI. The country's participatory approach to AI law development has been recognized by the [Inter-Parliamentary Union](#) as a model for inclusive governance in the Global South. Egypt leads regional AI governance efforts through the Arab AI Group, contributing to a unified Arab AI vision, and the African AI Group within the African Union, helping develop the continental AI strategy. The forthcoming AI Law is expected to draw lessons from international approaches like the EU AI Act while avoiding regulatory burdens inappropriate for Egypt's development context. Egypt serves as a bridge between global AI governance frameworks and the needs of the Middle East and Africa, adapting international standards to regional contexts while maintaining compatibility with global best practices.

Estonia — AI Regulatory Landscape Summary

Overview

Estonia's AI regulatory framework has matured from early strategic thinking into a coordinated mix of national strategy, iterative action plans, sectoral legal provisions, and implementation guidance aligned with European Union law. The 2019 expert group report set principles and priorities; the 2019–2021 national strategy established initial objectives and use cases; the Kratt action plans (2022–2023 and 2024–2026) converted strategy into operational projects; and the 2024–2030 Data and Artificial Intelligence White Paper provides a medium-term policy roadmap. Simultaneously, targeted statutory provisions in administrative law enable automated administrative acts in specific areas (notably taxation and environmental charges), and Estonia implements the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) directly as an EU regulation.

Regulatory Instruments

- [Report of Estonia's AI Expert Group \(Eesti tehisintellekti kasutuselevõtu ekspertrühma aruanne\)](#) - A foundational, evidence-based set of recommendations produced by an expert group. Status: Passed. Type: Expert report / policy recommendations.
- [Estonia's National Artificial Intelligence Strategy 2019–2021 \(Eesti riiklik tehisintellekti alane tegevuskava 2019–2021\)](#) - The first national strategy setting objectives for public-sector AI adoption, innovation incentives, and skills. Status: Ended. Type: National strategy.
- [AI Action Plan \(Kratt\) 2022–2023 \(Tehisintellekti tegevuskava 2022–2023\)](#) - Implementation plan that funded pilots and guided procurement for government AI projects. Status: Ended. Type: Action plan / implementation programme.
- [Data and Artificial Intelligence White Paper 2024–2030 \(Andmete ja tehisintellekti valge raamat 2024–2030\)](#) - A comprehensive white paper establishing policy priorities on data governance, interoperability, infrastructure, and regulatory alignment through 2030. Status: Enacted/Published. Type: White paper / policy roadmap.
- [AI and Data Action Plan \(Kratt\) 2024–2026 \(Tehisintellekti tegevuskava 2024–2026\)](#) - Current national action plan operationalising the White Paper's objectives in concrete projects, with designated leads and budgets. Status: In force. Type: Action plan / implementation programme.
- [Taxation Act provision on automated administrative acts \(Maksukorralduse seadus §46² – automated administrative acts and documents\)](#) - Sectoral statutory amendment that enables and regulates automated administrative acts in taxation, including documentary and procedural safeguards. Status: In force. Type: Statutory provision / administrative law.
- [Environmental Charges Act provision on automated administrative acts \(Keskkonnatasude seadus §33⁶ – automated administrative acts and documents\)](#) - Statutory provision enabling certain automated administrative processes in environmental charges and permitting administration. Status: In force. Type: Statutory provision / administrative law.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(applies in Estonia as EU regulation\)](#) - The EU's primary legal instrument regulating AI risk categories, obligations for providers and deployers, conformity assessment, and enforcement. Status: In force. Type: EU regulation (direct effect).
- [AI Leap — national AI in education initiative \(national programme to equip students and teachers with AI tools and training\)](#) - National programme focused on AI literacy, teacher training, and classroom tools to build skills and safe use of AI in education. Status: In force. Type: National programme / education initiative.

Key Themes and Priorities

Estonia's regulations coalesce around several recurring themes: (1) public-sector digital transformation and use of AI to increase efficiency of public services while maintaining legal safeguards for citizens; (2) robust data governance and interoperability to support safe AI development and reuse of public data; (3) legal clarity for automated administrative acts ("how machines make administrative decisions") coupled with appeal and oversight rights; (4) alignment with EU-level legal standards to ensure cross-border compliance and market access; and (5) investment in human capital and literacy, exemplified by the AI Leap education initiative and workforce skilling measures in the Kratt plans. These themes reflect Estonia's twin aim of enabling rapid, public-value AI deployment while preserving trust and legal accountability.

Governance Structure

Governance is distributed across central ministries, statutory agencies, and cross-cutting coordination bodies. The Ministry of Economic Affairs and Communications has led AI policy coordination historically; the Ministry of Finance is active on public procurement and tax law adaptations; technical agencies such as the State Information System Authority (Riigi Infosüsteemide Keskus) and other e-governance actors operationalise secure platforms and standards. Sectoral regulators (finance, environment, taxation) handle domain-specific rule-making and oversight, particularly where statutory provisions enable automated administrative acts. Coordination mechanisms created under the Kratt action plans and White Paper provide project governance, monitoring and evaluation points, and assigned accountability for deliverables.

Implementation Status

By 2025, the foundational strategy period (2019–2021) and the first Kratt action plan (2022–2023) have closed and produced lessons that informed the White Paper and the live Kratt 2024–2026 plan. The White Paper (2024–2030) is the current strategic compass and is being operationalised via the Kratt action plan, budget allocations, and public procurement updates. Statutory provisions enabling automated administrative acts are in force and being implemented selectively, with government services piloting rule-based automation, decision logs, and human-review points to remain compliant with administrative law and with EU AI Act obligations. The EU AI Act introduces conformity, documentation, and risk-management requirements that now shape procurement, vendor management, and technical architecture across public deployments.

Future Developments

Key near-term priorities include: (1) strengthening procedural safeguards and redress for automated administrative acts to ensure compatibility with EU standards; (2) refining procurement standards and technical conformity pathways under the EU AI Act; (3) rolling out the White Paper's data governance measures (interoperability frameworks, secure data access models); (4) scaling education initiatives such as AI Leap to ensure workforce readiness; and (5) developing monitoring and auditing infrastructure (including registries, benchmark suites, and post-deployment surveillance) to meet ongoing compliance demands.

International Context

Estonia's approach is firmly aligned with EU-level regulation and with broader OECD and Council of Europe commitments to trustworthy AI. The country leverages its e-governance strengths to pursue an innovation-friendly model that remains attentive to human rights, transparency and accountability. Stakeholders should watch the interaction between national action plans and EU enforcement practice, as regulatory compliance will increasingly drive technical and procurement choices.

Primary sources and further reading: [Estonian government AI portal](#), [Official sources](#), and the EU act: [Regulation \(EU\) 2024/1689 \(EUR-Lex\)](#).

Ethiopia — AI Regulatory Landscape Summary

Overview

Ethiopia established its artificial intelligence governance framework in 2024, positioning itself as an emerging leader in responsible AI development in Africa. The framework centers on two key instruments: the [National Artificial Intelligence Policy](#) approved by the Council of Ministers in June 2024, and the [Personal Data Protection Proclamation No. 1321/2024](#) enacted in July 2024. The [Ethiopian Artificial Intelligence Institute \(EAI\)](#), established in 2022, leads policy implementation and AI research, while the [Ethiopian Communications Authority \(ECA\)](#) oversees data protection enforcement. Ethiopia's approach emphasizes ethical AI development, indigenous innovation, data sovereignty, and alignment with continental African initiatives.

Regulatory Instruments

- [National Artificial Intelligence Policy](#) — Ethiopia's first comprehensive AI strategy approved in June 2024, establishing the vision for AI development across healthcare, agriculture, education, water management, energy, and governance sectors. The policy prioritizes ethical AI, capacity building, and indigenous innovation.
- [Personal Data Protection Proclamation No. 1321/2024](#) — Comprehensive data protection law enacted in July 2024, granting data subjects rights to access, rectify, erase, and restrict processing of their personal data. Establishes the Ethiopian Communications Authority as the supervisory authority with 72-hour breach notification requirements.

Key Themes and Priorities

Ethiopia's AI governance framework reflects several interconnected priorities:

- **Sectoral AI Applications:** Focus on deploying AI in healthcare diagnostics, agricultural productivity, education enhancement, and public service delivery to address development challenges.
- **Ethical AI Development:** Emphasis on AI systems that respect human rights, dignity, and Ethiopian cultural values, with the EAI providing ethical guidance.
- **Data Sovereignty:** Framework for local data storage and processing, ensuring Ethiopian data governance aligned with national interests.
- **Indigenous Innovation:** Prioritizing development of AI solutions tailored to Ethiopian contexts, including local language processing for Amharic, Oromo, Tigrinya, and other Ethiopian languages.
- **Capacity Building:** Training AI researchers, developers, and practitioners through educational programs and international partnerships.
- **Continental Alignment:** Supporting African Union AI initiatives and contributing to a shared African vision for responsible AI governance.
- **Digital Identity Integration:** Coordinating AI and data protection with the Fayda national digital identity system rollout.

Governance Structure

Ethiopia's AI governance involves coordination across multiple agencies:

- [Ethiopian Artificial Intelligence Institute \(EAI\)](#) — Primary institution for AI policy implementation, research, capacity building, and certification of AI technologies. Responsible for developing regulations, authorizing AI infrastructure use, and certifying imported AI systems.
- [Ministry of Innovation and Technology](#) — Provides policy oversight, strategic direction, and coordination across government agencies on AI matters.
- [Ethiopian Communications Authority \(ECA\)](#) — Independent supervisory authority for data protection, responsible for enforcing the Personal Data Protection Proclamation, receiving complaints, and imposing penalties.
- Sector-specific ministries (Health, Agriculture, Education) coordinate AI applications within their respective domains, working with EAI for technical guidance.

Implementation Status

Ethiopia's AI governance framework is in early implementation stages following the 2024 policy approvals. The EAI continues building institutional capacity and developing implementing regulations and guidelines. The Personal Data Protection Proclamation entered into force in July 2024, with the ECA working to operationalize registration and enforcement mechanisms. Controller and processor registration is underway, with a transitional period allowing organizations to achieve compliance. Pilot AI projects are being developed in priority sectors, with the government emphasizing capacity building and awareness campaigns. The Fayda digital identity system continues its phased rollout with data protection safeguards mandated by the Proclamation.

Future Developments

Ethiopia's AI governance landscape is expected to evolve with several anticipated developments:

- **Implementing Regulations:** Development of detailed regulations operationalizing the National AI Policy and specifying sector-specific requirements
- **ECA Guidance:** Issuance of data protection guidelines, codes of conduct, and sector-specific guidance
- **AI Legislation:** Potential enactment of AI-specific laws translating policy principles into binding requirements
- **Research Infrastructure:** Establishment of AI research centers at universities and creation of innovation hubs
- **Skills Development:** Expansion of AI training programs and curricula development
- **Public-Private Partnerships:** Increased collaboration with private sector and international partners

International Context

Ethiopia's AI governance aligns with key international and continental frameworks. The National AI Policy supports the [African Union Continental AI Strategy](#) and the Africa Declaration on Artificial Intelligence. Ethiopia hosted the High-Level Policy Dialogue on AI in Addis Ababa, convening participants from over 40 African countries. The Personal Data Protection Proclamation draws from the [African Union Malabo Convention](#) and incorporates principles consistent with international standards including the [OECD AI Principles](#). While not bound by the EU AI Act or GDPR, Ethiopia's framework reflects international best practices, facilitating partnerships and supporting the African Continental Free Trade Area through trusted data governance.

Business Compliance Requirements

Organizations operating in Ethiopia should address key compliance areas:

- **EAI Engagement:** Organizations developing or deploying AI systems should engage with EAI for certification and guidance

- **Data Protection Registration:** Register as data controller or processor with the Ethiopian Communications Authority
- **Lawful Processing Basis:** Establish and document lawful basis for all personal data processing activities
- **Privacy Notices:** Provide clear information to data subjects about processing purposes and rights
- **Data Subject Rights:** Implement procedures to respond to access, rectification, and erasure requests
- **Security Measures:** Deploy appropriate technical and organizational security controls
- **Breach Response:** Establish 72-hour breach notification procedures to ECA
- **Impact Assessments:** Conduct data protection impact assessments for high-risk processing

Sector-Specific Applications

Ethiopia's framework addresses AI applications across priority sectors:

- **Healthcare:** AI for disease diagnosis, epidemic prediction, health resource optimization, and telemedicine services
- **Agriculture:** Crop yield prediction, pest detection, irrigation optimization, and market information for smallholder farmers
- **Financial Services:** AI for financial inclusion, credit scoring for unbanked populations, and mobile banking innovation
- **Education:** AI-powered learning tools, adaptive education systems, and local language educational content
- **Water and Energy:** Resource management optimization, drought prediction, and renewable energy forecasting
- **Government Services:** E-government applications enhancing public service delivery and administrative efficiency

Enforcement and Penalties

Enforcement of Ethiopia's AI governance framework operates through multiple mechanisms. The ECA has authority to investigate data protection complaints, conduct inspections, and impose penalties under the Personal Data Protection Proclamation. Penalties include administrative fines, warnings, processing bans, and potential criminal sanctions for serious violations including unauthorized data access. The EAI may prohibit non-certified AI technologies from domestic use. Data protection violations must be reported within 72 hours, with failure to comply subject to additional penalties. Appeals against regulatory decisions may be lodged through administrative and judicial channels.

Rights and Protections

Ethiopia's framework provides protections for individuals:

- **Data Access Rights:** Right to access personal data held by controllers and receive copies
- **Rectification Rights:** Right to correct inaccurate or incomplete personal data
- **Erasure Rights:** Right to deletion of personal data under specified circumstances
- **Processing Restriction:** Right to restrict processing of personal data
- **Objection Rights:** Right to object to direct marketing and automated decision-making
- **Consent Withdrawal:** Right to withdraw consent at any time

- **Complaint Mechanisms:** Right to lodge complaints with the ECA regarding data protection violations

Resources and Further Information

Key resources for understanding Ethiopia's AI governance:

- [Ministry of Innovation and Technology](#)
- [Ethiopian Communications Authority](#)
- [Ministry of Justice - Data Protection Proclamation](#)
- [Ethiopian News Agency](#)
- [Digital Policy Alert - Ethiopia Digest](#)

European Union — AI Regulatory Landscape

Summary

Overview

The European Union has implemented a layered, risk-based regulatory framework for artificial intelligence designed to protect fundamental rights, ensure safety and foster innovation in the internal market. The keystone is the [Artificial Intelligence Act \(Regulation \(EU\) 2024/1689\)](#), supplemented by liability and product-safety updates, a dedicated European Artificial Intelligence Office, binding Council decisions on international engagement, multiple Commission guidelines to clarify substantive obligations, voluntary codes for general-purpose AI, and a continuing stream of policy communications and coordinated plans that set strategic priorities and coordinate Member State actions. This framework brings together hard-law obligations, sectoral rules, guidance documents, and voluntary instruments to create a comprehensive compliance environment for developers, deployers and operators of AI systems.

Regulatory Instruments

- [AI Board Sixth Meeting - Implementation and Interoperability](#) - Meeting and implementation guidance focused on interoperability of enforcement, technical standards and coordination across Member States (Status: In force; Type: Governance/Coordination).
- [Commission Antitrust Investigation into Meta WhatsApp AI Policy](#) - Ongoing competition/consumer-protection inquiry examining possible anticompetitive or unfair-terms related to AI-driven features in WhatsApp (Status: Under review; Type: Enforcement/Investigation).
- [Information Session: Protocols for Text and Data Mining Rights under AI Act and GPAI Code of Practice](#) - Stakeholder outreach clarifying text and data mining rights and application of the AI Act and voluntary GPAI code (Status: Under review; Type: Guidance/Outreach).
- [Coordinated Plan on Artificial Intelligence \(COM\(2018\)795\)](#) - Foundational strategic plan for Member State coordination on investment, skills and R&D (Status: Enacted/Published; Type: Policy/Strategy).
- [Communication: Artificial Intelligence for Europe](#) - Early Commission communication setting objectives for a European AI ecosystem (Status: Enacted/Published; Type: Communication/Policy).
- [Ethics Guidelines for Trustworthy AI \(High-Level Expert Group on AI\)](#) - Non-binding ethical principles and assessment guidance (Status: Enacted/Published; Type: Guidance/Ethics).
- [White Paper on Artificial Intelligence: A European approach to excellence and trust](#) - Roadmap toward regulation and standards to balance innovation and risk (Status: Enacted/Published; Type: Policy/White Paper).
- [Assessment List for Trustworthy Artificial Intelligence \(ALTAI\) — self-assessment tool](#) - Voluntary self-assessment checklist to operationalise ethical guidelines (Status: Enacted/Published; Type: Tool/Guidance).
- [Communication: Fostering a European approach to Artificial Intelligence](#) - Policy update emphasizing uptake, investment and trust-building measures (Status: Enacted/Published; Type: Communication/Policy).
- [Coordinated Plan on Artificial Intelligence — 2021 review](#) - Updated Member State coordination and milestones for implementation (Status: Enacted/Published; Type: Policy/Review).
- [Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office](#) - Establishes the EAIO to support implementation, guidance and coordination of the AI Act (Status: Enacted/Published;

Type: Decision/Institutional).

- [Directive \(EU\) 2024/2853 on liability for defective products \(revising product liability to cover software and AI\)](#) - Extends product liability rules to cover software and AI-driven products to improve access to redress (Status: Enacted/Published; Type: Directive/Liability).
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act](#) - Core horizontal regulation classifying AI systems by risk with obligations for high-risk systems and prohibitions on unacceptable practices (Status: In force; Type: Regulation/Primary).
- [Council Decision \(EU\) 2024/2218 of 28 August 2024 on the signing, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law](#) - Formal EU commitment to Council of Europe AI framework on rights and democracy (Status: Enacted/Published; Type: Council Decision/International).
- [Digital Omnibus Package — Simplifying EU Digital Rules on AI, Cybersecurity, and Data](#) - Legislative package intended to streamline digital rules and reduce fragmentation (Status: Proposed; Type: Legislative Package/Proposed).
- [Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence \(AI Liability Directive\) — Commission proposal withdrawn](#) - Attempt to harmonise non-contractual civil liability for AI; withdrawn, leaving other liability instruments in force (Status: Ended; Type: Proposal/Withdrawn).
- [European Commission Guidelines regarding the definition of an 'AI system' \(clarifying Article 3\(1\) of the AI Act\)](#) - Clarification on the scope and technical boundaries of what counts as an AI system under the AI Act (Status: Enacted/Published; Type: Guidance/Interpretation).
- [European Commission Guidelines regarding prohibited AI practices \(guidance on Article 5 prohibitions\)](#) - Detailed explanation of banned practices and edge cases for enforcement (Status: Enacted/Published; Type: Guidance/Interpretation).
- [General-Purpose AI Code of Practice \(voluntary Code of Practice for GPAI providers\)](#) - Voluntary code aimed at providers of large general-purpose models to promote responsible design and governance (Status: Enacted/Published; Type: Voluntary Code/Guidance).
- [European Commission Guidelines on the scope of obligations for providers of General-Purpose AI models](#) - Clarifies obligations and expected compliance practices for GPAI providers in the EU market (Status: Enacted/Published; Type: Guidance/Clarification).
- [Template for the public summary of training content for General-Purpose AI models \(training-data transparency template\)](#) - Standardised template to improve transparency about training data and limitations of models (Status: Enacted/Published; Type: Template/Transparency Tool).

Key Themes and Priorities

Across instruments, several consistent priorities emerge: a risk-based regulatory stance that differentiates obligations according to potential harm; strong emphasis on fundamental rights protection (privacy, non-discrimination, freedom of expression); transparency and documentation requirements; accountability through governance and liability mechanisms; promotion of technical standards and interoperability to enable a single market for safe AI; and international engagement to align rules and norms. The EU mixes hard law (the AI Act, liability and product rules) with soft law (guidelines, checklists, voluntary codes) to accelerate compliance and reduce legal uncertainty for innovators.

Governance Structure

Governance is multi-layered. The European Artificial Intelligence Office (EAIO), created by Commission decision, is the central coordinating body supporting the AI Board and national competent authorities. The AI Board provides

a forum for enforcement coordination and technical rule-making. Sectoral regulators (financial supervisors, medical device authorities, data protection authorities) retain roles where sector-specific law applies. Member State authorities implement and enforce obligations at national level, reporting and cooperating via the EAIO. The Commission also issues guidance and templates to standardise compliance practices across the Union.

Implementation Status

As of the current publication, the AI Act and Directive updates on product liability are in force, with implementing guidance and templates published to assist market participants. The EAIO is operational and the AI Board has convened multiple implementation meetings (including the sixth meeting focused on interoperability). Several guidance documents clarifying definitions, prohibited practices and GPAI obligations have been published to reduce legal uncertainty. Some proposals (for example the AI Liability Directive) were withdrawn, while the Digital Omnibus Package remains proposed and may affect the regulatory perimeter if adopted.

Future Developments

Watch for implementing and delegated acts under the AI Act that will detail technical and conformity assessment requirements, additional Commission guidance clarifying borderline cases, potential alignment of the Digital Omnibus Package with existing rules, and further international cooperation (notably under the Council of Europe framework and OECD/G20 fora). Enforcement actions and market investigations will generate case law and interpretive practice that will further shape obligations, especially for GPAI providers and large platforms.

International Context

The EU's regulatory model is influential globally: its combination of binding, risk-based rules, transparency obligations, and updated liability frameworks provides a template for other jurisdictions. The EU concurrently engages in international instruments (e.g., Council of Europe and multilateral dialogues) and encourages adoption of technical standards through standardisation organisations. Providers active globally will need to align with EU-specific requirements (e.g., documentation, public training summaries and conformity pathways) while monitoring bilateral and multilateral developments.

Key external resources and repositories for primary texts and guidance include the EU law database ([EUR-Lex](#)), Commission pages on AI and digital policy ([European Commission](#)), and the Council of Europe site for international frameworks ([Council of Europe](#)).

Finland — AI Regulatory Landscape Summary

Overview

Finland's AI policy landscape is programme-driven and sectorally differentiated. Rather than a single, omnibus AI statute, Finland has relied on a sequence of national programmes, strategy documents and sectoral initiatives to set priorities, support business uptake, modernise public services and build capacity. The goal has been to create an environment where AI can be adopted widely while upholding core Finnish and EU values — human-centricity, transparency, accountability and data protection. The instruments listed below together show a lifecycle: national programmes and final reports established strategy and principles, Business Finland and related instruments focused on commercialization and company support, sectoral programmes (health, labour, public services) explored safe deployment, and municipal-level measures (the City of Helsinki Algorithm and AI Register) operationalised transparency for citizens.

Regulatory Instruments

- [Artificial Intelligence Programme \(National AI Programme\)](#) - A time-limited national programme that initiated Finland's coordinated approach to AI. Status: Ended. Type: National programme / strategic initiative. Brief description: Established national priorities around skills, research, public sector pilots and ethical principles, and produced recommendations for follow-on activity.
- [Finland's Age of Artificial Intelligence](#) - Enacted/published national strategy document setting out Finland's vision for AI adoption. Status: Enacted/Published. Type: National strategy/white paper. Brief description: High-level vision emphasizing human-centric AI, economic competitiveness, and education and skills development.
- [AI Business Programme \(Business Finland\)](#) - Time-bound business support programme run by Business Finland to accelerate commercial AI uptake. Status: Ended. Type: Innovation & business support programme. Brief description: Focused on company pilots, scaling, internationalisation and creating partnerships between industry and research organisations.
- [Work in the Age of Artificial Intelligence](#) - Strategy and guidance on labour market impacts, workplace transformation and skills. Status: Enacted/Published. Type: Policy report / sectoral strategy. Brief description: Addressed workforce planning, continuing education, social dialogue and measures to mitigate displacement while maximising job quality.
- [Leading the Way into the Age of Artificial Intelligence \(Final report of Finland's Artificial Intelligence Programme\)](#) - Final report summarising results and recommendations of the National AI Programme. Status: Enacted/Published. Type: Final programme report. Brief description: Consolidated lessons, recommended policy actions and set follow-on priorities for research, public services and business support.
- [AuroraAI \(National AI programme for human-centric public services\)](#) - National programme piloting AI-enabled, user-centric public services and service coordination. Status: Ended. Type: Public service programme / pilot. Brief description: Explored interoperable digital service architectures and how AI can assist citizens in navigating services while emphasising consent, transparency and accountability.
- [Hyteairo — Well-being and Health Sector's Artificial Intelligence and Robotics Programme](#) - Sectoral programme for AI in health and social welfare. Status: Enacted/Published. Type: Sectoral programme. Brief description: Targeted safe clinical deployment, evidence generation, interoperability and compliance with health and data protection rules.

- [City of Helsinki AI Register \(Algorithm and AI Register\)](#) - Municipal registry documenting automated systems used by the city. Status: In force. Type: Municipal governance / transparency tool. Brief description: Operational register designed to increase public transparency about where and how algorithms and AI systems are used in municipal services and decision-making.
- [Artificial Intelligence 4.0 Programme](#) - Programme focused on next-generation AI adoption, scaling and ecosystem development. Status: Enacted/Published. Type: National programme / strategic initiative. Brief description: Continued emphasis on competitiveness, scaling of solutions, and strengthening national research and skills capacity.

Key Themes and Priorities

Across these instruments several cross-cutting themes appear consistently: (1) human-centric AI and ethical principles — emphasis on trust, transparency and explicability; (2) skills and labour market adaptation — investment in reskilling and lifelong learning; (3) business and innovation support — targeted programmes to accelerate commercialisation and internationalisation; (4) safe sectoral deployment — especially in health and welfare where clinical safety, evidence and legal compliance are emphasised; (5) transparency and accountability — exemplified by municipal registries and guidance for public sector procurement; and (6) multi-stakeholder collaboration — combining ministries, research organisations, local government and industry.

Governance Structure

Governance is distributed and collaborative. National ministries set strategy and funding priorities, innovation agencies (notably Business Finland) run business support programmes, public research organisations and health sector authorities shepherd sectoral pilots, and municipalities (notably the City of Helsinki) operate experimental governance tools. Traditional regulatory and supervisory frameworks — data protection authorities, health regulators and administrative law mechanisms — remain the primary legal backstops, meaning AI-specific governance to date complements rather than replaces existing law. Key public actors commonly engaged in AI work include central ministries (economic, social, health and public administration), Business Finland for innovation policy, sectoral agencies for implementation and city administrations for local experimentation. For more information on central government portals see [valtioneuvosto.fi](#) and innovation & funding information at [Business Finland](#).

Implementation Status

The instruments can be categorised by implementation phase. Several national programmes listed as "Ended" have produced reports, recommendations and pilot results that now inform ongoing policy. Enacted/published strategies and sectoral programmes are active policy references and have led to follow-on projects in public services and health care. The City of Helsinki AI Register is operational and functions as a living transparency tool maintained by municipal authorities. Implementation challenges commonly noted across the programmes include ensuring interoperability of data systems, reconciling rapid technological change with regulatory safeguards, scaling pilots into production while retaining safety assurances, and mobilising sustained funding for skills and infrastructure.

Future Developments

Finland's short- to medium-term priorities are likely to include aligning domestic programmes with evolving EU rules and standards, expanding registries and transparency instruments, embedding trustworthy AI criteria into public procurement, and scaling health sector innovations under strict evidence and patient-safety regimes. Continued investment in skills, regional innovation hubs and international cooperation is also expected. Finland's emphasis on experimental governance (registries, pilots) will likely continue as a proving ground for larger regulatory or legislative measures.

International Context

Finland positions its AI programmes to be compatible with EU-level developments and international standards. The mix of soft law (strategies, programmes, guidance) and practical governance tools (registries, sectoral roadmaps) is well suited to adapt to EU regulatory instruments and to contribute to transnational dialogues on trustworthy AI. Stakeholders should monitor EU legislative developments and national follow-through to ensure compliance and to capture funding and collaborative opportunities. Useful portals for EU and national coordination include the Government of Finland at <https://valtioneuvosto.fi>, Business Finland at <https://www.businessfinland.fi>, the City of Helsinki at <https://www.hel.fi>, and health-sector resources at <https://thl.fi>.

France — AI Regulatory Landscape Summary

Overview

France's AI regulatory framework combines: (1) a strong, rights-based foundation centred on data protection and administrative transparency; (2) sectoral and technical decrees enabling and constraining specific identity and authentication technologies; and (3) strategic policy instruments designed to accelerate research, industrial capacity and ethical stewardship. Core legal pillars include the national adaptation of the GDPR (Law No. 2018-493) and the Loi pour une République numérique (Law No. 2016-1321). These statutes are complemented by decrees that operationalise transparency and public-data obligations for algorithmic decision-making and by targeted measures authorising and governing electronic identity services.

Regulatory Instruments

- [Law No. 2016-1321 of 7 October 2016 - Law for a Digital Republic \(Loi pour une République numérique\)](#) - Introduced transparency and open-data obligations for public administration, including initial provisions requiring documentation and explanations for algorithmic decisions affecting individuals. Status: In force. Type: National law (administrative transparency, digital rights).
- [Decree No. 2017-330 of 14 March 2017 - Rights of persons subject to individual decisions based on algorithmic processing \(Décret relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique\)](#) - Establishes rights and procedures for persons affected by automated individual decisions, including access to algorithmic documentation and administrative recourse. Status: In force. Type: Executive decree (administrative implementation).
- [Decree No. 2017-331 of 14 March 2017 - Service public for provision of reference data \(Décret relatif au service public de mise à disposition des données de référence\)](#) - Requires public bodies to publish and provide reference datasets and metadata supporting automated decisions, to enable transparency and reproducibility. Status: In force. Type: Executive decree (open data/public sector infrastructure).
- [Law No. 2018-493 of 20 June 2018 - Law on the Protection of Personal Data \(adaptation of the French Data Protection Act to the GDPR\)](#) - National adaptation and implementation of the EU GDPR; establishes CNIL enforcement powers, data-subject rights, and rules that apply to AI systems processing personal data (including special categories such as biometric data). Status: In force. Type: National law (data protection).
- [Villani Report \("Donner du sens à l'intelligence artificielle"\) - Mission report and recommendations on AI \(Cédric Villani\), March 2018](#) - Strategic policy report recommending investments, ethical frameworks, data access measures, and institutional arrangements to promote trustworthy AI in France. Status: Enacted/Published (policy guidance). Type: Strategy/mission report.
- Decree No. 2019-452 of 13 May 2019 - Authorising creation of the Alicem mobile certified online authentication system (Décret autorisant la création d'un moyen d'identification électronique ALICEM) - Authorised a mobile e-identity authentication mechanism; programme subsequently ended after legal and privacy review. Status: Ended. Type: Executive decree (electronic ID experiment/authorisation).
- [France 2030 investment plan \(includes dedicated AI funding and programmes\) - national industrial and innovation strategy \(announced 12 October 2021\)](#) - Major national investment and industrial policy package with dedicated funding lines to support AI research, industrial adoption, data infrastructure and sovereign capabilities. Status: Enacted/Published (strategy and funding). Type: National investment strategy/programme.
- [Decree No. 2022-676 of 26 April 2022 - Authorising creation of the 'Service de garantie de l'identité numérique' \(SGIN\) electronic identification service \(Décret autorisant la création d'un moyen d'identification\)](#)

[électronique SGIN](#)) - Authorises a state-guaranteed digital identity service intended to provide secure, certified identification for online services; frames governance and technical assurance. Status: In force. Type: Executive decree (electronic ID service).

- [Proposition de loi relative à la reconnaissance biométrique dans l'espace public \(Proposal / parliamentary bill on biometric recognition in public space\) - report deposited 31 May 2023](#) - Parliamentary proposal and accompanying report focusing on limits, safeguards and authorisation regimes for biometric recognition in public spaces, reflecting political and legal debate. Status: Proposed. Type: Parliamentary bill / proposal.

Key Themes and Priorities

Across instruments, recurring themes are: (1) data protection and privacy (GDPR-aligned rules and CNIL oversight); (2) transparency, documentation and contestability of administrative algorithmic decisions; (3) secure, certified digital identity as infrastructure for trustworthy services (SGIN, ALICEM experiment); (4) strategic industrial policy to build sovereign AI capabilities (Villani recommendations, France 2030 funding); and (5) cautious treatment of biometric surveillance with political and legal scrutiny.

Governance Structure

Primary regulatory and governance actors include the CNIL (<https://www.cnil.fr>) as the principal data protection authority and enforcer; ministries that drive strategy and procurement (notably the Ministry for the Economy and Finance and the Ministry of Research and Innovation); ANSSI for cybersecurity considerations (<https://www.ssi.gouv.fr>); and inter-ministerial coordination led by the Prime Minister's office for national programmes such as France 2030 (<https://www.gouvernement.fr/en/france-2030>). The Villani mission influenced institutional design and attention to ethics and research priorities; CNIL issues operational guidance and decisions that materially affect both public and private deployment of AI systems.

Implementation Status

Most listed instruments are in force: the Loi pour une République numérique (2016), the two 2017 decrees on algorithmic rights and public reference data, the 2018 data-protection adaptation to the GDPR, the 2022 SGIN decree, and France 2030 programmes. ALICEM (2019) is recorded as ended, illustrating how privacy and legal review can terminate or reframe initiatives. The 2023 parliamentary proposal on biometric recognition is a current policy negotiation point; because it is a parliamentary proposal its provisions are not yet binding but illustrate legislative attention to live biometric use-cases. On the ground, CNIL guidance, sectoral approvals for identity services, and procurement rules govern day-to-day compliance and rollout of AI-enabled services in public administration.

Future Developments

France's domestic framework will continue to evolve alongside EU-level regulation (notably implementation and interaction with the European AI Act and evolving GDPR jurisprudence). Anticipated developments include additional sectoral guidance from CNIL, legislative activity on biometric surveillance, regulatory clarification for identity services and certifications, and continued allocation of France 2030 funds to accelerate national AI capabilities. Stakeholders should monitor CNIL publications, parliamentary proceedings on biometric recognition, and implementation rules for state identity services.

International Context

France aligns its national approach with EU frameworks (GDPR and the European approach to AI: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>) while pursuing national industrial

sovereignty objectives (France 2030). The country engages in international standardisation and ethics fora and often advocates for a balance between rights protection and competitive innovation.

For implementation and compliance, practitioners should prioritise GDPR compliance (personal data governance, lawful bases, DPIAs), adherence to CNIL guidance on algorithmic transparency and biometric data, documentation practices for public-sector automated decisions required by the 2017 decrees, and close monitoring of parliamentary initiatives that could impose additional constraints on biometric use in public spaces. Official portals and supervisory guidance (e.g. <https://www.cnil.fr>, national government sites) are primary sources for up-to-date procedures, formal notices and decisions.

Germany — AI Regulatory Landscape Summary

Overview

Germany's national AI landscape is characterised by a layered combination of strategic steering, operational action plans, workplace-focused observatories and labs, technical standardisation, and legal measures — all implemented in the broader context of the European Union's regulatory framework. The Federal Government's original Strategy for Artificial Intelligence ("Strategie Künstliche Intelligenz" / "AI Made in Germany") established policy objectives to foster excellence in research, increase technology transfer to industry, strengthen data infrastructure and public-sector use, and promote ethical and legal frameworks for trustworthy AI. The 2020 update ("Fortschreibung der KI-Strategie") sharpened priorities and resource allocation, while the 2023 BMBF Action Plan provides concrete funding and programme architecture for research, talent, regional ecosystems and application-oriented development.

Regulatory Instruments

- [Strategy for Artificial Intelligence of the Federal Government \('Strategie Künstliche Intelligenz' / 'AI Made in Germany'\)](#) - National strategy document setting vision, objectives and initial measures for research, innovation and governance. Status: Enacted/Published. Type: Strategic policy framework.
- [National AI Strategy — Update \('Fortschreibung der KI-Strategie' / National AI Strategy: Update 2020\)](#) - Update refining objectives, funding priorities and implementation pathways; emphasises faster technology transfer and societal impact assessment. Status: Enacted/Published. Type: Strategic update.
- [BMBF AI Action Plan 2023 \('Aktionsplan Künstliche Intelligenz 2023'\)](#) - Operational action plan from the Federal Ministry of Education and Research detailing funding programmes, research clusters, skills and international cooperation measures. Status: Enacted/Published. Type: Implementation/action plan.
- [AI Observatory for Work and Society \(KI-Observatorium, BMAS\)](#) - Ongoing monitoring and research platform run by the Federal Ministry of Labour and Social Affairs to observe AI use in workplaces, collect data on effects for employment, and recommend policy responses. Status: In force. Type: Observational/research body.
- [KI-Studios \(BMAS project: participatory workplace AI labs / 'KI-Studios – KI-Erlebniswerkstätten'\)](#) - Practical, participatory labs where workers, employers and technologists co-design AI applications and governance patterns; supports evidence-based workplace guidance. Status: In force. Type: Pilot/participatory programme.
- [Plattform Lernende Systeme \(Platform for Learning Systems\) — national multi-stakeholder platform](#) - Cross-sector platform convening industry, academia, government and social partners for guidance, position papers and best practices. Status: In force. Type: Multi-stakeholder advisory platform.
- [German AI Standardisation Roadmap \(DIN/DKE\) — Roadmap for AI standardisation and conformity](#) - Roadmap produced by national standards bodies (DIN/DKE) to coordinate technical standards, testability and conformity assessment. Status: Enacted/Published. Type: Standardisation roadmap.
- [Data Strategy of the Federal Government \('Datenstrategie der Bundesregierung'\)](#) - Framework to improve public-sector data availability, promote secure data-sharing, and align data governance to facilitate trustworthy AI. Status: Enacted/Published. Type: National data policy.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(applies in Germany as EU regulation\)](#) - EU-level binding regulation introducing a risk-based legal regime for AI systems with obligations for high-risk systems, transparency, conformity assessment and market surveillance. Status: Enacted/Published (EU regulation; directly applicable). Type: Supranational regulation.

- [Federal Council draft: Criminal-law protection of personality rights against Deepfakes \(Drucksache 222/24 - proposal for new §201b StGB\)](#) - Bundesrat draft proposing a new criminal offence to protect personality rights from manipulated deepfake content; seeks to address reputational harms and automated misuse. Status: Proposed. Type: Legislative proposal (criminal law).
- [BMJ Eckpunkte for a Law against Digital Violence \('Eckpunkte für ein Gesetz gegen digitale Gewalt'\)](#) - Key points issued by the Federal Ministry of Justice proposing civil/criminal measures and procedural tools to combat targeted online abuse (including technology-facilitated harms). Status: Draft/Policy proposal. Type: Policy framework / draft legislation guidance.

Key Themes and Priorities

Common themes across Germany's instruments are: (1) a strong emphasis on trustworthy AI — ethics, safety, transparency and human oversight; (2) worker-centred governance — dedicated observatories and participatory labs to understand and manage workplace impacts; (3) operationalisation through funding and regional innovation ecosystems to translate research into deployment; (4) technical harmonisation and conformity — proactive standardisation work to support certification and market trust; and (5) protective legal measures for personal rights and online safety that address harms amplified by automated tools (deepfakes, digital violence).

Governance Structure

Implementation is distributed across federal ministries and independent bodies. The BMBF leads research, funding and innovation programmes; BMAS leads workplace-focused monitoring and participatory pilots; BMJ steers legal-policy development on criminal and civil protections; DIN/DKE coordinates national standardisation; Plattform Lernende Systeme convenes stakeholders for guidance; and the EU institutional framework (European Commission, designated national supervisory authorities and market surveillance bodies) imposes regulatory obligations via the EU AI Act. Cross-ministerial coordination mechanisms and publicly funded research consortia support policy coherence.

Implementation Status

Strategic documents and the BMBF Action Plan are published and active; BMBF funding instruments and research clusters have been rolled out. The KI-Observatorium is operational and producing monitoring outputs to inform labour and social policy; KI-Studios operate as pilots with case studies informing guidance. DIN/DKE's roadmap has advanced prioritisation of standards and alignment with international standard-setting. The EU AI Act is applicable across Germany and imposes compliance obligations on providers and deployers of regulated AI systems. Legislative measures on deepfakes and digital violence are under parliamentary and Bundesrat consideration and have not yet produced new criminal statutes at the federal level (status: proposed/draft as indicated).

Future Developments

Key near-term developments to monitor include final decisions on the Bundesrat deepfake proposal and any resulting amendments to the Criminal Code; progress from BMJ on formal draft legislation addressing digital violence; continuing standardisation and conformity assessment instruments (technical specifications, testing frameworks and certification schemes) following the DIN/DKE roadmap; and national implementation guidance to operationalise EU AI Act obligations, including designation of national supervisory and market surveillance authorities.

International Context

Germany's approach explicitly aligns national strategy and standards activity with EU policy and international standardisation bodies. The EU AI Act provides the primary legal baseline in the EU single market; Germany's national measures emphasise enabling innovation and protecting workers and individuals while contributing to EU-level implementation through cross-border standardisation and market surveillance cooperation. For official information and national portals see [German Federal Government — Artificial Intelligence](#) and the BMBF AI pages (e.g. [BMBF](#)), the BMAS KI-Observatorium pages (e.g. [BMAS](#)), and DIN/DKE standardisation materials (e.g. [DIN](#)).

Overall, Germany pursues a pragmatic, coordinated policy mix: strategic funding and research, workplace-centred monitoring and participation, technical standardisation to enable trustworthy deployment, and targeted legal proposals to address harms — all operating under the new EU-wide regulatory baseline established by the EU AI Act.

Ghana — AI Regulatory Landscape Summary

Overview

Ghana has established itself as a leader in AI governance on the African continent, developing a comprehensive regulatory framework that emphasizes ethical AI development, inclusive growth, and international cooperation. The country's approach builds on its [National AI Strategy 2023-2033](#) and partnership with UNESCO on [ethical AI readiness assessment](#). Ghana is recognized among Africa's AI pioneers alongside Rwanda, Senegal, and Benin, and played a significant role in the endorsement of the [African Union Continental AI Strategy](#) in Accra in July 2024.

Regulatory Instruments

- [Ghana National Artificial Intelligence Strategy 2023-2033](#) - Comprehensive 10-year roadmap establishing Ghana's vision for an AI-powered society, built on eight strategic pillars covering education, workforce development, infrastructure, and ethical AI governance.
- [Readiness Assessment Measurement \(RAM\) for Ethical Use of AI](#) - UNESCO-developed assessment framework evaluating Ghana's national preparedness for ethical AI implementation, launched in collaboration with the Data Protection Commission.

Key Themes and Priorities

- **Inclusive Growth:** Leveraging AI to benefit all Ghanaians and address socioeconomic development challenges.
- **Ethical AI Development:** Strong emphasis on responsible AI that addresses bias, privacy, and fairness concerns.
- **African Leadership:** Positioning Ghana as a continental leader and AI trailblazer in Africa.
- **Digital Inclusion:** Bridging the digital divide to ensure AI benefits reach underserved communities.
- **Workforce Development:** Building AI skills and capabilities across the economy.
- **Public Sector Innovation:** Deploying AI to improve government services and efficiency.
- **International Cooperation:** Partnership with UNESCO, Smart Africa, and alignment with AU frameworks.
- **Local Context Adaptation:** Developing AI systems suited to Ghana's specific needs and circumstances.

Governance Structure

- [Ministry of Communications and Digitalisation](#): Lead implementing agency coordinating AI strategy execution and policy development.
- [Data Protection Commission](#): Central role in ethical AI oversight and coordinating UNESCO RAM assessment.
- [National Communications Authority](#): Telecommunications regulation supporting AI infrastructure.
- [National Information Technology Agency](#): Digital infrastructure and eGovernment coordination.
- **Proposed Responsible AI Office:** Recommended under strategy to oversee implementation and ethical AI governance.

Implementation Status

Ghana's AI governance framework is in early-to-mid implementation phase. The [National AI Strategy](#) launched in October 2023 establishes the policy foundation with phased implementation through 2033. Initial activities focus on governance structure establishment and pilot programs. The [RAM assessment](#) launched in September 2024 is collecting baseline data on national AI readiness. Ghana hosted the AU Continental AI Strategy endorsement in July 2024, demonstrating regional engagement. The recommended Responsible AI Office has not yet been established. No dedicated AI legislation exists, with governance relying on existing data protection and cybersecurity laws. Multi-stakeholder engagement continues through consultations involving government, industry, academia, and civil society.

Future Developments

- **AI-Specific Legislation:** Strategy recommends developing dedicated AI regulations to address gaps in current frameworks.
- **Responsible AI Office:** Expected establishment of oversight body for strategy implementation.
- **RAM Assessment Results:** Initial findings expected to inform policy priorities and regulatory development.
- **Infrastructure Enhancement:** Continued investment in digital infrastructure supporting AI deployment.
- **Workforce Programs:** Scaling AI education and training initiatives across educational levels.
- **Regional Cooperation:** Continued engagement with AU Continental AI Strategy implementation.

International Context

Ghana's AI governance demonstrates strong international alignment and regional leadership. The country draws extensively from [UNESCO's Recommendation on AI Ethics](#) and was selected as one of only two African nations for UNESCO's RAM assessment, funded by the European Commission. Partnership with [Smart Africa](#) and [GIZ FAIR Forward](#) supported strategy development. Ghana's hosting of the [African Union Continental AI Strategy](#) endorsement in Accra in July 2024 underscores its continental leadership. The framework positions Ghana among African AI pioneers alongside Rwanda, Senegal, and Benin. Cross-continental cooperation through European partnerships strengthens capacity building and knowledge exchange.

Greece — AI Regulatory Landscape Summary

Overview

Greece's AI regulatory framework is the result of a deliberate policy mix that couples statutory digital governance with national strategy documents and EU-driven implementation measures. The Code on Digital Governance ([Law 4727/2020](#)) established baseline rules for digital administration, public-sector services, and the digital rights of citizens—forming the legal scaffolding for subsequent AI-relevant rules. The [Digital Transformation Bible 2020–2025](#) and the strategic blueprint by the High-Level Advisory Committee on AI provide policy direction and priorities (skills, research, trustworthy AI, data infrastructures). Building on these foundations, Greece enacted targeted statutory measures: [Law 4961/2022](#) introduced provisions for emerging ICT and strengthened digital governance; [Law 5039/2023](#) made omnibus amendments including transparency obligations and adjustments to Law 4961/2022; and [Law 5188/2025](#) implements the EU Data Governance Act's principles at the national level and advances the National Strategy for public sector data. In 2024 the government published the list of national authorities designated to supervise fundamental-rights obligations under the EU Artificial Intelligence Act, clarifying institutional roles and signaling readiness for the new European regime.

Regulatory Instruments

- [Law 4961/2022: Emerging information and communication technologies, strengthening digital governance and other provisions](#) - Status: In force. Type: National law (sectoral/tech governance). Summary: Introduces measures to govern emerging ICT within public administration and private-sector interfaces with state platforms; strengthens digital governance structures and enables administrative use of digital tools while creating obligations on transparency and service continuity.
- [Law 5039/2023: Omnibus measures \(includes amendments affecting Law 4961/2022 and transparency provisions\)](#) - Status: In force. Type: National omnibus statute (amendatory). Summary: Contains targeted amendments to Law 4961/2022 and other laws to tighten transparency requirements, clarify responsibilities for algorithmic decision-making where used by public entities, and update procurement and ICT resilience obligations.
- [Law 5188/2025: Measures for the implementation of the Data Governance Act and the National Strategy for public sector data](#) - Status: Enacted/Published. Type: National implementation law. Summary: Implements parts of the EU Data Governance Act in national law, establishes frameworks for data-sharing services, public sector data reuse, and governance arrangements to enable cross-agency data flows while protecting privacy and fundamental rights.
- [Digital Transformation Bible 2020-2025 \(National digital strategy / National Data Strategy elements\)](#) - Status: In force. Type: National strategy/white paper. Summary: Sets medium-term objectives for digital transformation, including data-driven public services, digital skills, trustworthy AI objectives, and interoperability of government information systems.
- [A Blueprint for Greece's AI Transformation \(High-Level Advisory Committee on AI report / foundational national AI strategy blueprint\)](#) - Status: Enacted/Published. Type: Strategic advisory report / blueprint. Summary: Provides foundational policy recommendations on research, skills, data infrastructures, ethics and governance to accelerate national AI adoption consistent with EU standards.
- [Publication of national authorities/bodies designated to supervise/enforce fundamental-rights obligations under the EU Artificial Intelligence Act \(national designation under Art.77\)](#) - Status: Enacted/Published. Type: Administrative designation (implementation step). Summary: Lists national competent authorities and

supervisory bodies charged with enforcement and coordination under the EU AI Act, clarifying responsibilities for high-risk systems and fundamental-rights compliance.

- [Law 4727/2020: Code on Digital Governance \(Digital Governance Law\)](#) - Status: In force. Type: Foundational national law. Summary: Establishes core rules for digital public administration, service delivery, interoperability, and administrative digital rights—serving as the basis for AI-related public-sector obligations.

Key Themes and Priorities

Across instruments the main emphases are: (1) public-sector transformation and data enablement—priority on reusing public sector data, improving interoperability, and enabling AI-assisted public services; (2) transparency and accountability—statutory transparency obligations for automated or algorithmic decision-support used by public bodies; (3) alignment with EU law—active implementation of the Data Governance Act and administrative preparation for the EU Artificial Intelligence Act; (4) governance and institutional readiness—designation of supervisory bodies and clearer ministerial responsibilities; (5) enabling innovation while safeguarding rights—support for research, skills and AI adoption together with procedural and technical safeguards against bias, discrimination and privacy harms. These priorities reflect a dual objective: accelerate digital and AI-enabled public services while minimizing risk to fundamental rights.

Governance Structure

Governance is distributed across ministries and independent authorities. Principal actors include the ministry responsible for digital governance (central policy and coordination), the General Secretariat for Digital Governance and related agencies that manage infrastructure and interoperability, sectoral ministries operating public services, and supervisory bodies designated for EU AI Act enforcement and rights protection. The Hellenic Data Protection Authority plays a central role on privacy and data protection matters. The 2024–2025 publication of national designations under Article 77 of the EU AI Act clarifies which authorities will supervise fundamental-rights obligations for high-risk systems and coordinate with the future EU Board and other national regulators. Operationalization relies on interministerial working groups, technical standards bodies and public procurement offices to translate legal obligations into procurement templates and compliance checklists.

Implementation Status

Implementation is partial but active. Foundational laws (Law 4727/2020 and the Digital Transformation Bible) are already in force and have informed administrative reform and digital service delivery. Law 4961/2022 and Law 5039/2023 are enacted and being applied to public administration activities where ICT and algorithmic methods are used, with particular focus on increasing transparency and resilience. Law 5188/2025 (Data Governance Act implementation) is enacted/published and introduces enabling mechanisms for data sharing and governance; secondary legislation, implementing decrees and operational guidance will be required to make many provisions effective. The publication of designated national authorities for the EU AI Act is a critical step in readiness; however, the full supervisory regime, sanctioning powers, and sectoral guidance will depend on further administrative instruments and cross-border coordination at EU level. Practically, many public agencies have started to map AI uses, update procurement clauses, and plan for risk assessments and documentation requirements. Key gaps remain in standardized conformity assessment infrastructure, sectoral technical standards, and comprehensive compliance guidance for private-sector providers working with the state.

Future Developments

Expect near-term action in several areas: (1) secondary regulations and technical guidance to operationalize Law 5188/2025 and the Data Governance Act; (2) administrative rules and templates to meet EU AI Act obligations (transparency, risk assessments, logging and human oversight) for public sector high-risk systems; (3) procurement reforms and contractual clauses that embed AI governance across public tenders; (4) capacity-

building and certification schemes to support trustworthy AI deployment in government; (5) potential amendments to align domestic penalties and enforcement tools with EU-level enforcement under the AI Act. The government will likely prioritize harmonizing national guidance with EU standards (conformity assessment frameworks, standardization bodies) and accelerating public-sector data availability under protected, governed conditions.

International Context

Greece's framework is explicitly anchored to EU law and policy: the Data Governance Act, the EU Artificial Intelligence Act and related European strategies are primary reference points. At the same time, Greece leverages national strategies (the Digital Transformation Bible and the national AI blueprint) to target domestic priorities—public sector modernization, workforce skills, and regional innovation. The designation of national authorities to supervise obligations under the EU AI Act ensures Greece is aligned institutionally with cross-border enforcement and cooperation mechanisms. For additional context and reference materials see the EU page on the AI Act ([EUR-Lex](#)), the Hellenic Data Protection Authority (www.dpa.gr), and national digital governance resources such as the Ministry/Secretariat portals (example: <https://digital.gov.gr>).

In sum, Greece combines statutory digital governance and strategy documents with recent targeted laws to create a coherent national approach to AI governance that is closely aligned with EU regulation. The next phase—secondary rules, technical standards, procurement integration and supervisory rulemaking—will determine how effectively the stated aims translate into consistent practice across government and the market.

Hong Kong — AI Regulatory Landscape Summary

Overview

Hong Kong has developed a principles-based approach to artificial intelligence governance that emphasizes ethical guidelines, data privacy protection, and smart city development over prescriptive legislation. As a Special Administrative Region of China and a leading international financial center, Hong Kong balances innovation promotion with citizen protection through flexible, guidance-oriented frameworks. The territory's AI governance rests on three pillars: the foundational [Personal Data \(Privacy\) Ordinance](#), the [Ethical Artificial Intelligence Framework](#) providing comprehensive ethical guidance, and the [Smart City Blueprint 2.0](#) driving public sector AI adoption. This combination creates a coherent ecosystem supporting responsible AI development while maintaining Hong Kong's competitive edge as a regional technology hub.

Regulatory Instruments

- [Personal Data \(Privacy\) Ordinance \(Cap. 486\)](#) — Hong Kong's foundational data protection law enacted in 1996, establishing comprehensive privacy principles including data collection limitations, purpose specifications, and security requirements. While predating AI, it governs automated decision-making and profiling activities through its six Data Protection Principles.
- [Smart City Blueprint for Hong Kong 2.0](#) — Released in December 2020, this strategic framework outlines the government's vision for technology-enabled urban development including AI applications across healthcare, transportation, education, and public services. It establishes governance principles for public sector AI deployment and catalyzes innovation initiatives.
- [Ethical Artificial Intelligence Framework](#) — Issued by the Privacy Commissioner in August 2021, this comprehensive guidance document establishes ethical principles for AI development and deployment including fairness, transparency, accountability, and human oversight. It provides practical recommendations adaptable to various organizational contexts.

Key Themes and Priorities

Hong Kong's AI governance framework reflects several interconnected priorities:

- **Data Privacy Protection** — Ensuring personal data used in AI systems is collected, processed, and stored in compliance with established privacy principles, with particular emphasis on automated decision-making transparency
- **Ethical AI Development** — Promoting fairness, non-discrimination, and accountability in AI systems through voluntary adherence to ethical principles rather than mandatory compliance requirements
- **Smart City Transformation** — Leveraging AI and emerging technologies to enhance public services, improve urban management, and increase government efficiency
- **Innovation Ecosystem Support** — Maintaining regulatory flexibility to encourage AI innovation and startup development while ensuring adequate safeguards
- **Financial Services Excellence** — Applying AI governance principles specifically to banking, securities, and insurance sectors where algorithmic systems increasingly drive operations

Governance Structure

Hong Kong's AI governance involves coordinated efforts across multiple agencies:

- [Office of the Privacy Commissioner for Personal Data \(PCPD\)](#) — Primary authority for data protection and AI ethics guidance, responsible for issuing the Ethical AI Framework and interpreting PDPO requirements for AI applications
- [Innovation and Technology Bureau](#) — Oversees technology policy, research and development funding, and strategic technology initiatives including AI promotion
- [Office of the Government Chief Information Officer \(OGCIO\)](#) — Coordinates digital government transformation, smart city implementation, and AI adoption across public sector agencies
- [Hong Kong Monetary Authority \(HKMA\)](#) — Provides sector-specific AI governance guidance for banking institutions including model risk management requirements
- [Securities and Futures Commission \(SFC\)](#) — Regulates AI applications in securities trading, robo-advisory services, and algorithmic trading systems

Implementation Status

Hong Kong's AI governance framework has reached substantial operational maturity. The PDPO has been in force since 1996 and actively enforced, with the PCPD conducting regular investigations and issuing guidance on AI-related privacy matters. The Ethical AI Framework, while voluntary, has seen widespread adoption among major corporations and financial institutions. The Smart City Blueprint 2.0 has progressed through multiple implementation phases, with numerous AI-enabled public services now operational including smart lampposts, traffic management systems, and e-government platforms. Financial regulators have integrated AI governance into their supervisory frameworks, with banks required to demonstrate sound model governance practices. The government continues monitoring implementation and adjusting guidance based on practical experience and emerging challenges.

Future Developments

Hong Kong's AI governance landscape continues evolving with several anticipated developments:

- **Enhanced Data Protection Reforms** — Potential amendments to the PDPO to address AI-specific challenges including algorithmic transparency and automated decision-making rights
- **AI-Specific Guidelines** — Development of additional sector-specific guidance for healthcare, education, and other domains with significant AI adoption
- **Cross-Border Data Frameworks** — Alignment mechanisms with Mainland China's AI regulations and international data protection standards
- **Generative AI Guidance** — Expected guidance addressing large language models, content generation systems, and associated risks
- **Public Sector AI Standards** — Formalization of AI governance requirements for government agencies building on Smart City Blueprint principles

International Context

Hong Kong's AI governance approach positions it uniquely between international frameworks and Chinese regulations. The Ethical AI Framework aligns substantially with [OECD AI Principles](#), emphasizing human-centered values, transparency, and accountability. Hong Kong maintains awareness of EU developments including the AI Act, though it has not adopted risk-based classification approaches. As a Special Administrative Region, Hong Kong must consider compatibility with Mainland China's AI regulations while maintaining its distinct common law legal system. The territory participates in international standards development and maintains regulatory dialogue

with peer jurisdictions including Singapore, which has adopted similar principles-based approaches. Hong Kong's status as an international financial center influences its regulatory philosophy toward maintaining competitiveness while ensuring robust governance.

Business Compliance Requirements

Organizations deploying AI systems in Hong Kong should address several key compliance areas:

- **Data Protection Compliance** — Ensure all personal data used in AI systems complies with PDPO requirements including consent, purpose limitation, and security measures
- **Ethical Framework Alignment** — Conduct self-assessments against the Ethical AI Framework principles and document governance measures
- **Sector-Specific Requirements** — Financial institutions must comply with HKMA and SFC guidance on model governance, algorithmic trading, and customer-facing AI systems
- **Privacy Impact Assessments** — Conduct assessments for AI systems processing personal data, particularly those involving profiling or automated decisions
- **Transparency Obligations** — Inform individuals when AI systems make significant decisions affecting them and provide explanations upon request

Sector-Specific Applications

AI governance in Hong Kong addresses sector-specific considerations:

- **Financial Services** — Comprehensive requirements for credit scoring algorithms, trading systems, anti-money laundering AI, and robo-advisory platforms under HKMA and SFC supervision
- **Healthcare** — Guidance on AI-assisted diagnostics, clinical decision support, and medical device regulations under Hospital Authority and Department of Health oversight
- **Public Sector** — Smart City Blueprint principles governing AI deployment in government services, public infrastructure, and citizen-facing applications
- **Transportation** — Emerging framework for autonomous vehicles and AI-enabled traffic management systems

Enforcement and Penalties

Enforcement of AI-related requirements in Hong Kong operates primarily through the PDPO regime and sector-specific regulatory frameworks. The Privacy Commissioner has authority to investigate complaints, conduct inspections, and issue enforcement notices for PDPO violations. Serious breaches can result in criminal prosecution with penalties including fines up to HK\$1 million and imprisonment. Financial regulators can impose disciplinary actions, license revocations, and monetary penalties for non-compliance with AI governance requirements. The Ethical AI Framework, being voluntary, is not directly enforceable but may be referenced in regulatory assessments and litigation proceedings. Organizations face reputational risks from publicized enforcement actions and regulatory findings.

Rights and Protections

Hong Kong's framework provides several protections for individuals affected by AI systems:

- **Data Access Rights** — Individuals can request access to personal data held about them, including data used in AI systems
- **Correction Rights** — Right to request correction of inaccurate personal data in AI databases

- **Explanation Rights** — Ethical AI Framework encourages organizations to provide meaningful explanations for automated decisions
- **Complaint Mechanisms** — Individuals can file complaints with the Privacy Commissioner regarding data protection violations in AI systems
- **Non-Discrimination** — Framework principles emphasize fairness and non-discrimination in AI system design and operation

Resources and Further Information

Key resources for understanding Hong Kong's AI governance framework:

- [PCPD Guidance on AI and Data Protection](#)
- [Smart City Blueprint for Hong Kong 2.0](#)
- [HKMA AI Guidance for Banking](#)
- [OGCIO Digital Government Resources](#)

Hungary — AI Regulatory Landscape Summary

Overview

Hungary's artificial intelligence (AI) regulatory architecture as of 2025 is the product of layered policy instruments: a national strategy (Magyarország Mesterséges Intelligencia Stratégiája), multiple Government Resolutions that set discrete policy and programmatic priorities, and national legislation and implementing regulation to give effect to the European Union's AI Regulation within Hungary. The overall trajectory is dual: enable and strengthen a national innovation ecosystem while ensuring legal alignment with the EU's risk-based regulatory approach. The policy framework is designed to support public awareness and workforce preparedness, concentrate development in prioritized domains, and foster international cooperation to amplify domestic capacity.

Regulatory Instruments

- [Hungary's National Artificial Intelligence Strategy \(Magyarország Mesterséges Intelligencia Stratégiája\)](#) - The foundational strategic document articulating national objectives for AI research, commercialization, public-sector adoption, education and workforce development, and ethical considerations. Type: National strategy (policy). Status: Changed/updated (policy in force).
- [Government Resolution on measures to increase social awareness of artificial intelligence \(A mesterséges intelligenciával kapcsolatos társadalmi tudatosság növelését szolgáló intézkedésekről\)](#) - A targeted resolution directing programs and communications to raise public understanding of AI risks, benefits, and rights. Type: Government resolution (executive policy measure). Status: Enacted/Published.
- [Government Resolution on measures to strengthen domestic AI strategy and priority development areas \(A mesterséges intelligencia hazai stratégiai megerősítését és kiemelt fejlesztési területeit szolgáló intézkedésekről\)](#) - Identifies priority domains for public support (e.g., health technologies, intelligent transport, digital public services) and instruments for stimulating R&D and commercialization. Type: Government resolution (executive policy measure). Status: Enacted/Published.
- [Government Resolution on measures promoting international cooperation supporting AI development \(A mesterséges intelligencia fejlesztését támogató nemzetközi együttműködést előmozdító intézkedésekről\)](#) - Sets out measures to deepen bilateral and multilateral research partnerships, secure participation in EU and international programs, and improve cross-border regulatory coordination. Type: Government resolution (executive policy measure). Status: Enacted/Published.
- [Act LXXV of 2025 on the domestic implementation of the European Union Regulation on Artificial Intelligence \(Az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról\)](#) - Primary national implementing law to translate obligations of the EU AI Regulation into Hungarian administrative and enforcement structures (designation of competent authorities, sanctions, procedural law). Type: National Act (legislation). Status: Not yet in force (adopted).
- [Government Decree 344/2025 on the implementation of the Act executing the EU Artificial Intelligence Regulation \(a 2025. évi LXXV. törvény végrehajtásáról\)](#) - Deploys delegated and administrative details required by the Act (procedural rules, timelines, administrative forms and enforcement mechanics). Type: Government decree (subordinate regulation). Status: Not yet in force (adopted).

Key Themes and Priorities

Across Hungary's instruments several cross-cutting priorities are evident: (1) capacity building through targeted R&D funding, clustering of public-private partnerships, and support for start-ups and scale-ups in priority sectors;

(2) workforce development and education to mitigate skills gaps and support public-sector digital transformation; (3) public awareness and trust-building measures to improve societal literacy about AI and manage social risks; (4) legal alignment with the EU AI Regulation to ensure that domestic markets, conformity assessment, and enforcement meet EU standards; and (5) international cooperation to attract investment, participate in joint research, and harmonize standards.

Governance Structure

Governance responsibility is shared. Strategic coordination and high-level policy direction sit with the Prime Minister's Office and line ministries that cover innovation, economy, interior, justice and education. The implementing Act foresees designation of national competent authorities for specific sectors and functions (market surveillance, fines, oversight of high-risk AI systems). The national strategy and resolutions also direct research funding agencies, national research institutions and universities to implement capacity-building measures. Where EU competences apply (conformity assessment, high-risk classification), Hungarian authorities will act as national focal points implementing EU procedures domestically.

Implementation Status

Implementation in 2025 is transitional. The national strategy and three Government Resolutions are operational instruments guiding programs, budget allocation and administrative priorities. Act LXXV of 2025 and Government Decree 344/2025 have been adopted to implement the EU AI Regulation domestically but are recorded as "not yet in force" in the inventory supplied. Before full operational enforcement can occur, practical steps remain: (a) setting commencement dates for the Act and Decree; (b) publishing secondary guidance and administrative forms; (c) formally designating competent authorities and establishing market surveillance and enforcement units; (d) standing up registries/notification platforms (if required under implementing rules); and (e) stakeholder outreach and guidance to industry, public procurers, and research institutions to ensure compliance pathways are understood.

Future Developments

Near-term developments to monitor include the exact entry-into-force dates for Act LXXV of 2025 and Government Decree 344/2025, publication of implementing guidance (including conformity assessment and notification procedures), and the formal appointment and resourcing of national competent authorities. Medium-term actions will include enforcement practice, sector-specific guidance (particularly in health, transport and public administration), and further regulatory or budgetary measures to accelerate prioritized development areas. Hungary's international cooperation measures may yield new joint programs, research partnerships and investments that shape the domestic AI ecosystem.

International Context

Hungary's legislative and policy choices are explicitly aligned with the EU's AI Regulation and wider EU priorities for digital sovereignty, interoperability and standards. The national implementing Act mirrors the EU's risk-based approach, while resolutions focus on competitiveness and public trust. Hungary also seeks broader international collaboration to enhance research capacity and attract talent and capital. Stakeholders operating across borders should watch harmonization efforts and EU-level guidance because these will shape national enforcement and cross-border market access. For the official EU regulatory framework context, see the European Commission and EU legal resources (for example, the EU's legal and policy portals such as [Eur-Lex](#) and the European Commission digital policy pages).

Practical takeaways: organizations should (1) map their products and services against the EU risk categories to anticipate whether their systems will be treated as high-risk; (2) prepare for conformity assessment and recordkeeping obligations; (3) follow Hungarian guidance as soon as the Act and Decree enter into force and

competent authorities publish operational rules; and (4) engage with government awareness and cooperation initiatives to benefit from funding and partnership opportunities. For Hungarian-language official materials and program announcements consult the Hungarian government portals and ministry pages, and watch for administrative notices that set commencement dates and procedural rules.

For a consolidated list of the instruments summarized above see the national regulation index and the government AI portal (government pages and ministerial releases are primary sources for up-to-date commencement dates and administrative guidance).

Iceland — AI Regulatory Landscape Summary

Overview

Iceland has developed a comprehensive AI governance framework suited to its position as a small, technologically advanced Nordic nation. The framework combines the foundational 2021 Policy on Artificial Intelligence with the detailed AI Action Plan 2024-2026, which introduces 25 targeted measures across five strategic pillars. The [Government of Iceland](#) coordinates AI policy with emphasis on responsible development, workforce preparation, and preservation of Icelandic language and culture. As an EEA member, Iceland will implement the [EU AI Act](#) upon incorporation, ensuring alignment with European standards while maintaining flexibility for national priorities.

Regulatory Instruments

- [Iceland AI Action Plan 2024-2026](#) - Comprehensive action plan with 25 measures across five pillars: AI for society, competitive working life, education, public sector adoption, and healthcare integration. Projects 55% workforce transformation and 0.8-6% annual GDP growth from AI.
- [Iceland Policy on Artificial Intelligence](#) - Foundational 2021 policy establishing three core pillars: AI for the benefit of all, competitive working life, and education in line with the times. Laid groundwork for subsequent action plan.

Key Themes and Priorities

- **Responsible AI Development:** Emphasis on ethical AI aligned with European values and human-centered principles.
- **Icelandic Language Preservation:** Specific focus on developing AI tools for Iceland's unique language, addressing challenges faced by small language communities.
- **Workforce Transformation:** Proactive approach to preparing 55% of jobs expected to change due to AI through reskilling and education.
- **Public Sector Efficiency:** Targeting 30% time savings through AI adoption in government services.
- **Healthcare Innovation:** Pilot projects for AI in diagnostics and healthcare delivery.
- **AI Literacy:** Integration of AI education from primary school through university levels.
- **European Alignment:** Coordination with EU AI Act and EEA regulatory frameworks.

Governance Structure

- [Ministry of Culture, Innovation and Higher Education](#): Lead ministry for AI policy coordination and Action Plan implementation.
- **Inter-ministerial Coordination:** Whole-of-government approach ensuring alignment across sectors.
- [Icelandic Centre for Research \(Rannís\)](#): Research funding and support for AI innovation.
- **Universities:** Educational programs and AI research capacity.

Implementation Status

The 2021 AI Policy has been in effect since adoption, providing strategic direction for government and stakeholder initiatives. The AI Action Plan 2024-2026 was released in late 2024 and is in early implementation, with government agencies working on assigned measures. Educational integration of AI literacy is progressing across school levels. Public sector pilot projects for AI adoption are being developed. Healthcare AI initiatives are in planning stages. The EU AI Act will be implemented once incorporated into the EEA Agreement, with Iceland preparing for compliance requirements. Language technology initiatives for Icelandic continue as an ongoing priority.

Future Developments

Iceland's AI governance will evolve along several tracks. Implementation of the 25 Action Plan measures will continue through 2026, with mid-term review informing adjustments. EU AI Act incorporation into the EEA Agreement will introduce binding regulatory requirements with significant penalties. A successor framework to the 2024-2026 Action Plan will be developed. Healthcare AI pilots may expand based on results. Educational AI programs will mature and expand. Icelandic language AI capabilities will continue development. Iceland may contribute to Nordic and European AI governance discussions as a model small-country approach.

International Context

Iceland's AI governance demonstrates strong alignment with European frameworks while addressing unique national considerations. As an EEA member, Iceland participates in the European single market and will implement the [EU AI Act](#). The framework incorporates [OECD AI Principles](#) on trustworthy AI. Nordic cooperation through the Nordic Council of Ministers provides regional coordination on AI governance. Iceland's approach to small language AI preservation may serve as a model for other small language communities. The country participates in international AI governance discussions, contributing perspectives as a small, advanced democracy.

India — AI Regulatory Landscape Summary

Overview

India's artificial intelligence (AI) regulatory landscape as of 2025 is shaped by a combination of national strategy documents, expert committee reports, draft data-governance policies and a small set of enforceable digital rules. The overall posture adopted by central policy actors such as NITI Aayog and the Ministry of Electronics and Information Technology (MeitY) emphasizes enabling innovation, building public AI infrastructure, and establishing governance mechanisms for data while moving carefully on legally binding AI-specific regulation. This hybrid architecture leaves substantial scope for sectoral regulation, future statutory developments (notably activation of the Digital Personal Data Protection Act, 2023) and incremental governance instruments.

Regulatory Instruments

- [National Strategy for Artificial Intelligence \(#AIforAll\) - NITI Aayog](#) - Strategic policy document (Published/Enacted as guidance). Sets national priorities for AI in India, recommending sectoral focus (healthcare, agriculture, education, smart cities, etc.), public-private partnerships, skilling and establishing a pro-innovation regulatory stance.
- [Report of the Committee on Platforms and Data on Artificial Intelligence \(MeitY report\)](#) - Expert committee report (Published). Examines platform responsibilities, data flows and recommendations for technical and governance measures to support trustworthy AI, including platform-level accountability mechanisms.
- [AIRAWAT \(AI Research, Analytics and Knowledge Assimilation platform\) - Approach Paper](#) - Approach / infrastructure paper (Published). Proposes a national AI compute and data platform to provide shared compute, datasets and tools for research and responsible AI development.
- [RAISE 2020 \(Responsible AI for Social Empowerment\) Summit - MeitY & NITI Aayog](#) - Conference summary and commitments (Published). High-level convening that advanced the concept of Responsible AI for social empowerment and outlined priorities for collaboration and initiatives.
- [Report by the Committee of Experts on Non-Personal Data Governance Framework \(Gopalakrishnan Committee\)](#) - Committee report (Published). Recommended a governance model for non-personal data including data access, benefit-sharing, and proposals for custodians, data trusts and a regulatory architecture for non-personal data.
- [Towards Responsible AI for All \(Approach Document, Part I\) - NITI Aayog](#) - Policy approach document (Published). Expands on principles for responsible AI, focusing on inclusion, fairness, transparency and context-appropriate governance measures.
- [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules, 2021](#) - Statutory subordinate legislation (In force). Imposes duties on intermediaries and digital media, including traceability, grievance redressal, content takedown timelines and significant social media intermediary compliance obligations.
- [Draft National Data Governance Framework Policy / India Data Accessibility and Use Policy \(drafts\)](#) - Draft policy instruments (Draft). Propose principles, institutional arrangements and mechanisms to enable access to public and private non-personal data for research and public interest while protecting legitimate rights.
- [Digital Personal Data Protection Act, 2023](#) - Enacted statute (Not yet in force). Establishes a statutory regime for processing of digital personal data, sets out obligations, rights and supervisory authority; activation and rulemaking pending.

Key Themes and Priorities

Common themes across India's AI-related documents include: a risk-based, sector-sensitive approach to regulation; prioritization of economic empowerment and social benefit (e.g., healthcare and agriculture); investment in public digital infrastructure and datasets (AIRAWAT); emphasis on explainability, fairness and human oversight; and an orientation towards enabling secondary use of data (especially non-personal or anonymized data) subject to governance safeguards. India favors regulatory modesty where possible—preferring guidance, standards and enabling platforms—while using targeted statutory instruments (e.g., IT Rules) for discrete risks such as online harm and intermediary conduct.

Governance Structure

Key national bodies shaping AI policy and governance are NITI Aayog and MeitY. NITI Aayog has authored flagship strategy and approach documents while MeitY has convened expert committees and drafted technical reports. Other actors include the Ministry of Health and Family Welfare (sectoral AI in health), Ministry of Agriculture (agritech use cases), the Department of Consumer Affairs and the Ministry of Information and Broadcasting (digital media governance). Expert committees (such as the Gopalakrishnan committee) and multi-stakeholder consultations contribute recommendations. Once in force, the Digital Personal Data Protection Act will create a statutory supervisory authority responsible for enforcement of personal data rules.

Implementation Status

Implementation is uneven. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are operational and have had immediate compliance implications for large platforms, especially "significant social media intermediaries." NITI Aayog and MeitY initiatives (e.g., RAISE, AIRAWAT approach) have mobilized public-private activity and pilot infrastructure, but require continued funding and operational governance arrangements to scale. The Gopalakrishnan Committee and NDGF drafts have informed debate on non-personal data governance but have not been fully crystallized into enforceable law; significant legal, technical and commercial issues remain to be resolved, including interface with personal data protections and intellectual property. The Digital Personal Data Protection Act, 2023 is an important statutory milestone but had not been brought into force as of the reporting date; consequential rulemaking and appointments will determine its practical effect. The net result is a landscape where high-level strategic direction and technical proposals exist, while statutory and regulatory teeth are currently concentrated in sectorally-focused or platform-focused rules rather than a comprehensive AI statute.

Future Developments

Near-term priorities likely include activation of the Digital Personal Data Protection Act and its rulemaking; finalization (or revision) of the National Data Governance Framework / India Data Accessibility and Use Policy; operational rollout of public AI infrastructure proposals such as AIRAWAT; and increased sectoral rulemaking for high-risk uses (health tech, financial services, education). India is also expected to calibrate its domestic approach with international developments: EU regulatory models, OECD AI principles, G20 commitments and multilateral norms will be influential. Private sector self-regulation, standards bodies and technical consortia will also shape implementation practices for fairness, robustness and auditability.

International Context

India's approach aims to balance innovation and safety and therefore maps to global trends favoring risk-based and sectoral regulation rather than blanket prohibitions. India participates in international dialogues on AI governance (G20/OECD/Global Partnership on AI) and seeks interoperability with global data flows while asserting policy space to promote national economic and social priorities. The interplay between domestic data governance proposals and extraterritorial regulatory regimes (such as the EU's AI Act and data protection standards) will be an

important determinant of compliance burdens for multinational providers and for cross-border research collaboration.

Overall, India is operating a policy-first, capacity-building-and-infrastructure second, statutory-enforcement third model for AI governance. This incremental, adaptive approach is intended to preserve space for innovation while progressively establishing legal protections for privacy, platform accountability, and responsible data use.

Indonesia — AI Regulatory Landscape Summary

Overview

Indonesia's AI regulatory framework is best described as layered and incremental: it leverages established digital laws and new data-protection legislation as the legal backbone, while soft- and hard-sectoral instruments (ministerial circulars, regulator guidance and industry codes) build operational expectations for AI deployment. Parallel to these binding instruments, national planning documents provide strategic direction to stimulate innovation, skills and public-sector adoption. The present mix reflects an intent to balance economic opportunity, national security, and individual rights, and it is evolving toward more centralised AI governance through draft national-level instruments.

The principal legal building blocks in force are: Government Regulation No.71/2019 on Electronic Systems and Transactions (PP71/2019), Undang-Undang No.27/2022 on Personal Data Protection (UU PDP), and the Second Amendment to the Information and Electronic Transactions Law enacted as Undang-Undang No.1/2024 (the 2024 UU ITE amendment). These statutes confer obligations on operators of electronic systems, impose privacy and data-handling duties, and extend responsibilities for online information management—each of which has direct bearing on AI systems that collect, process or publish data or generate user-facing content.

Regulatory Instruments

- [Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik \(Government Regulation No.71/2019 on Electronic Systems and Transactions\)](#) - In force; regulatory government regulation governing registration, obligations and administrative oversight of electronic systems, including availability, reliability and security requirements that apply to platforms and large-scale systems commonly used in AI deployments. Type: Government Regulation (binding).
- [Strategi Nasional Kecerdasan Artifisial Indonesia \(National Strategy for Artificial Intelligence\) 2020–2045](#) - Enacted/published; long-term national strategy setting priorities for AI research, talent development, infrastructure and responsible deployment across public and private sectors. Type: Strategic policy document.
- [Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi \(Law No.27/2022 on Personal Data Protection\)](#) - In force; comprehensive personal data protection law that introduces legal bases for processing, data subject rights, obligations for controllers/processors, breach notification, cross-border transfer rules and sanctions. Type: National statute.
- [Panduan Kode Etik Kecerdasan Buatan yang Bertanggung Jawab dan Terpercaya di Industri Teknologi Finansial \(OJK & Associations' AI Code of Ethics for Fintech\)](#) - Enacted/published; sectoral ethics code developed with OJK and industry associations addressing fairness, transparency, model validation, customer protection and governance for AI in fintech. Type: Sectoral code / guidance.
- [Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial \(Ministerial Circular No.9/2023 on AI Ethics\)](#) - Enacted/published; non-binding ministerial circular articulating ethical principles (e.g., human oversight, non-discrimination, safety) and calls for industry compliance and transparency. Type: Ministerial circular (policy guidance).
- [Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik \(Second Amendment to the Electronic Information and Transactions Law\)](#) - In force; updates to the ITE framework impacting content liability, intermediary obligations and enforcement powers that affect AI systems producing or distributing information. Type: National statute (amendment).

- [Buku Panduan Tata Kelola Kecerdasan Artifisial Perbankan Indonesia \(OJK Guidance on AI Governance for Indonesian Banking\)](#) - Enacted/published; regulator guidance for banks covering risk management, model validation, data governance, third-party oversight and audit expectations for AI used in banking. Type: Regulator guidance.
- [Rancangan Undang-Undang tentang Kecerdasan Buatan \(Draft Bill on Artificial Intelligence\)](#) - Draft; proposed horizontal AI statute under legislative consideration intended to introduce risk-based obligations, accountability, and a governance regime for high-risk AI systems. Type: Draft law.
- [Buku Putih Peta Jalan Kecerdasan Artifisial Nasional \(White Paper / Roadmap for National AI\)](#) - Under review; a policy roadmap aligning ministries, industry and research priorities, intended to support implementation of Stranas AI. Type: White paper / roadmap (policy document under review).
- [Konsep Pedoman Etika Kecerdasan Artifisial \(Concept Draft of Ethical Guidelines for AI\)](#) - Under review; draft ethical guidelines detailing principles and suggested practices for responsible AI across sectors. Type: Draft ethical guideline.
- [Rancangan Peraturan Presiden tentang Kecerdasan Buatan \(Draft Presidential Regulation on Artificial Intelligence\)](#) - Draft; expected to set executive-level governance, interagency coordination mechanisms and implementation architecture for national AI policy. Type: Draft presidential regulation.

Key Themes and Priorities

Across Indonesia's instruments several persistent themes emerge: (1) data protection and privacy—driven by UU PDP 2022 and operationalised through data governance requirements for AI; (2) risk-based governance—a preference for calibrating obligations according to societal risk and criticality (e.g., finance, public services); (3) sectoral supervision—OJK and other regulators translate general principles into sector-specific supervisory expectations; (4) transparency and accountability—emphasis on explainability, human oversight and documentation; (5) innovation and capacity building—Stranas AI and the White Paper highlight R&D, talent pipelines and public-private collaboration; and (6) cybersecurity and resilience—intersection with BSSN mandates and PP71/2019 security expectations.

Governance Structure

Responsibility for AI policy and oversight is distributed. Key actors include the Ministry of Communication and Informatics (Kominfo) for information policy and ethical guidance; the Financial Services Authority (OJK) for financial-sector AI governance; the National Cyber and Crypto Agency (BSSN) for cybersecurity aspects affecting AI systems; the National Research and Innovation Agency (BRIN) and related ministries for R&D and capacity-building initiatives; and line ministries that regulate sectoral risk (health, transportation, education). Draft horizontal instruments aim to create clearer cross-ministerial coordination, possibly with a central oversight body or council to orchestrate compliance, standards and public procurement.

Implementation Status

Implementation is active but uneven. Binding laws (PP71/2019, UU PDP 2022, UU ITE 2024) are enforceable and have immediate compliance implications. Kominfo's circular and OJK guidance are being operationalised through industry practice and supervisor expectations, especially within finance where OJK has prioritized governance and model risk management. Draft instruments remain the principal vehicles for addressing gaps: the Draft AI Bill and Draft Presidential Regulation are the most consequential for establishing unified obligations and enforcement models for high-risk AI. Practical challenges include capacity for technical supervision, harmonising sectoral rules, and building standards and certification regimes for model validation and safety testing.

Future Developments

Major near-term changes to watch include finalisation of the Draft AI Bill, issuance of a Presidential Regulation to coordinate agencies, publication of the White Paper and the formalisation of ethical guidelines. These moves are likely to introduce risk-tiering, mandatory compliance for certain high-risk systems, enhanced oversight mechanisms and more explicit rules for government use of AI and for cross-border data flows. Industry should expect a phased approach combining voluntary standards, supervisory requirements and eventual statutory duties for critical AI applications.

International Context

Indonesia's trajectory aligns with global patterns: reliance on data protection, risk-based controls, sectoral supervision and ethical guidance while seeking to preserve innovation. The government references international norms in planning documents and aims to position Indonesia as a regional hub for responsible AI. For further details and primary references see the government portal: <https://government.ai.portal> and institutional sites such as Kominfo and OJK (refer to official sources listed below).

Official sources (examples): <https://kominfo.go.id>, <https://www.ojk.go.id>, <https://www.brin.go.id>, and the national legal repository.

Iran — AI Regulatory Landscape Summary

Overview

Iran's artificial intelligence regulatory framework represents a distinctive governance approach combining ambitious technological development goals with strong emphasis on cultural value alignment and national sovereignty. Since the Supreme Leader's 2021 directive calling for a national AI strategy, Iran has rapidly developed comprehensive policy and legislative instruments. The framework aims to position Iran among the world's top 10 AI-harnessing countries by 2032, with targets including AI integration into 45% of industries and 12% GDP contribution. Despite international sanctions limiting access to advanced computing hardware, Iran ranks 13th globally in AI research output according to [Nature's index](#), demonstrating significant domestic research capabilities. The governance philosophy emphasizes trustworthy AI development aligned with Islamic values, domestic capability building, and strategic independence from Western technology influence.

Regulatory Instruments

- [Computer Crimes Law](#) (2009) — Foundational cybersecurity legislation incorporated into the Islamic Penal Code, establishing criminal penalties for unauthorized access, data theft, computer fraud, and cybercrimes. Comprises 5 parts and 55 sections with penalties including imprisonment and monetary fines. Mandates ISP data retention and VoIP recording capability, providing essential infrastructure for digital governance.
- [National Artificial Intelligence Document](#) (2024) — Comprehensive policy blueprint approved by the Supreme Council of the Cultural Revolution in June 2024, containing 14 policies and 11 major goals. Defines AI-related responsibilities for all government agencies and directly led to establishment of the National AI Organization. Emphasizes cultural value alignment and independence from Western influence.
- [National Artificial Intelligence Plan](#) (2025) — Legislative framework approved by Parliament in May 2025 with overwhelming 187-33 majority, allocating \$115 million for AI research and development. Establishes 2032 targets for industrial integration and GDP contribution, supported by projected \$8 billion cumulative investment. Provides funding authority through grants and National Development Fund loans.

Key Themes and Priorities

- **National Sovereignty in AI:** Strong emphasis on developing domestic AI capabilities independent of Western technology influence, with review processes ensuring AI frameworks are not "tainted by Western influence."
- **Cultural and Islamic Value Alignment:** All AI development must conform to Islamic principles and Iranian cultural values, with the Supreme Council of the Cultural Revolution providing oversight to ensure alignment.
- **Strategic Global Positioning:** Ambitious goal to become a top 10 AI power globally by 2032, responding to regional competition particularly from Gulf states receiving US technology cooperation.
- **Trustworthy AI Ecosystem:** Building ethical and legal infrastructure for responsible AI deployment, including public awareness initiatives and workforce development.
- **Cybersecurity and Data Control:** Comprehensive cybersecurity framework with ISP data retention requirements and restrictions on encryption that could deny authorized access.
- **Industrial Integration:** Mandate for AI adoption across 45% of industries with significant GDP contribution targets.

- **Regional Technology Leadership:** Maintaining strategic position as AI leader in the Persian Gulf and Middle East region.

Governance Structure

- **Supreme Council of the Cultural Revolution:** Strategic policy body answering only to the Supreme Leader, providing oversight of AI governance to ensure alignment with national values. Established Defense AI Commission in September 2022.
- **National AI Organization:** Independent coordinating body established July 2024 under direct presidential supervision, serving as the primary authority for steering Iran's AI ecosystem toward 2032 goals.
- **Vice Presidency for Science and Technology:** Leads operational implementation of AI initiatives, including the national AI platform development. Has already implemented significant portions of the National AI Document.
- **Islamic Consultative Assembly:** Parliament provides legislative authority and oversight, with Industries Commission maintaining review of implementation progress.
- **National Development Fund of Iran:** Administers \$100 million loan facility for AI projects under the National AI Plan.
- **Judiciary and FATA Police:** Enforce Computer Crimes Law through investigation and prosecution of cybercrimes and unauthorized access.

Implementation Status

Iran's AI governance framework has achieved significant implementation milestones since 2021. The [National AI Document](#) has been substantially implemented by the Vice Presidency for Science, Technology and Knowledge-Based Economy, establishing institutional structures and agency responsibilities. The [National AI Plan's](#) \$115 million allocation became effective in early 2025, with grants and NDFI loans being disbursed to research institutions and AI projects. A prototype of Iran's national open-source AI platform was publicly unveiled on March 15, 2025, with a stable version expected within one year. The [Computer Crimes Law](#) continues to be enforced through the Judiciary and FATA Police, providing cybersecurity infrastructure for AI governance. ISP data retention requirements under Articles 21 and 48 are operational. Implementation challenges include international sanctions limiting access to advanced computing hardware and gaps in comprehensive data protection legislation, though a Draft Protection of Personal Data Law remains under parliamentary review.

Future Developments

Iran's AI governance framework anticipates significant developments as the country works toward its 2032 objectives. The national AI platform is scheduled for stable release by 2026, providing domestic infrastructure for AI applications aligned with Iranian values. Investment is expected to scale progressively toward the \$8 billion cumulative target by 2032. Comprehensive data protection legislation may advance if the Draft Protection of Personal Data Law (2018) proceeds through parliamentary review, addressing gaps in current privacy protections. The National AI Organization is expected to issue additional guidance and requirements as the ecosystem matures. Defense AI applications will continue development under SCCR oversight through the Defense AI Commission. Regional competition, particularly following US-Gulf state AI agreements, may accelerate Iran's implementation timeline and investment levels. Bilateral cooperation with Russia on AI ethics and potentially other aligned nations may expand. Industrial AI integration will be monitored against the 45% target, with potential regulatory adjustments to accelerate adoption across priority sectors.

International Context

Iran's approach to AI governance diverges significantly from Western frameworks, reflecting its emphasis on national sovereignty and cultural value alignment. Unlike the [EU AI Act's](#) risk-based approach, Iran's framework prioritizes cultural and religious conformity alongside technical considerations. Iran has supported the [UNESCO Recommendation on AI Ethics](#) but has not ratified the Budapest Convention on Cybercrime. The March 2024 Iran-Russia Memorandum of Understanding on AI ethics demonstrates preference for bilateral arrangements with aligned nations. Iran's 94th ranking in the 2024 Oxford Insights government AI readiness index contrasts with its 13th-place research output ranking, indicating implementation gaps despite research strength. The [Computer Crimes Law's](#) encryption restrictions and content controls have drawn criticism from international human rights organizations including [ARTICLE 19](#). Regional competition drives Iran's acceleration, particularly following AI-related agreements between the United States and Gulf states including the UAE and Saudi Arabia. Iran positions itself as an alternative technology leader in the Middle East, emphasizing values-aligned AI development independent of Western influence.

Iraq — AI Regulatory Landscape Summary

Overview

Iraq is at an early but significant stage in developing its artificial intelligence governance framework. The country's approach combines established digital commerce legislation with emerging dedicated AI policy initiatives. Under the leadership of Prime Minister [Mohammed Shia al-Sudani](#), Iraq has demonstrated commitment to AI development through the formation of the Supreme Committee for Artificial Intelligence in August 2024 and the recent activation of its electronic signature infrastructure in September 2025. The regulatory landscape reflects Iraq's recognition that AI governance requires both foundational digital infrastructure and specific AI policy frameworks. As a major Middle Eastern nation with significant reconstruction and development priorities, Iraq's approach to AI governance balances technological advancement with economic development goals and capacity-building needs.

Regulatory Instruments

- [Electronic Signature and Transactions Law No. 78 of 2012](#) - Iraq's foundational legislation for electronic commerce, establishing legal validity for electronic signatures and digital contracts. Recently activated in September 2025 with the launch of Iraq's official electronic signature system, this law provides critical infrastructure for AI-enabled digital services across government and private sector.
- [Iraqi National Strategy for Artificial Intelligence \(INSAIN\)](#) - Iraq's dedicated national AI strategy currently under development. The Supreme Committee for AI, chaired by PM al-Sudani, held its first meeting in August 2024 to begin formulating Iraq's comprehensive approach to AI governance, development, and adoption. The strategy aims to position Iraq as a regional leader in AI.

Key Themes and Priorities

Iraq's emerging AI governance framework reflects several key themes:

- **Digital Infrastructure Development:** Building the technical and legal foundation for digital services, including electronic signatures and secure digital transactions, as prerequisites for AI adoption.
- **High-Level Government Commitment:** Direct engagement by the Prime Minister and Council of Ministers demonstrates AI governance as a national priority rather than a technical ministry matter.
- **Human Capital Development:** Emphasis on building domestic AI expertise through new university programs, with two AI colleges planned at University of Baghdad, and training initiatives for digital leaders.
- **International Capacity Building:** Engagement with international organizations like UNESCO for AI ethics training and alignment with global best practices.
- **Economic Development Integration:** Positioning AI adoption within broader economic development and post-conflict reconstruction priorities.
- **Regional Leadership Aspiration:** Ambition to become a regional leader in AI adoption among Middle Eastern and Arab nations.

Governance Structure

Iraq's AI governance involves multiple government bodies working together:

- **Council of Ministers:** Provides executive leadership for AI policy under PM Mohammed Shia al-Sudani, who chairs the Supreme Committee for AI.
- **Supreme Committee for Artificial Intelligence:** Established in 2024, this committee coordinates national AI strategy development and brings together representatives from key ministries and agencies.
- **Ministry of Higher Education and Scientific Research:** Oversees AI education and research initiatives, including the establishment of new AI colleges and research programs.
- **Ministry of Communications:** Responsible for telecommunications and digital infrastructure policy, including the electronic signature system.
- **Communications and Media Commission (CMC):** Regulatory body overseeing telecommunications and digital service standards, including certification authorities for electronic signatures.

Implementation Status

Implementation varies across Iraq's regulatory instruments. The [Electronic Signature and Transactions Law](#), enacted in 2012, remained largely dormant for over a decade until September 2025 when PM al-Sudani approved the launch of Iraq's official electronic signature system. This milestone marked the practical activation of the law, enabling government agencies, businesses, and citizens to use legally valid electronic signatures. The system is now being rolled out across government institutions with plans for broader private sector adoption. The [National AI Strategy \(INSAIN\)](#) remains under active development. The Supreme Committee for AI has been conducting consultations and planning sessions since its August 2024 inaugural meeting. No final strategy document has been published yet, but preparatory work includes identifying priority sectors, governance mechanisms, and implementation timelines.

Future Developments

Iraq's AI governance framework is expected to evolve significantly in the coming years:

- **INSAIN Completion:** The National AI Strategy is expected to be finalized and formally adopted, providing dedicated policy guidance for AI development and deployment.
- **AI Education Expansion:** Two new AI colleges at the University of Baghdad are planned for the 2025-2026 academic year, creating domestic AI expertise and research capacity.
- **Digital Infrastructure Growth:** Continued expansion of the electronic signature system and related digital infrastructure will enable broader AI-enabled service adoption.
- **100 Digital Leaders Program:** Training initiative announced to develop digital leadership capacity across government and industry.
- **Sector-Specific Regulations:** As AI adoption grows, Iraq may develop sector-specific regulations for high-priority areas such as government services, healthcare, and finance.
- **Regional Cooperation:** Potential engagement with regional AI governance initiatives in the Arab world and broader Middle East.

International Context

Iraq's AI governance approach is developing within a global context of evolving AI regulation. While Iraq does not yet have comprehensive AI legislation like the [EU AI Act](#), its emerging framework shows awareness of international trends. The UNESCO AI ethics training conducted in Iraq in July 2024 reflects engagement with the [UNESCO Recommendation on the Ethics of Artificial Intelligence](#). Iraq's focus on human capital development and international best practices aligns with [OECD AI Principles](#) emphasis on human-centered AI. The Electronic Signature and Transactions Law draws from international models including the [UNCITRAL Model Law on](#)

[Electronic Signatures](#). As Iraq finalizes its National AI Strategy, alignment with international frameworks and regional approaches will likely be a key consideration, particularly given Iraq's interest in positioning itself as a regional AI leader.

Ireland — AI Regulatory Landscape Summary

Overview

Ireland's AI regulatory framework is composed of EU-level binding law, national strategic policy documents and operational guidance issued by supervisory authorities and sectoral bodies. The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) is the principal legal instrument that applies directly in Ireland and introduces a risk-based classification of AI systems with obligations for providers and deployers. At the national level, Ireland supplements the EU framework with strategic guidance, public-sector rules and supervisory guidance addressing data protection and cyber security.

Regulatory Instruments

- [AI – Here for Good: National Artificial Intelligence Strategy for Ireland](#) - Published national strategy (2021) setting out Ireland's vision to harness AI for economic growth and public good. Status: Enacted/Published. Type: Strategy / Policy.
- [AI – Here for Good: National AI Strategy Refresh \(2024\)](#) - Updated strategic priorities (2024) that refocus on implementation, skills, public trust and international cooperation. Status: Enacted/Published. Type: Strategy / Policy.
- [Interim Guidelines for Use of AI \(Public Service\)](#) - Short-term operational guidance for government departments and public bodies to manage AI adoption safely while longer-term policy and legislative measures are developed. Status: Enacted/Published. Type: Guideline / Operational.
- [Guidelines for the Responsible Use of AI in the Public Service](#) - More developed and comprehensive public service guidance emphasising governance, procurement controls, human oversight, transparency and DPIAs. Status: Enacted/Published. Type: Guideline / Operational.
- [Data Protection Commission Guidance on AI and Large Language Models](#) - Data protection focused guidance addressing lawful basis, transparency, data minimisation, model training datasets, DPIAs, and specific considerations for LLM deployments. Status: Enacted/Published. Type: Regulatory guidance.
- [National Cyber Security Centre: Cyber Security Guidance on Generative AI for Public Sector Bodies](#) - Practical cyber security mitigations and operational controls for generative AI use in public sector contexts. Status: Enacted/Published. Type: Technical guidance.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(EU AI Act\) \(applicable in Ireland as an EU Regulation\)](#) - EU regulation establishing binding obligations for AI systems across the EU, directly applicable in Ireland. Status: In force. Type: Supra-national binding regulation.
- [Statutory Instrument No. 366/2025 — Designation of National Competent Authorities and Single Point of Contact for AI Act implementation](#) - Legal designation of Irish authorities and a single point of contact to implement and enforce the EU AI Act domestically. Status: Enacted/Published. Type: Statutory Instrument / Administrative designation.
- [Regulation of Artificial Intelligence and Non-Personal Data Bill \(heads of bill / preparation stage\)](#) - Draft domestic legislation under preparation intended to address national governance of AI, non-personal data access and complementary measures to the EU AI Act. Status: Draft / Preparation. Type: Bill / Proposed legislation.

Key Themes and Priorities

Common themes across Ireland's AI regulations and guidance include a risk-based regulatory approach (derived from the EU AI Act), strong emphasis on data protection and privacy, robust cybersecurity expectations for models and infrastructure, transparency and human oversight requirements for systems that affect people, and a focus on enabling innovation through skills development and research support. Public trust, ethical deployment in government services, and clarity on procurement and accountability are recurring priorities in national guidance.

Governance Structure

Governance is shared across European and national bodies. The EU AI Act provides the legal backbone and creates obligations enforced via designated national competent authorities. In Ireland, the Data Protection Commission (DPC) plays a central role for data protection-related obligations; the National Cyber Security Centre (NCSC) issues security guidance for public-sector deployments; and SI No. 366/2025 formalises which national authorities will lead on conformity assessment, market surveillance and enforcement. Public-sector governance is reinforced by departmental AI leads and single points of contact for procurement and oversight.

Implementation Status

As of the date of this summary, the EU AI Act is in force and applicable across Ireland. The national strategy and its 2024 refresh have been published and inform policy priorities. The DPC and NCSC have published operational guidance documents that public bodies and private organisations are expected to consider in practice. The Statutory Instrument designating competent authorities is enacted, clarifying enforcement responsibilities. The domestic Regulation of Artificial Intelligence and Non-Personal Data Bill remains at the heads-of-bill or preparation stage and has not yet been enacted; it is a near-term item to watch for domestic measures complementing EU rules.

Future Developments

Key future developments include the final passage and content of the Regulation of Artificial Intelligence and Non-Personal Data Bill, further sectoral guidance and technical standards to operationalise the EU AI Act obligations, and ongoing enforcement guidance from the DPC and the designated national competent authorities. Additional guidance on conformity assessment, market registration and reporting procedures under the EU AI Act is expected. Ireland will also need to refine cross-border cooperation mechanisms with other Member States for market surveillance and enforcement.

International Context

Ireland's regulatory approach is closely aligned with EU law and EU-level policy. The country also seeks interoperability with international standards and promotes innovation-friendly measures consistent with transnational data flows. Irish guidance documents reference internationally accepted best practices in privacy, cybersecurity and AI governance while the national strategy emphasises international cooperation, research partnerships and adherence to EU obligations.

Relevant official and reference sources include the European Union legal repository and Irish national regulator websites. For further reading, consult the European Union's legal database (EUR-Lex), the Irish Data Protection Commission at <https://www.dataprotection.ie>, the National Cyber Security Centre at <https://www.ncsc.gov.ie>, and the Irish Statute Book at <http://www.irishstatutebook.ie>.

Israel — AI Regulatory Landscape Summary

Overview

Israel's AI regulatory landscape in 2025 is the product of deliberate policy choices that combine strategic state action to accelerate innovation with pragmatic, principles-based regulation and targeted legal guidance. Government Decision No. 212 (authorising the Ministry of Innovation, Science and Technology — MIST — to develop a national AI strategy) and Government Decision No. 173 (approving the National Program for Artificial Intelligence and allocating budget and implementation roadmaps) set the political and financial foundation for the national AI effort. Rather than immediately pursuing a single omnibus AI statute, authorities have relied on a mix of white papers, joint policy statements, ministerial legal opinions and regulator guidance to deliver clarity on high-priority legal and ethical questions (privacy, copyright, finance) while preserving regulatory flexibility.

Regulatory Instruments

- [Government Decision No. 212 – Program for the advancement of innovation, encouragement of high-tech sector growth and strengthening Israel's technological and scientific leadership \(authorized MIST to develop a national AI strategy\)](#) - Status: Passed. Type: Government decision / strategic mandate. Establishes mandate for MIST to coordinate development of a national AI strategy and to integrate AI into broader innovation policy.
- [Government Decision No. 173 – Adoption of the National Program for Artificial Intelligence / Strengthening Israel's technological leadership](#) - Status: Enacted/Published. Type: Government decision / national program. Approves the national AI program, budget authorisation, implementation roadmap and institutional responsibilities.
- [White Paper: Principles of Policy, Regulation and Ethics in Artificial Intelligence \(Ministry of Innovation, Science and Technology\)](#) - Status: Published for public consultation. Type: Policy white paper / consultative instrument. Sets out guiding principles (responsible innovation, risk-based regulation, transparency) and invites stakeholder comment on proposed approaches.
- [Israel's Policy on Artificial Intelligence Regulation and Ethics \(MIST and Ministry of Justice\) - 'Responsible Innovation' AI policy](#) - Status: Enacted/Published. Type: Joint policy statement. Articulates the Government's Responsible Innovation approach and operational priorities for coordination and ethics.
- [Office of Legal Counsel and Legislative Affairs \(Ministry of Justice\) opinion on the use of copyrighted works for machine-learning purposes](#) - Status: Enacted/Published. Type: Legal opinion. Provides interpretive guidance on copyright risks and licensing considerations when using copyrighted works in ML training datasets.
- [Interim report on AI regulation in the financial sector \(Office of Legal Counsel and Legislative Affairs, Ministry of Justice\)](#) - Status: Enacted/Published. Type: Sectoral report / interim guidance. Reviews AI-related risks in financial services and recommends safeguards and supervisory focus areas.
- [Privacy Protection Authority opinion / guidance on algorithmic processing and notification obligations \(automated decision-making guidance\)](#) - Status: Enacted/Published. Type: Regulator guidance. Clarifies obligations under Israel's privacy law for automated decision-making, documentation, transparency and PIAs.

Key Themes and Priorities

Across instruments, common themes include: promoting innovation and export-oriented high-tech growth; adopting a risk-based and proportionate regulatory stance; emphasising privacy and data-protection by design; clarifying IP implications for data and model training; advancing sectoral safeguards (notably in finance and

healthcare); and committing to iterative policy development through public consultation, pilot projects and sandboxes. Israeli policy prioritises practical legal certainty for startups and established firms while reserving the option to tighten oversight where systemic or individual harms are identified.

Governance Structure

Key actors and their functional roles include:

- Ministry of Innovation, Science and Technology (MIST) — overall strategy, funding, R&D priorities, public consultation leadership and coordination of cross-government AI activities.
- Ministry of Justice (Office of Legal Counsel and Legislative Affairs) — provides legal opinions, prepares sectoral reports, interprets existing law as applied to AI (IP, administrative law, consumer protection) and supports drafting of any future legislation.
- Privacy Protection Authority (PPA) — issues binding and interpretive guidance under privacy law, enforces data-protection obligations and clarifies automated decision-making and notification duties.
- Sectoral regulators (e.g., Bank of Israel and financial supervisors) — translate national guidance into supervisory expectations and impose sector-specific controls where needed.
- Executive decision-makers (Cabinet) — issue Government Decisions that provide budgetary authority and formal mandates (e.g., Decisions 212 and 173).

Implementation Status

The institutional foundations are in place: Government Decisions 212 and 173 have created a funded national program with a roadmap and MIST mandate. The White Paper and joint Responsible Innovation policy are published and have guided outreach and consultation. MOJ opinions and the PPA guidance have clarified legal issues in priority areas (copyright, finance, automated decision-making), and sectoral regulators have begun integrating those analyses into supervision and guidance. Many instruments remain non-binding policy or interpretive instruments; binding obligations today derive primarily from existing statutory frameworks (privacy law, consumer protection, sectoral regulation). Implementation is therefore mixed: strong strategic support and legal guidance, but no single binding AI statute as of 2025.

Future Developments

Expected near-term developments include further sector-specific rules (especially for finance and health), possible legislative initiatives to codify key obligations if risks materialise, wider use of regulatory sandboxes and standards adoption, and increased international alignment. Stakeholders should anticipate iterative tightening of oversight in areas where risk-outcomes are demonstrable and should prepare governance, documentation and privacy safeguards now.

International Context

Israel positions its regulatory approach to be interoperable with global frameworks. Government documents and MIST outreach reference international standard-setting bodies and comparator regimes; pragmatic alignment with the [OECD AI principles](#), ongoing developments in the [European Union \(AI Act\)](#) and ISO/IEC technical standards are relevant for exporters and multinational compliance. Israel's emphasis on "Responsible Innovation" and risk-based governance aims to lower friction for trade while enabling domestic regulatory autonomy.

In conclusion, Israel's AI regulatory landscape through 2025 is best characterised as strategic, consultative and sectorally-targeted: strong state support for AI development coupled with detailed legal and regulatory guidance on privacy, IP and high-risk sectors, and a willingness to evolve toward more formal regulation when evidence of harm warrants it. Organisations operating in Israel should prioritise privacy compliance, data licensing clarity,

algorithmic transparency measures and active engagement with MIST, MOJ and the PPA to remain aligned with the rapidly evolving national program.

External reference portals: [MIST](#), [Ministry of Justice](#), [Privacy Protection Authority](#).

Italy — AI Regulatory Landscape Summary

Overview

Italy's AI regulatory landscape is a composite of strategic plans, sectoral implementation tools, supervisory interventions by the data protection authority, draft technical guidance and a new national law enacted in 2025. The approach seeks to balance innovation, competitiveness and public-sector modernization with protection of fundamental rights, data privacy and procedural transparency. National documents are designed to align with European Union-level requirements, notably the GDPR and the EU AI Act, while addressing specific domestic priorities such as public administration digital transformation and national research capacity.

Regulatory Instruments

- [Programma Strategico per l'Intelligenza Artificiale \(Strategic Programme on Artificial Intelligence\) 2022-2024](#) - National strategic framework published to coordinate public funding, research priorities and initial governance structures. Status: Enacted/Published. Type: Strategic policy document.
- [Strategia Italiana per l'Intelligenza Artificiale 2024-2026 \(Italian Strategy for Artificial Intelligence 2024-2026\)](#) - Successor strategy refining priorities for the 2024–2026 period, including skills, research, regulatory readiness and public sector adoption. Status: Enacted/Published. Type: Strategic policy document.
- [Italia Digitale 2026 \(National Digital Strategy / Italy Digital 2026\)](#) - Broader national digital plan that places AI as an enabling technology, setting investment targets for infrastructure, cloud services and interoperability. Status: Enacted/Published. Type: National digital strategy.
- [Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026 \(Three-Year ICT Plan for the Public Administration\)](#) - Operational plan for digital transformation of public administration, addressing procurement, interoperability, cloud, data governance and controlled AI adoption. Status: Enacted/Published. Type: Implementation/operational plan.
- [Bozza - Linee guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione \(AgID draft guidelines on AI adoption in the PA\)](#) - Technical and governance guidance from AgID setting out lifecycle governance, conformity checks, procurement approaches and testing practices for AI systems in public bodies. Status: Draft. Type: Technical guidance (draft).
- [Provvedimento n.329 \(20 May 2024\) - Nota informativa su web scraping per finalità di addestramento di intelligenza artificiale generativa \(Garante per la protezione dei dati personali\)](#) - Supervisory note clarifying legal issues and safeguards when using web-scraped data for training generative AI models. Status: Enacted/Published. Type: Supervisory guidance / interpretative note.
- [Provvedimento 11 April 2023 - Misure cautelari e ordine temporaneo contro ChatGPT \(Garante per la protezione dei dati personali\)](#) - Temporarily ordered measures addressing data-protection concerns in a major generative AI service; set enforcement precedent. Status: Ended. Type: Supervisory order (temporary enforcement measure).
- [Disegno di legge n.1146 - Disposizioni e deleghe al Governo in materia di intelligenza artificiale \(Parliamentary bill on AI\)](#) - Parliamentary bill that guided legislative debate and provided delegations for executive implementing acts. Status: Passed (led to national law). Type: Parliamentary bill (legislative instrument).
- [Legge n.132 del 23 settembre 2025 - Disposizioni e deleghe al Governo in materia di intelligenza artificiale \(National Law on Artificial Intelligence\)](#) - National statute containing provisions and delegations to the

Government to issue implementing rules, create governance bodies and align domestic law with EU obligations. Status: Enacted/Published. Type: National law.

Key Themes and Priorities

Across instruments, common themes include: (1) risk-based governance and proportionality, mirroring EU approaches; (2) a strong emphasis on public-sector adoption, procurement, and interoperability; (3) protection of fundamental rights and privacy, driven by the Garante's supervisory activity; (4) investment in research, skills and industrial uptake; (5) transparency, accountability and human oversight of high-risk systems; and (6) reliance on implementing secondary measures and technical standards to operationalize strategic goals.

Governance Structure

Key national actors include the Agenzia per l'Italia Digitale (AgID) which leads technical and public-administration guidance ([AgID](#)), the Garante per la protezione dei dati personali which enforces privacy and data-protection rules ([Garante](#)), central ministries (notably the Ministry for Technological Innovation and Digital Transition and the Ministry of Economy/Research ministries), Parliament (which legislates), and the Presidency of the Council which coordinates policy. The 2025 law delegates powers to the Government to define technical rules, assign roles and create or empower national coordination bodies; these implementing acts will clarify the distribution of responsibilities and enforcement authority.

Implementation Status

As of the date of this summary, strategic plans and the three-year public-administration ICT plan are published and active. The Garante has issued binding and interpretative measures of practical significance (e.g., the 2023 temporary order and the 2024 web-scraping note). AgID's guidance remains at draft stage and awaits final adoption; it is widely referenced in procurement and pilot projects but has not yet acquired binding force. Legge n.132/2025 is enacted, but multiple implementing decrees, technical rules and institution-level procedures remain to be drafted and adopted by the Government and relevant agencies. Operational capacity building in ministries and public administrations is ongoing, and procurement practices are being adapted to incorporate AI-specific requirements.

Future Developments

Anticipated next steps include: issuance of implementing decrees and ministerial orders under Law No.132/2025; formal adoption of AgID's guidelines and sector-specific technical standards; expanded enforcement and guidance from the Garante on lawful training data practices; establishment or designation of a national AI coordinator/oversight entity; and alignment exercises to ensure domestic law coheres with the fully adopted EU AI Act and complementary European standards. Stakeholders should expect an intense period of regulatory drafting and stakeholder consultation in the months following the enactment of the 2025 law.

International Context

Italy's framework is explicitly EU-oriented: national instruments are designed to work alongside the GDPR and the EU AI Act. Italy also participates in international policy dialogues within the OECD, G7 and EU forums promoting interoperable rules, shared technical standards and cross-border enforcement cooperation. For EU-level texts and coordination, stakeholders should consult official EU resources such as the European Commission and EUR-Lex ([European Commission](#), [EUR-Lex](#)).

For practical compliance and implementation, public bodies and private-sector actors should monitor publication of implementing decrees under Legge n.132/2025, finalize adoption of AgID guidelines for administrative deployments, and follow the Garante's evolving supervisory practice on training data, transparency and rights of

data subjects. Italy's model centers on coordinated governance, incremental operationalization and close alignment with EU instruments while leveraging national plans to stimulate adoption and capacity building.

Japan — AI Regulatory Landscape Summary

Overview

Japan's AI regulatory framework is deliberately hybrid: a sequence of national strategies and principles (soft law) set high-level objectives, detailed practical guidance helps public and private actors operationalize those objectives, and statutory reforms — notably amendments to the Act on the Protection of Personal Information (APPI) and the 2025 Act on Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies (AI Promotion Act) — provide legal certainty on data protection and a statutory basis for coordinated R&D and implementation support. This layered approach reflects Japan's policy priorities: promoting innovation and economic diffusion of AI while maintaining a human-centric, trustworthy stance that protects individual rights and promotes international harmonization.

Regulatory Instruments

- [Artificial Intelligence Technology Strategy](#) - Foundational national strategy that outlines long-term objectives for AI technologies, emphasizing research investment, human resources, and public-private partnership. Status: Enacted/Published. Type: National strategy (soft law).
- [Draft AI R&D Guidelines for International Discussion](#) - Early technical and ethical guidance intended for international dialogue on best practices for R&D in AI, focusing on reproducibility, transparency, and collaborative research norms. Status: Enacted/Published (draft for discussion). Type: Guidelines (soft law / international-facing).
- [Social Principles of Human-Centric AI](#) - Core principles articulating human-centricity, safety, transparency and accountability for AI use across society; commonly referenced in procurement and policy documents. Status: Enacted/Published. Type: Principles (soft law).
- [AI Strategy 2019: AI for Everyone \(People, Industries, Regions and Governments\)](#) - Implementation-focused strategy aimed at broad diffusion of AI benefits across regions and industries, including workforce development and regional pilot programs. Status: Enacted/Published. Type: Strategy (soft law).
- [AI Utilization Guidelines \(Practical Reference for AI Utilization\)](#) - Practical reference offering checklists and operational guidance for organizations adopting AI, covering lifecycle management, risk assessment, and stakeholder communication. Status: Enacted/Published. Type: Practical guidance (soft law).
- [Contract Guidelines on Utilization of AI and Data](#) - Model contractual clauses and negotiation guidance covering data sharing, IP, liability, maintenance and model stewardship. Useful for public procurement and private contracting. Status: Enacted/Published. Type: Contractual guidance (soft law).
- [Amendment to the Act on the Protection of Personal Information \(APPI\)](#) - Legislative reform updating personal data protections, clarifying cross-border transfer rules, pseudonymization/de-identification standards and controller obligations for AI processing. Status: In force. Type: Statutory amendment (binding law).
- [AI Strategy 2021](#) - Updated national strategy that builds on 2019 priorities with expanded emphasis on data infrastructure, social implementation, and governance mechanisms. Status: Enacted/Published. Type: Strategy (soft law).
- [Act on Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies \(AI Promotion Act\)](#) - Statutory framework (2025) to coordinate R&D funding, create testbeds and data platforms, and institutionalize promotion measures for AI while preserving oversight. Status: In force. Type: Statutory Act (binding law).

Key Themes and Priorities

Common themes across Japan's instruments include: human-centricity and trust (safety, explainability, human oversight); promotion and diffusion of AI across regions, industries and the public sector; practical governance and contractual clarity to manage risk and encourage data sharing; data protection and de-identification under APPI; workforce development and research capacity building; and international alignment with OECD/G7 principles. Japan emphasizes enabling innovation through non-prescriptive guidance combined with targeted statutory action for coordination and funding.

Governance Structure

Primary domestic actors include: the Cabinet Office and the Council for Science, Technology and Innovation (CSTI) which steer national strategy and cross-ministerial coordination; the Ministry of Economy, Trade and Industry (METI) which focuses on industrial adoption, standards and business guidance; the Digital Agency which supports digital transformation and data infrastructure; the Personal Information Protection Commission (PPC) which enforces APPI and issues operational guidance on anonymization and cross-border transfers; and sectoral regulators (finance, health, transport) that translate general guidance into sector-specific requirements. Interagency councils and public-private councils are commonly used to implement strategy and allocate funding.

Implementation Status

Most strategies and guidance documents are published and serve as reference frameworks for procurement, funding, and corporate governance. The APPI amendments are in force and impacting data practices in AI development notably through strengthened rules on cross-border transfers and clearer requirements for pseudonymized data. The AI Promotion Act of 2025 provides a statutory engine for coordinated R&D investment, testbeds and data platforms; ministries are in the process of issuing implementing measures, funding calls and program schedules. Uptake of practical guidelines is progressing in the private sector and in public procurement, but effective implementation often depends on sectoral integration by regulators and the roll-out of concrete standards, certification schemes and procurement requirements.

Future Developments

Near-term priorities include: defining measurable standards or certification schemes for high-risk applications; clarifying liability and auditability expectations for complex models; expanding interoperable, privacy-preserving data platforms; and intensifying international cooperation on technical standards. The Government is expected to issue detailed implementing guidelines under the AI Promotion Act, align procurement rules with trustworthiness principles, and work with industry on voluntary codes and possible certification mechanisms.

International Context

Japan actively aligns with OECD, G7 and other international frameworks and promotes international discussion through its R&D guidelines. The country emphasizes interoperable, principle-based approaches rather than nationalistic regulatory divergence, seeking to contribute to global standards while preserving domestic flexibility for innovation and sectoral adaptation.

For further official information, see: [Cabinet Office / CSTI \(English\)](#), [Ministry of Economy, Trade and Industry \(METI\)](#), [Personal Information Protection Commission \(PPC\)](#), and [Digital Agency](#). These sites host strategy documents, guidelines and statutory texts or links to them.

Kazakhstan — AI Regulatory Landscape Summary

Overview

This detailed summary explains Kazakhstan's present AI regulatory framework, its chronology, major instruments, governance architecture and likely implementation trajectory. Between 2022 and 2025 Kazakhstan progressed from ministerial technical orders addressing data governance to national strategic concepts and finally to an enacted national Law on Artificial Intelligence accompanied by amendments to the Code of Administrative Offences. The combined package signals a move from fragmented technical regulation toward a unified, statute-based approach that pairs ambition for digital transformation with administrative enforcement tools.

Regulatory Instruments

- [Order of the Minister No. 385/NQ - On Approval of Requirements for Data Management \(Приказ Министра №385/НК «Об утверждении Требований по управлению данными»\)](#) - Ministerial order introduced detailed requirements for data management (technical and procedural measures). Status: Ended. Type: Ministerial order (secondary regulation / normative act).
- [Concept of Digital Transformation, ICT Industry Development and Cybersecurity for 2023–2029 \(Концепция цифровой трансформации, развития отрасли ИКТ и кибербезопасности на 2023–2029 годы\)](#) - High-level government concept defining national objectives for digital transformation, ICT sector growth and cybersecurity for the 2023–2029 period. Status: In force. Type: Strategic policy document.
- [Order of the Minister No. 90/NQ \(23 February 2024\) — On Amendments and Additions to Order No. 385/NQ \(О внесении изменений и дополнения в приказ Министра от 14.10.2022 №385/НК\)](#) - Ministerial amendments that modified the 385/NQ data management requirements. Status: Ended. Type: Ministerial amendment.
- [Concept for the Development of Artificial Intelligence for 2024–2029 \(Концепция развития искусственного интеллекта на 2024–2029 годы\)](#) - Focused national concept elaborating objectives, priority sectors, R&D and workforce measures for AI development over 2024–2029. Status: In force. Type: Strategic policy document.
- [Order of the Minister No. 691/NQ \(11 November 2024\) — On Recognition as Having Lost Force of Prior Orders No.385/NQ and No.90/NQ \(Приказ Министра №691/НК\)](#) - Formal revocation recognizing that earlier data management orders (385/NQ and 90/NQ) have lost legal force. Status: In force. Type: Ministerial order (repeal/recognition of loss of force).
- [Draft Law \(Bill\) 'On Artificial Intelligence' — parliamentary bill submitted/considered \(Проект Закона «Об искусственном интеллекте»\)](#) - Legislative draft that set out proposed statutory framework for AI (responsibilities, oversight and risk management). Status: Passed (moved through parliamentary consideration). Type: Legislative bill (now enacted as the Law on AI).
- [Law of the Republic of Kazakhstan on Amendments and Additions to the Code of Administrative Offences \(No. 232-VIII\) — related to AI/ digitization \(Закон РК о внесении изменений и дополнений в Кодекс об административных правонарушениях\)](#) - Enacted amendments introducing administrative offence categories, fines and related enforcement measures connected to AI and digitization obligations. Status: Enacted/Published. Type: Legislative amendment (КОАП).
- [Law of the Republic of Kazakhstan 'On Artificial Intelligence' \(Закон Республики Казахстан «Об искусственном интеллекте»\)](#) - National law establishing the legal framework for AI systems, obligations for developers/operators, compliance expectations and governance arrangements. Status: Enacted/Published. Type: Primary legislation.

Key Themes and Priorities

Across these instruments, several consistent priorities emerge: (1) enabling digital and AI industry growth while ensuring national cybersecurity; (2) clarifying data governance and secure data flows to facilitate AI development; (3) assigning responsibilities and administrative accountability for AI system providers and public deployers; (4) building national capacity, research and workforce skills to support AI adoption; and (5) harmonizing state procurement and public sector use of AI with transparency, human oversight and control. The two policy Concepts emphasize a long-term horizon (2023–2029 and 2024–2029) to cascade objectives into sectoral programs and investments. The Law and KOAP amendments translate many of those priorities into binding duties and sanctioning mechanisms.

Governance Structure

Legal and executive responsibilities are distributed across levels: Parliament legislates (the AI Law and KOAP amendments), the Government and relevant ministries issue strategic concepts and subordinate acts, and particular ministries or designated agencies will be tasked with implementation, supervision and enforcement. The ministerial orders demonstrate that operational rulemaking historically came from ministerial authority; the revocation of earlier orders (Order No. 691/NQ) indicates a transition toward implementing instruments consistent with the national Law and the Concepts. Sectoral regulators and local authorities will retain roles for industry-specific supervision, while central coordinating bodies named in the Concepts or the Law are expected to manage policy coordination, standards, and national AI initiatives.

Implementation Status

As of the retrieval date included below, the strategic Concepts are in force and provide the policy backbone. Ministerial technical orders 385/NQ and 90/NQ are no longer in force as of Order No. 691/NQ (11 November 2024). The Draft Law on Artificial Intelligence progressed through Parliament and the Law on Artificial Intelligence has been enacted and published; similarly, the amendments to the Code of Administrative Offences (No. 232-VIII) have been enacted and published to provide administrative enforcement mechanisms. The immediate implementation phase focuses on developing subordinate regulations, compliance guidance, and administrative processes (registration, reporting, auditing or certification, if required by the Law), and the operationalization of enforcement under the amended KOAP.

Future Developments

Expect extensive secondary rulemaking following the Law's enactment: (a) implementing regulations that define technical standards, data-sharing rules and procedural obligations; (b) agency guidance on risk classification, algorithmic impact assessments, transparency reporting and human oversight; (c) sectoral integration for health, transport, finance and public administration; and (d) enforcement guidance and administrative practice from agencies using KOAP penalties. Monitoring by stakeholders will focus on whether the Law mandates registration or audit regimes, how it treats high-risk systems, and how it balances innovation incentives with protective measures for individuals and critical infrastructure.

International Context

Kazakhstan's framework mirrors international trends in combining strategic national AI roadmaps with statutory commitments to oversight and administrative sanctions. It aligns conceptually with global priorities — cybersecurity, data governance, responsible deployment and promotion of domestic capability — while reflecting national institutional preferences for centralized coordination and administrative enforcement. International cooperation, interoperability of standards and cross-border data arrangements will become important as Kazakhstan operationalizes its AI regime.

Primary sources and portals for official publication include the national government and ministerial publication channels (see [government AI portal](#) and [official sources](#) as listed in the summary metadata). For implementation, stakeholders should track ministerial orders, implementing regulations and agency guidance issued after the Law's entry into force.

Retrieval metadata: retrievedAt: 2025-11-22T15:03:20.581Z; lastCheckedAt: 2025-11-22T15:03:20.581Z; lastUpdated: 2025-11-22T15:03:20.581Z.

Kenya — AI Regulatory Landscape Summary

Overview

This document provides a comprehensive overview of Kenya's AI regulatory framework as of November 22, 2025. The country's approach combines a published national strategy with standards development, media practice guidance and parliamentary initiatives. Kenya emphasizes a principles-first approach supported by technical standards, sectoral guidance for media, and legislative direction from Parliament. Implementation is multi-stakeholder and incremental: some instruments are enacted or published while others remain draft and consultative.

Regulatory Instruments

- [Kenya Robotics and Artificial Intelligence Society Bill 2023](#) - A private or civil-society led bill proposing governance, registration and oversight mechanisms for robotics and AI societies and practitioners. Status: Paused/Blocked. Type: Bill (private/civil-society initiative).
- [Information Technology — Artificial Intelligence \(AI\) — Code of Practice for AI Applications \(Draft DKS 3007:2024\) — Kenya Bureau of Standards](#) - A draft national standard and code of practice prepared by the Kenya Bureau of Standards (KEBS) that seeks to set technical and process-oriented requirements for AI development, testing, documentation, risk assessment and certification. Status: Draft (consultation). Type: National standard / code of practice.
- [Data Governance Guide for Media Practice in Kenya \(Media Council of Kenya draft\)](#) - Draft guidance aimed at journalists and media organizations covering responsible collection, storage, processing and sharing of personal and sensitive data in media practice. Status: Draft. Type: Sectoral guidance (media).
- [Media Guide on the Use of Artificial Intelligence in Kenya \(Media Council of Kenya draft\)](#) - Draft practical guidance for media organizations on use of synthetic content, automated decision tools, content labelling, provenance and verification. Status: Draft. Type: Sectoral guidance (media).
- [Media Handbook for Reporting on Artificial Intelligence in Kenya \(Media Council of Kenya draft\)](#) - Draft handbook aimed at improving journalistic reporting on AI topics, promoting accuracy, context and public interest coverage. Status: Draft. Type: Educational/sectoral handbook.
- [Guide on the Use of Social Media and the Internet for Media Practice in Kenya \(Media Council of Kenya draft\)](#) - Draft guidance dealing with online engagement, content moderation, verification and ethical social media use by journalists. Status: Draft. Type: Sectoral guidance (media / social media).
- [Kenya National Artificial Intelligence Strategy 2025–2030](#) - The national strategy document that sets priorities for AI research, infrastructure, standards adoption, public sector deployment, capacity building and international cooperation. Status: Enacted/Published. Type: National strategy / policy.
- [Motion on the Formulation of a Regulatory Framework on Artificial Intelligence \(National Assembly motion\)](#) - A parliamentary motion that was passed and requests formulation of a comprehensive regulatory framework, often prompting committee review and potential draft legislation. Status: Passed (motion). Type: Parliamentary motion (legislative direction).

Key Themes and Priorities

Across the instruments the following themes predominate: data governance and privacy; risk-based oversight for high-impact systems; media integrity, provenance and labelling of synthetic content; standards and technical

interoperability; capacity building and inclusion; and promotion of research and innovation, including sandboxes and testing environments. The national strategy frames these priorities and asks sector bodies to operationalize them using standards, guidance and, where necessary, legislative measures.

Governance Structure

Primary actors include the Ministry of ICT and Digital Economy (policy leadership), the Kenya Bureau of Standards (KEBS) for technical standards, the Media Council of Kenya (professional regulation for media practice), the Office of the Data Protection Commissioner (data privacy oversight), and Parliament (law-making and oversight). Other stakeholders include research institutions, the private sector, civil society and international partners. Coordination is currently achieved through the national strategy and inter-agency consultations rather than through a single dedicated AI regulator.

Implementation Status

The Kenya National Artificial Intelligence Strategy 2025–2030 is published and serves as the central policy anchor. KEBS' DKS 3007:2024 remains at draft and consultation stage and is likely to influence procurement, certification and technical compliance once finalized. The Media Council of Kenya's suite of drafts are consultative and aimed at bringing journalistic practice into alignment with AI-era risks; they are non-binding unless adopted as part of regulatory or professional standards. The Kenya Robotics and Artificial Intelligence Society Bill 2023 is paused or blocked and has not progressed to enactment. The National Assembly motion is a significant political signal but does not itself create binding obligations; it is likely to lead to committee work or draft legislation. Overall, enforcement today relies on existing statutes (for example, the Data Protection Act) and professional disciplinary mechanisms, with new, dedicated AI enforcement mechanisms still in formation.

Future Developments

Near-term expectations include KEBS finalizing its AI code of practice, the Media Council consolidating some draft guidance into formal advisories or revamped professional rules, and Parliament following up the motion with committee inquiries or proposed legislation. There is a credible prospect of a consolidated regulatory proposal or sectoral statutes in the medium term. Kenya is also expected to deepen international cooperation on standards and to pilot regulatory sandboxes to enable controlled innovation. Stakeholders should monitor consultations and engage to shape practical, risk-based rules.

International Context

Kenya's documents reference international principles and standards and show intent to align with global frameworks such as OECD principles, UNESCO recommendations, and ongoing ISO efforts. Kenya's approach—using national strategy, standards and sectoral guidance—mirrors international practice in jurisdictions that prefer incremental harmonization before a single omnibus AI law. This pathway supports interoperability with regional African frameworks and global trade partners while enabling local capacity building.

Official and reference links: [Ministry of ICT and Digital Economy](#), [Kenya Bureau of Standards \(KEBS\)](#), [Media Council of Kenya](#), [Office of the Data Protection Commissioner](#), [National Assembly of Kenya](#).

Latvia — AI Regulatory Landscape Summary

Overview

Latvia has developed a coherent, multi-layered regulatory and policy framework for artificial intelligence that combines strategic guidance, targeted legislation, and institutional creation to support AI development while protecting key public interests. The framework is anchored by national strategies and guidelines that prioritise digital transformation and AI adoption, supported by an informative report that served as an evidence base for lawmaking. Recent legislative steps include two principal laws enacted in 2025—the [Law on the Development of Artificial Intelligence \(Mākslīgā intelekta attīstības likums\)](#) and the [Law on the Latvian Artificial Intelligence Centre \(Mākslīgā intelekta centra likums\)](#)—together creating a statutory foundation for a national AI governance ecosystem. At the same time, Latvia has introduced precise legal limits on misuse of AI for electoral manipulation via amendments to the Criminal Law and the Pre-election Agitation Law.

Regulatory Instruments

- [Developing Artificial Intelligence Solutions \(National AI Strategy\)](#) - National strategy document setting strategic objectives, priorities for research, workforce development, public sector adoption and international cooperation. Status: In force. Type: Strategic policy/roadmap.
- [Digital Transformation Guidelines 2021–2027 \(Digitālās transformācijas pamatnostādnes 2021.–2027.\)](#) - Multi-year guidelines laying out digital public administration modernization, interoperability, e-services expansion and foundational digital infrastructure that supports AI deployment. Status: In force. Type: Policy guidance.
- [Informative Report 'On the Development of Artificial Intelligence Solutions' \(Informatīvais ziņojums 'Par mākslīgā intelekta risinājumu attīstību'\)](#) - Analytical report compiling use cases, risk assessments and recommended interventions; used as a government reference in legislative drafting. Status: Enacted/Published. Type: Report/evidence base.
- [Amendments to the Criminal Law \(Article 90.1\) — criminalising use of deepfake technology to influence elections](#) - Targeted criminal law amendment creating an offence for deployment of synthetic media or deepfakes intended to alter electoral outcomes, providing criminal penalties and investigative pathways. Status: In force. Type: Penal provision.
- [Amendments to the Pre-election Agitation Law regulating use of AI in campaigning \(Grozījumi Priekšvēlēšanu aģitācijas likumā\)](#) - Adjusts electoral law to require transparency and limit undisclosed AI generated campaign materials; sets administrative sanctions and obligations for platforms and campaign actors. Status: In force. Type: Electoral regulation.
- [Law on the Development of Artificial Intelligence \(Mākslīgā intelekta attīstības likums\)](#) - Primary legislative instrument establishing objectives, coordination mechanisms, funding measures, duties for public bodies and a legal framework to support trustworthy AI development. Status: In force. Type: Primary legislation.
- [Law on the Latvian Artificial Intelligence Centre \(Mākslīgā intelekta centra likums\)](#) - Establishes the AI Centre as a central agency for implementation, coordination, research support, standards guidance and operational programmes to accelerate AI uptake. Status: In force. Type: Institutional/administrative law.
- [National Data Governance Strategy \(Nacionālā datu pārvaldības stratēģija\) - \(in development\)](#) - Draft strategy focused on improving data accessibility, quality, sharing frameworks and governance safeguards that underpin public interest AI uses. Status: Draft (in development). Type: Strategy/draft regulation.

Key Themes and Priorities

Across instruments, common priorities emerge: enablement of AI for public sector modernization and economic competitiveness; institution building and coordination through a national AI Centre; responsible use of AI guided by ethical principles and data governance; and targeted legal safeguards in areas posing acute social risk — notably electoral integrity and malicious synthetic media. Latvia's approach mixes soft law (strategies, guidelines, reports) with hard law (new statutes and penal amendments) to both promote uptake and set clear prohibitions and duties.

Governance Structure

Governance is distributed among ministries responsible for digital transformation, justice and economic development, with statutory roles for the new AI Centre as the operational hub. Supervisory and enforcement roles are shared with independent agencies such as the Data State Inspectorate (for data protection matters), competition and consumer authorities (where AI affects markets or consumers), and law enforcement for criminal provisions. Parliament retains legislative oversight and budgetary control for funding the Centre and programme measures.

Implementation Status

Most strategic instruments are active and in force; the AI Centre and the AI development law enacted in 2025 require operationalisation — recruitment, budget allocation, rulemaking and standard setting are ongoing implementation tasks. The criminal and electoral amendments are in force and provide immediate enforcement tools; implementation requires guidance documents, enforcement protocols, cooperation agreements with platforms and investigative capacity for synthetic media forensics. The National Data Governance Strategy remains in draft form and is a critical next step for enabling data access frameworks and public data infrastructures that the AI Centre will rely on.

Future Developments

Expected near-term developments include final adoption of the National Data Governance Strategy, secondary legislation and regulations under the AI development law (including funding rules, certification or conformity assessment schemes, and transparency/reporting requirements), and establishment of memoranda of understanding with sectoral regulators. Latvia is also likely to develop guidance on labeling of AI-generated content in non-electoral contexts and interoperability standards to align with EU instrumentation such as the prospective EU AI Act. Ongoing capacity building — legal, technical and forensic — will be required to make criminal and electoral safeguards effective.

International Context

Latvia's framework is explicitly designed to align with European Union priorities: interoperability with EU digital and AI policy, adherence to EU data protection baseline (GDPR), and readiness to implement or complement EU-level regulatory instruments. The combination of national institutional capacity (the AI Centre) and targeted national laws positions Latvia to both participate in EU policy implementation and address domestic risks quickly. For further reference and official publications consult the government portals such as [Cabinet of Ministers of Latvia](#) and the official legal publication [Latvijas Vēstnesis](#), and the individual regulation pages linked above.

Sources: national strategy and guidelines, the published informative report, enacted legislative texts and drafts, and official government portals that publish laws and policy materials. For the consolidated list of instruments referenced here see the national regulations index and the AI Centre's forthcoming implementation guidance.

Lithuania — AI Regulatory Landscape Summary

Overview

Lithuania's AI regulatory framework is a layered, pragmatic mix of strategic guidance, actionable planning, parliamentary direction for public use, and targeted statutory amendments to harmonise domestic law with European Union AI obligations. The framework's principal goals are to accelerate safe AI adoption, support research and commercialisation, ensure public-sector trustworthiness and to prepare national law and institutions for implementation of the EU AI Act. The core national instruments are the [Lithuanian Artificial Intelligence Strategy: A Vision of the Future](#), the [Action Plan for the Development of Artificial Intelligence Technologies in Lithuania 2023–2026](#), the [Seimas Resolution on the Use of Artificial Intelligence Technologies in the Public Sector](#), a process updating the national strategy through the [National AI Strategy update / National AI Governance Forum \(strategy review process\)](#), and two sets of legislative amendments: [Amendments to the Law on Technology and Innovation](#) and [Amendments to the Law on Information Society Services](#).

Regulatory Instruments

- [Lithuanian Artificial Intelligence Strategy: A Vision of the Future](#) - Enacted/Published. Type: National strategy document. Description: Sets long-term vision, strategic objectives, priority sectors, and cross-cutting principles (human-centric AI, ethical considerations, skills and R&D). Status: Foundational policy guiding subsequent measures.
- [Action Plan for the Development of Artificial Intelligence Technologies in Lithuania 2023–2026](#) - Enacted/Published. Type: Multi-year implementation plan. Description: Operationalises the Strategy with concrete measures, timelines, responsible ministries/agencies, funding priorities and pilot initiatives (sandboxes, capacity-building, data access measures). Status: Active (2023–2026 timeframe) and driving implementation activity.
- [Seimas Resolution on the Use of Artificial Intelligence Technologies in the Public Sector](#) - Passed. Type: Parliamentary resolution (non-statutory guidance with high political weight). Description: Provides binding intent and expectations for public bodies on procurement, risk assessment, transparency, algorithmic impact assessments and protection of fundamental rights in government AI use. Status: Adopted and informing public-sector practice.
- [National AI Strategy update / National AI Governance Forum \(strategy review process\)](#) - Under review. Type: Strategy refresh / consultative governance process. Description: Formal review and update mechanism to recalibrate national priorities, integrate lessons from initial implementation and align with final EU AI Act provisions. Status: Ongoing review and stakeholder consultation.
- [Amendments to the Law on Technology and Innovation \(measures to implement EU AI Act / accelerate AI development\)](#) - Passed. Type: Statutory amendments. Description: Introduce measures to enable innovation (e.g., sandbox regimes, R&D incentives), create legal hooks for compliance obligations and prepare enforcement mechanisms to align with EU AI Act obligations for high-risk systems. Status: Adopted into national law; implementation delegated to ministries/agencies.
- [Amendments to the Law on Information Society Services \(measures to implement EU AI Act / accelerate AI development\)](#) - Passed. Type: Statutory amendments. Description: Adjust information-society rules to cover AI service providers, transparency obligations for algorithmic outputs, reporting duties and cross-border service considerations consistent with EU-level regulation. Status: Adopted into national law; expected to interact with sectoral supervision.

Key Themes and Priorities

Common themes across Lithuania's instruments are: (1) a risk-based approach that differentiates by use-case and context; (2) enabling innovation through sandboxes, public funding and streamlined R&D support; (3) public-sector leadership combined with safeguards (impact assessments, procurement requirements, transparency and human oversight); (4) capacity building—skills development, research infrastructure and talent pipelines; (5) preparing national law and supervision for alignment with the EU AI Act; and (6) international cooperation and standards alignment. These priorities reflect dual goals: to make Lithuania an attractive place for AI development while protecting citizens' rights when AI systems are used by the state or in sensitive domains.

Governance Structure

Governance responsibility is shared across national ministries, parliamentary bodies and independent regulators. The Ministry of Economy and Innovation is the primary coordinator for industry-facing measures and the Action Plan. The Seimas (parliament) provides high-level direction and oversight through resolutions and legislation. Sectoral regulators and the national data protection authority are assigned supervisory and enforcement roles, especially where privacy, data rights or high-risk systems intersect with existing regulatory remits. Cross-ministerial coordination and a national governance forum/stakeholder platform are used to update the strategy and to align administrative action with legislative mandates.

Implementation Status

Implementation is in active progress: the Strategy and Action Plan are in the execution phase for the 2023–2026 cycle; the Seimas Resolution has been passed and incorporated into public-sector guidance; and the two statutory amendment packages have been passed to ensure domestic rules are consistent with the EU AI Act and supportive of innovation. The strategy update and governance forum are working to refine priorities and produce implementing guidance. Authorities are developing secondary instruments — guidance documents, procurement checklists, sandbox procedures and supervisory plans — to make the statutory and strategic objectives operational. Resourcing remains an implementation challenge, particularly for supervisory bodies expected to enforce EU-style obligations.

Future Developments

Near-term developments to monitor include: publication of detailed implementing regulations and guidance that operationalise the statutory amendments; supervisory frameworks and enforcement roadmaps from sectoral regulators and the national data protection authority; output from the National AI Governance Forum and the updated national AI strategy; and the degree to which sandboxes, pilot projects and public-sector procurements proceed under the adopted Seimas Resolution. As EU-level implementing measures and standards for the AI Act continue to emerge, Lithuania is expected to align domestic technical and procedural requirements accordingly.

International Context

Lithuania positions its domestic framework to be coherent with EU policy and law. The national instruments explicitly anticipate application of the EU AI Act and are constructed to translate EU obligations into Lithuanian administrative and legal practice. Lithuania also engages with international standardisation and governance initiatives to ensure interoperability, cross-border compliance and attraction of international investment. For a consolidated view of EU-level AI policy, see the European Commission's AI policy overview: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> and for national materials consult the Lithuanian government AI portal: [https://\[government AI portal\]](https://[government AI portal]).

Overall, Lithuania's AI regulatory landscape blends ambition for technological growth with attention to legal alignment, public trust and rights protection. Stakeholders should track implementing guidance, supervisory

planning and the National AI Governance Forum outputs to understand practical compliance expectations and opportunities for engagement.

Luxembourg — AI Regulatory Landscape Summary

Overview

Luxembourg's AI regulatory landscape as of 2025 is a deliberate mix of EU-led regulatory compliance and national strategic planning. The country implements the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) as its primary legal backbone for AI risk management, obligations, prohibited practices, and enforcement. At the same time Luxembourg has published strategic policy instruments — including "Artificial Intelligence: A Strategic Vision for Luxembourg" and a National Artificial Intelligence Strategy embedded within the cross-cutting national roadmap "Accelerating Digital Sovereignty 2030" — that align AI policy with national priorities of digital sovereignty, economic innovation, public-sector modernization, and skills development. A National Data Strategy designed to dovetail with AI and quantum policies reinforces the central role of data governance. Sector-specific guidance such as the [KI Kompass — Strategic framework / guidelines for the use of artificial intelligence in Luxembourg schools](#) (under review) shows a practical orientation toward safe public-sector deployment.

Regulatory Instruments

- [Artificial Intelligence: A Strategic Vision for Luxembourg](#) - Strategic policy document setting long-term objectives for AI adoption, research, skills, and governance. Status: Enacted/Published. Type: National strategy/vision document.
- [National Artificial Intelligence Strategy \(part of 'Accelerating Digital Sovereignty 2030'\)](#) - Operational national strategy integrated into the broader digital sovereignty agenda; addresses implementation priorities, coordination mechanisms, investment and skills. Status: Enacted/Published. Type: National strategy embedded in a cross-sector roadmap.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act](#) - The EU-level regulation establishing a risk-based, horizontal legal framework for the design, development, and deployment of AI systems across Member States. Status: In force. Type: Supranational regulation with direct effect in Member States.
- [Law of 20 December 2024 on implementing rules and penalties related to the EU Artificial Intelligence Act](#) - National implementing statute clarifying Member State discretionary measures under the EU AI Act, specifying national competent authorities, enforcement powers and penalty regimes. Status: Enacted/Published. Type: National implementing legislation and sanctioning framework.
- [National Data Strategy \(aligned with the national AI and quantum strategies — 'Accelerating Digital Sovereignty 2030'\)](#) - Cross-cutting national data policy that addresses data governance, access, reuse, and infrastructure in support of AI and digital sovereignty goals. Status: Enacted/Published. Type: National strategy (data policy).
- [KI Kompass — Strategic framework / guidelines for the use of artificial intelligence in Luxembourg schools](#) - Sectoral guidance aimed at schools and educational authorities to steer adoption of AI in education in a rights-respecting and pedagogically sound manner. Status: Under review. Type: Sectoral guidance/framework.

Key Themes and Priorities

Several recurring themes run across Luxembourg's AI regulatory corpus: first, strict alignment with EU law and standards (notably the EU AI Act and GDPR) to ensure legal coherence and cross-border interoperability; second, an emphasis on digital sovereignty, which frames AI and data initiatives as critical components of national resilience and competitiveness; third, protection of fundamental rights and privacy, where the CNPD's role and GDPR remain central; fourth, promotion of innovation through research, sandboxes and targeted investment; and

fifth, sectoral pragmatism — producing practical guidance where national authorities can support implementation (for example, the KI Kompass for education).

Governance Structure

Governance is coordinated across ministerial portfolios and independent oversight bodies. The national implementing law identifies one or more national competent authorities responsible for enforcing the EU AI Act at the domestic level and for cooperating with EU supervisory networks. The National Commission for Data Protection (CNPDP) retains primary competency on data protection matters that intersect with AI deployment. Ministries responsible for digital transformation, the economy, education, and research coordinate strategic policy, funding, and operational deployment. Research institutions and public-private partnerships underpin innovation and workforce development. Luxembourg's governance model emphasizes close coordination between strategy-setting ministries and operational regulators to translate EU obligations into actionable domestic rules.

Implementation Status

By late 2025 Luxembourg had: (1) published strategic documents (Strategic Vision; National AI Strategy integrated into Accelerating Digital Sovereignty 2030; National Data Strategy) to establish policy direction and investment priorities; (2) adopted national implementing legislation (Law of 20 December 2024) to give domestic effect to Member State-discretionary elements of the EU AI Act and to set penalty regimes and administrative procedures; and (3) begun sectoral roll-out and guidance development (e.g., KI Kompass under review) to support public institutions. Operationalization activities such as national guidance on conformity assessment, provider obligations, market surveillance, enforcement protocols and capacity building are ongoing priorities. Authorities are focusing on building administrative capacity to classify systems by risk level, to oversee high-risk systems, and to coordinate cross-border enforcement as required by the EU AI Act.

Future Developments

Expected near-term developments include detailed national guidance for regulated entities, formal designation and staffing of national competent authorities for AI oversight, publication of sectoral guidance and educational materials, establishment or expansion of testing/sandbox environments, and cross-border coordination mechanisms with EU supervisory networks. Enforcement practice and interpretative guidance will evolve as authorities apply the risk-based rules in real-world contexts. Luxembourg is also likely to refine data governance implementations to operationalize the National Data Strategy in ways that support safe AI development while preserving privacy and national digital sovereignty objectives.

International Context

Luxembourg's approach is firmly anchored in EU law and institutions. The EU AI Act (see the official text at <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>) and the GDPR remain the primary international-legal reference points. Luxembourg also aligns its national strategies with EU-wide initiatives on data governance and digital sovereignty and participates in multilateral dialogues on trustworthy AI. For practical guidance on privacy and data impacts, the CNPDP provides interpretation and oversight (see <https://cnpdp.public.lu>). In short, Luxembourg pursues national policy objectives while seeking interoperability and harmonization across the EU and relevant international fora.

For further reference and official materials consult national government portals and the EU legislative text: <https://gouvernement.lu>, [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act](#), and the CNPD site at <https://cnpd.public.lu>.

Malaysia — AI Regulatory Landscape Summary

Overview

Malaysia's AI regulatory framework is intentionally hybrid: statutory laws, sectoral supervisory guidance, national strategies and operational institutions combine to reduce risk while enabling adoption. The first phase (roughly 2020–2024) focused on strategy and capability-building (the Malaysia Cyber Security Strategy 2020–2024, MyDIGITAL, and the Malaysia National AI Roadmap 2021–2025). The second phase (from 2024 onward) emphasizes operational governance and oversight, with new instruments (Cyber Security Act 2024; Personal Data Protection (Amendment) Act 2024), institutional anchors (the National Artificial Intelligence Office — NAIIO), and practical enabling tools (AI Sandbox 2024, AI Talent Roadmap 2024–2030, MAIC and MY AI NEXUS).

This combination reflects three parallel priorities: (1) unlock economic and public-service value through deliberate adoption and pilot-testing; (2) manage systemic risk via updated data protection, cybersecurity and sectoral risk rules; and (3) build human capital and public literacy to sustain long-run adoption.

Regulatory Instruments

- [Personal Data Protection Act 2010 \(PDPA\)](#) - The foundational data privacy statute that governs personal data processing by private-sector actors. (Status: Changed; Type: Primary legislation)
- [Personal Data Protection \(Amendment\) Act 2024](#) - Modernizes PDPA provisions to address algorithmic processing, cross-border transfers and stronger enforcement; aligns data protection obligations with AI uses. (Status: In force; Type: Primary legislation / amendment)
- [Malaysia Cyber Security Strategy 2020–2024 \(MCSS\)](#) - A time-bound national strategy that informed capacity-building and resilience efforts. (Status: Ended; Type: Strategy)
- [Malaysia Digital Economy Blueprint \(MyDIGITAL\)](#) - National blueprint for digital transformation and economic adoption of digital technologies, including AI infrastructure and incentives. (Status: In force; Type: National policy)
- [Malaysia National Artificial Intelligence Roadmap 2021-2025 \(AI-RMAP\)](#) - Early roadmap setting priorities (research, pilots, sector focus); many roadmap pilots have transitioned to operational programmes. (Status: Ended; Type: Roadmap)
- [National Artificial Intelligence Office \(NAIO\)](#) - Central coordinating body for AI policy, responsible for cross-sector coordination and delivery of the AI Technology Action Plan 2026–2030. (Status: In force; Type: Institutional)
- [AI Sandbox 2024 \(National AI sandbox pilot programme\)](#) - Pilot sandbox to allow controlled experimentation, regulatory collaboration and data-access arrangements for innovators. (Status: Enacted/Published; Type: Pilot / programme)
- [AI Talent Roadmap for Malaysia 2024–2030](#) - National plan to build AI skills across industry and public sector, with training pipelines and incentives. (Status: Enacted/Published; Type: Strategy / workforce plan)
- [AI untuk Rakyat \(AI literacy / public self-learning programme\)](#) - Public literacy initiative to raise citizen understanding of AI and facilitate safer interactions with AI-driven services. (Status: Enacted/Published; Type: Public programme)
- [Malaysia Artificial Intelligence Consortium \(MAIC\)](#) - Multi-stakeholder consortium to coordinate R&D, industry standards and shared infrastructure. (Status: In force; Type: Consortium / partnership)

- [Malaysia Artificial Intelligence Nexus \(MY AI NEXUS\) 2024](#) - National initiative to connect private innovators, government projects and academic research for deployment and knowledge-sharing. (Status: Enacted/Published; Type: Initiative / platform)
- [Cyber Security Act 2024](#) - New statutory framework strengthening national cyber resilience, incident reporting and powers relevant to critical information infrastructure and AI-related cyber risk. (Status: In force; Type: Primary legislation)
- [Bank Negara Malaysia — Policy Document on Risk Management in Technology \(RMiT\) \(updated\)](#) - Prudential expectations for financial institutions on technology risk, third-party outsourcing and AI model risk management. (Status: In force; Type: Regulator policy / prudential standard)
- [Securities Commission Malaysia — Guidelines on Technology Risk Management \(GTRM\) \(revised\)](#) - Revised expectations for capital-markets intermediaries on technology risk governance and operational resilience, including AI systems. (Status: Enacted/Published; Type: Regulator guidance)
- [National Guidelines on AI Governance & Ethics \(AIGE\)](#) - National ethics and governance guidance outlining principles and recommended controls for public- and private-sector AI deployments. (Status: Enacted/Published; Type: Non-binding guidance)
- [AI Technology Action Plan 2026–2030 \(planned / NAIO deliverable\)](#) - Proposed NAIO roadmap to operationalize regulation, standards, procurement and sectoral adoption in the next five-year cycle. (Status: Proposed / planned; Type: Planned action plan)

Key Themes and Priorities

Several persistent themes cut across Malaysia's AI instruments: data protection and responsible data flows; cybersecurity and resilience; sectoral risk management; enablement through sandboxes and talent development; and multi-stakeholder coordination. The PDPA amendment and ethics guidance balance enabling innovation with stronger individual rights and obligations on deployers. Financial and capital markets regulators emphasize model governance and third-party risk, requiring documented controls and oversight. The combined emphasis on sandboxes, MAIC and MY AI NEXUS shows a priority to accelerate experimentation while maintaining oversight.

Governance Structure

Governance is distributed but coordinated. NAIO provides central coordination and will deliver the AI Technology Action Plan 2026–2030. Sectoral regulators (Bank Negara Malaysia, Securities Commission Malaysia) maintain supervisory authority over regulated firms and issue binding prudential rules and guidance (RMiT, GTRM). MAIC and MY AI NEXUS are industry–academia platforms for standards, research and capability sharing, while the AI Sandbox and national literacy programmes operationalize testing and public engagement. The Attorney-General's Chambers and relevant ministries retain statutory and enforcement roles for laws like PDPA and the Cyber Security Act.

Implementation Status

Implementation is mixed but progressing. Legal updates (Cyber Security Act 2024; PDPA Amendment 2024) and sectoral guidance (RMiT, GTRM) are in force and require compliance by covered entities. NAIO and MAIC are active and enabling programmes (AI Sandbox, AI Talent Roadmap, MY AI NEXUS) are published and entering operational phases. The earlier national strategies and the AI-RMAP have informed programmatic choices; some pilot activities have matured into permanent mechanisms. Key operational gaps remain in cross-agency operational standards, unified data-sharing frameworks and certified technical standards for high-risk AI systems, which the upcoming AI Technology Action Plan intends to address.

Future Developments

Near-term priorities include the NAIIO-led AI Technology Action Plan 2026–2030 (planned), more detailed sectoral guidance around high-risk AI use-cases, and standard-setting for data access and model validation. Expect increased supervisory scrutiny in financial and critical-infrastructure sectors and further development of sandboxes and procurement rules that embed governance requirements. International interoperability (cross-border data transfer rules, standards alignment) will be a focus as Malaysia pursues trade and digital cooperation. Stakeholder engagement and workforce scaling (AI Talent Roadmap delivery) will be essential to realize adoption goals.

International Context

Malaysia's approach is broadly aligned with global principles (risk-based regulation, proportionality, human-centric AI) and with regional initiatives in ASEAN. The mix of national strategies, non-binding ethics guidance and sectoral prudential rules mirrors approaches elsewhere that balance enabling innovation and protecting fundamental rights. Malaysia is likely to prioritize pragmatic alignment — e.g., adopting international technical standards where useful — while retaining domestic controls on data, national security and critical infrastructure. Readers can monitor NAIIO publications and the government's central portal for up-to-date materials: [government AI portal](#).

Overall, Malaysia's AI regulatory landscape in 2025 is characterized by active operationalization: legal foundations have been modernized, sectoral supervisors have strengthened expectations, and national coordination and enabling instruments are being scaled to support a second phase of adoption and governance.

Maldives — AI Regulatory Landscape Summary

Overview

The Republic of Maldives is actively developing its artificial intelligence governance framework as part of broader digital transformation efforts. As a Small Island Developing State (SIDS) comprising nearly 1,200 islands across the Indian Ocean, the Maldives faces unique challenges in deploying AI technologies while ensuring connectivity and equitable access across its dispersed population. The government's approach combines strategic national planning through the draft National AI Masterplan 2025-2035 with foundational regulatory instruments governing telecommunications and data protection. This framework aims to harness AI for economic diversification beyond tourism, improve public service delivery to remote islands, and enhance climate resilience while protecting citizen rights and fostering responsible innovation. Key regulatory agencies including the [Communications Authority of Maldives \(CAM\)](#) and the [Ministry of Environment, Climate Change and Technology](#) lead the development and implementation of policies governing AI and related technologies. The Maldives participates in international initiatives including UNESCO's AI readiness assessments and UN ESCAP consultations on data protection, positioning the nation within global conversations on responsible AI governance.

Regulatory Instruments

- [Maldives Telecommunications Act 2015](#) - Foundational legislation establishing the regulatory framework for telecommunications services, spectrum management, and infrastructure licensing. Administered by the Communications Authority of Maldives, this Act ensures reliable connectivity infrastructure essential for AI deployment across the islands.
- [Privacy and Personal Data Protection Bill](#) - Draft comprehensive data protection legislation released for public consultation in May 2023. The bill establishes data subject rights, controller obligations, and enforcement mechanisms aligned with international standards. When enacted, it will significantly strengthen the regulatory foundation for responsible AI deployment.
- [National AI Masterplan 2025-2035](#) - Strategic document setting the vision for AI adoption across government, private sector, and society. The masterplan addresses infrastructure development, skills building, ethical principles, and sector-specific applications in tourism, fisheries, healthcare, and public services.
- [UNESCO AI Readiness Assessment Report](#) - Baseline assessment of the Maldives' preparedness for AI adoption across policy, infrastructure, skills, and institutional dimensions. The findings inform government prioritization and investment decisions for advancing the national AI agenda.

Key Themes and Priorities

The Maldives' AI governance framework reflects several interconnected priorities shaped by the nation's unique circumstances and development aspirations:

- **Economic Diversification:** Leveraging AI to reduce dependence on tourism and develop new sectors including fisheries optimization, financial services, and creative industries.
- **Inclusive Digital Development:** Ensuring AI benefits reach all citizens across dispersed atolls, addressing the digital divide between the capital Male and remote islands.
- **Climate Resilience:** Applying AI technologies to address existential climate challenges including sea level rise monitoring, disaster early warning, and sustainable resource management.

- **Ethical AI Principles:** Embedding transparency, fairness, accountability, and human oversight in AI systems deployed in the Maldives.
- **Data Protection:** Strengthening personal data protections to build citizen trust and enable responsible data-driven innovation.
- **Infrastructure Development:** Expanding digital connectivity and computing capacity across the islands to enable AI deployment.
- **Skills Development:** Building human capital in AI and digital technologies through education and training initiatives.
- **International Cooperation:** Engaging with global partners including UNESCO, UN ESCAP, and regional bodies to access expertise and align with international frameworks.

Governance Structure

Multiple government agencies share responsibility for AI and related digital governance in the Maldives:

- **Ministry of Environment, Climate Change and Technology:** Lead ministry for digital transformation and technology policy, including development of the AI Masterplan and Data Protection Bill. Coordinates across government on AI strategy implementation.
- **Communications Authority of Maldives (CAM):** Independent regulatory body for telecommunications, spectrum management, and postal services. Ensures infrastructure enabling AI connectivity across the islands.
- **Ministry of Homeland Security and Technology:** Oversight ministry for CAM following 2024 restructuring. Addresses cybersecurity and critical infrastructure protection relevant to AI systems.
- **Data Protection Authority (proposed):** Independent supervisory body proposed under the Data Protection Bill to oversee compliance, investigate complaints, and enforce data protection requirements.
- **National Centre for Information Technology (NCIT):** Government technology agency supporting digital transformation and e-government services that may incorporate AI.

Implementation Status

The implementation status of the Maldives' AI regulatory framework varies across instruments. The Maldives Telecommunications Act 2015 is fully operational, with the Communications Authority of Maldives actively regulating the sector, issuing licenses, managing spectrum, and enforcing quality standards. The three main telecommunications operators—Dhiraagu, Ooredoo Maldives, and Raajje Online—operate under this framework, providing the connectivity infrastructure essential for AI deployment.

The National AI Masterplan 2025-2035 remains in draft form as of late 2024, with the government engaging stakeholders and refining provisions before finalization. Implementation will occur progressively across the ten-year timeframe, with priority initiatives addressing immediate infrastructure and capacity gaps identified through the UNESCO assessment.

The Privacy and Personal Data Protection Bill continues through the legislative process following public consultation in mid-2023. Stakeholder input from the UN ESCAP webinar and written submissions is being incorporated into revised drafts. Parliamentary consideration and enactment are anticipated in the coming period, after which implementation will include establishing the Data Protection Authority and a transition period for organizations to achieve compliance.

The UNESCO AI Readiness Assessment provides ongoing benchmarking, with periodic updates tracking progress against baseline metrics. Findings continue informing policy development and investment prioritization.

Future Developments

Several developments are anticipated in the Maldives' AI regulatory landscape over the coming years. The National AI Masterplan is expected to be finalized and formally adopted, triggering implementation of priority initiatives across infrastructure, skills, and sector applications. The first phase through 2030 will focus on foundational capacity building.

The Data Protection Bill is likely to be enacted, establishing comprehensive personal data protections and the Data Protection Authority. This will significantly strengthen the regulatory foundation for responsible AI deployment and enable the Maldives to participate in international data flows requiring adequate protection standards.

As AI adoption accelerates, the government may develop AI-specific regulation addressing issues such as algorithmic transparency, automated decision-making rights, and sector-specific requirements for high-risk applications. The approach will likely build on international frameworks while addressing local circumstances.

Continued engagement with international partners including UNESCO, UN ESCAP, ITU, and regional bodies will support capacity building and knowledge transfer. The Maldives may pursue mutual recognition arrangements for AI governance with trading partners as frameworks mature.

International Context

The Maldives' approach to AI governance aligns with international frameworks while reflecting national priorities. The draft Data Protection Bill incorporates principles from the EU General Data Protection Regulation (GDPR), positioning the Maldives for potential adequacy recognition supporting data flows with Europe and other jurisdictions requiring equivalent protections.

Engagement with [UNESCO](#) through the AI Readiness Assessment demonstrates alignment with the UNESCO Recommendation on the Ethics of Artificial Intelligence, the first global standard-setting instrument in this field. The Maldives' emphasis on ethical AI principles, human oversight, and inclusive development reflects these international norms.

The National AI Masterplan draws on frameworks from OECD AI Principles, the G20 AI Guidelines, and strategies adopted by comparable jurisdictions. Regional engagement through organizations such as the [South Asian Telecommunication Regulators' Council \(SATRC\)](#) and the Asia-Pacific Telecommunity facilitates knowledge sharing and regulatory harmonization.

As a Small Island Developing State, the Maldives contributes perspectives on AI governance challenges unique to SIDS including connectivity constraints, climate vulnerability, and capacity limitations. These insights inform international discussions on inclusive AI development that leaves no country behind.

Malta — AI Regulatory Landscape Summary

Overview

Malta's AI regulatory framework is a multi-layered combination of (1) strategic policy documents that set national aims and priorities for AI-driven growth, trust and skills; (2) domestic statutory and administrative instruments that create certification and supervisory mechanisms; and (3) implementation of the EU-level Artificial Intelligence Act (Regulation (EU) 2024/1689) through national legal notices and designated competent authority arrangements. The overall intent is to marry an innovation-friendly approach with safeguards to protect fundamental rights, privacy and public trust.

Regulatory Instruments

- [Malta — The Ultimate AI Launchpad: A Strategy and Vision for Artificial Intelligence in Malta 2030](#) - High-level national strategy articulating Malta's long-term vision for AI adoption across government, industry and society. Status: Enacted/Published (Policy/Strategy).
- [Malta — Towards Ethical and Trustworthy AI \(Malta's Ethical AI Framework\)](#) - National ethical framework providing principles and guidance for public and private sector AI deployment (human-centricity, fairness, transparency). Status: Enacted/Published (Policy/Guidance).
- [AI Innovative Technology Arrangement \(AI ITA\) scheme / National AI certification programme \(MDIA\)](#) - MDIA-run certification pathway for AI systems intended to provide voluntary assurance and technical/governance validation for innovators. Status: Enacted/Published (Programme/Certification).
- [Malta Digital Innovation Authority Act](#) - Foundational statute establishing the MDIA, its powers, and functions with respect to certification of digital innovation arrangements. Status: In Force (Primary Legislation).
- [Malta Digital Innovation Authority \(Amendment\) Act, Act No. XIX of 2024](#) - Amendment expanding or clarifying MDIA's remit (including certification and supervisory capacities relevant to AI assurance). Status: Enacted/Published (Primary Legislation/Amendment).
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act](#) - The EU-level regulation establishing harmonised rules for AI across member states, including risk classifications, prohibited practices, and obligations for providers and deployers. Status: In Force (EU Regulation).
- [226 of 2025 - Artificial Intelligence Regulations, 2025 \(Legal Notice\)](#) - National implementing legal notice providing domestic detail and operational provisions to support application of the EU AI Act in Malta. Status: Enacted/Published (Secondary Legislation/Legal Notice).
- [227 of 2025 - Artificial Intelligence \(Designation of the Information and Data Protection Commissioner for the purposes of Regulation \(EU\) 2024/1689\) Regulations, 2025 \(Legal Notice\)](#) - Legal Notice designating the Information and Data Protection Commissioner (IDPC) as a national competent authority for specified functions under the EU AI Act. Status: Enacted/Published (Secondary Legislation/Designation).
- [Digital Education Strategy 2024–2030 \(Ministry for Education, Youth, Sport, Research & Innovation\)](#) - Strategy aligning education policy with digital and AI skill needs for learners and educators. Status: Enacted/Published (Policy/Strategy).
- [National eSkills Strategy 2022–2025 \(eSkills Malta Foundation\)](#) - National skills strategy focused on digital and AI-related skill building for the labour force. Status: Enacted/Published (Policy/Strategy).

- [Malta Digital Strategy 2023–2027](#) - Cross-government digital transformation plan supporting AI adoption, public sector digitisation and economic development. Status: Enacted/Published (Policy/Strategy).

Key Themes and Priorities

Across Malta's instruments several recurring themes appear: (1) Trustworthy and ethical AI — emphasised in the Ethical AI Framework and linked to legal duties under the EU AI Act and data protection law; (2) Innovation and market support — a strong focus on facilitating innovation through the MDIA, certification (AI ITA) and testbeds/sandboxes; (3) Skills and education — targeted action through the Digital Education Strategy and National eSkills Strategy to develop workforce capacity and digital literacy; (4) Clear governance and administrative arrangements — national legal notices and MDIA statutes that define supervisory and certifying roles; and (5) EU alignment and legal harmonisation — implementation and operationalisation of Regulation (EU) 2024/1689 at national level.

Governance Structure

Key public bodies and roles include the Malta Digital Innovation Authority (MDIA), responsible for certification, standards and innovation arrangements; the Information and Data Protection Commissioner (IDPC), designated under national regulations to perform functions required by the EU AI Act; relevant ministries (notably the Ministry for Education, Youth, Sport, Research & Innovation) responsible for strategy and skills policies; and other agencies involved in digital transformation (public procurement, sector regulators). The MDIA Act and its 2024 amendment define MDIA's statutory authority; Legal Notices 226/2025 and 227/2025 set out the national supervisory and coordination structure to operationalise EU obligations.

Implementation Status

As of 2025 the EU AI Act (Regulation (EU) 2024/1689) is in force and Malta has issued national Legal Notices to formalise domestic arrangements. The IDPC has been designated for purposes under the EU Act by Legal Notice 227 of 2025. The MDIA's AI ITA scheme is published and active as a national certification option, supported by the MDIA Act and its 2024 amendment. Strategic policy documents (AI Strategy 2030, Ethical AI Framework, Digital Education Strategy) are enacted and published as guidance and policy direction; they inform public sector roll-out and support private sector uptake but are not themselves direct legal prohibitions except where they intersect with binding EU or national legal instruments. Operational work continues on guidance, enforcement mechanisms, and capacity building across authorities.

Future Developments

Expected future activity includes: further operational guidance and sectoral guidance documents to clarify obligations under the EU AI Act; MDIA development of technical and procedural guidance for the AI ITA certification pathway; inter-agency coordination mechanisms between MDIA, IDPC and sectoral regulators; and continued investment in education and workforce upskilling per the Digital Education Strategy 2024–2030 and eSkills programmes. Monitoring and review cycles will determine how voluntary certification interacts with mandatory compliance for high-risk systems.

International Context

Malta's approach is closely aligned with EU-level regulatory objectives while pursuing national measures to support competitiveness and innovation. The MDIA's certification scheme and strategic policy emphasis on skills and testbeds position Malta within a broader EU ecosystem seeking to balance rights-protecting regulation with innovation-friendly instruments. For further official reference consult the Malta Government portals and

institutions such as the MDIA (<https://mdia.gov.mt>), the Information & Data Protection Commissioner (<https://idpc.org.mt>), and the EU legal text for the Artificial Intelligence Act ([Regulation \(EU\) 2024/1689](#)).

Mexico — AI Regulatory Landscape Summary

Overview

Mexico's AI regulatory landscape through 2025 consists of a two-track approach: an enacted layer of strategic documents, interministerial coordination mechanisms and public-sector guidance; and a legislative pipeline of diverse proposed laws addressing criminal, labor, intellectual property and constitutional issues raised by AI and generative systems. Enacted instruments focus on governance, capacity building, risk assessment and secure ICT administration. Proposed instruments aim to introduce substantive legal rules and prohibitions tailored to AI-specific harms.

Regulatory Instruments

- [Hacia una Estrategia de IA en México: Aprovechando la Revolución de la IA \(Toward an AI Strategy in Mexico\)](#) - National strategy document setting objectives for research, capacity building, public-sector adoption and ethical considerations. Status: Enacted/Published; Type: Strategy/policy guidance.
- [Consortio / Alianza en Inteligencia Artificial \(CONACYT\)](#) - Research and funding consortium coordinated by CONACYT to promote AI R&D and collaboration between academia, industry and government. Status: Enacted/Published; Type: Institutional/consortium initiative.
- [Principios generales y guía de análisis de impacto para el desarrollo y uso de sistemas con elementos de inteligencia artificial en la Administración Pública Federal](#) - Mandatory guidance for impact assessments and general principles for AI systems used by the federal administration, emphasising transparency, proportionality and risk mitigation. Status: Enacted/Published; Type: Administrative guidance/obligations for federal agencies.
- [Acuerdo que expide la Estrategia Digital Nacional 2021-2024](#) - Sets broader digital transformation priorities including digital inclusion, data governance and AI integration across public services. Status: Enacted/Published; Type: National digital strategy.
- [Decreto por el que se crea la Comisión Intersecretarial de Tecnologías de la Información y Comunicación y de la Seguridad de la Información \(CITICSI\)](#) - Decree establishing an interministerial commission to coordinate ICT policy and information security across federal agencies. Status: Enacted/Published; Type: Institutional decree.
- [Proyecto de Ley Federal de Gobernanza Digital / Sistema Nacional de Gobernanza Digital](#) - Proposed law to create a national governance system for digital policy, potentially centralising standards and roles. Status: Proposed; Type: Legislative proposal (federal law).
- [Proyecto: Ley para la Regulación Ética de la Inteligencia Artificial y la Robótica](#) - Proposed comprehensive ethical regulation covering design, deployment and liability concerns for AI and robotics. Status: Proposed; Type: Legislative proposal.
- [Iniciativa que adiciona el artículo 199 Octies al Código Penal Federal para sancionar la creación de contenido íntimo sexual con IA sin consentimiento](#) - Bill proposing criminal sanctions for producing non-consensual intimate content generated by AI. Status: Proposed; Type: Criminal law amendment.
- [Iniciativa para reformar la fracción XVII del artículo 73 de la Constitución en materia de Inteligencia Artificial](#) - Constitutional amendment proposal to expressly grant Congress competence to legislate on AI matters. Status: Proposed; Type: Constitutional reform initiative.

- [Iniciativa que adiciona disposiciones para el uso de Inteligencia Artificial por unidades de seguridad pública](#) - Proposed measures to regulate how public security agencies may use AI tools in investigations, with proposed limits and procedural safeguards. Status: Proposed; Type: Public security/legal framework.
- [Proyecto de decreto que reforma la Ley Federal de Cinematografía, la Ley Federal del Derecho de Autor y la Ley Federal del Trabajo para proteger a actores de doblaje frente al uso de IA](#) - Proposed reforms aimed at protecting voice artists and dubbing actors against unauthorized AI reproduction of performance. Status: Proposed; Type: Cross-sector legislative proposal (IP and labor).
- [Proyecto de decreto que regula tecnologías emergentes, disruptivas e inteligencia artificial](#) - Broad proposed regulatory project addressing emerging and disruptive technologies including AI; seeks overarching rules for testing and deployment. Status: Proposed; Type: Regulatory omnibus bill.
- [Laboratorio Nacional de Inteligencia Artificial \(LNIA\) — programa anunciado en el marco del Plan México](#) - National AI Laboratory initiative to coordinate public research, datasets, standards and pilot projects. Status: Enacted/Published (program announced); Type: Research infrastructure/program.
- [Iniciativa que reforma diversas disposiciones del Código Penal Federal y de la Ley Federal del Derecho de Autor en materia de IA generativa](#) - Proposed amendments targeting offences and copyright rules related to generative AI outputs and unlawful data use. Status: Proposed; Type: Criminal and IP law amendments.
- [Iniciativa que reforma la Ley General de Educación y la Ley General de Educación Superior para incorporar la enseñanza de la Inteligencia Artificial](#) - Proposed educational reform to integrate AI teaching into basic and higher education curricula. Status: Proposed; Type: Education law reform.

Key Themes and Priorities

Several recurrent themes run across Mexico's enacted and proposed instruments: (1) public-sector risk management and impact assessment, emphasising the need for federal agencies to evaluate AI systems before deployment; (2) capacity building, research and collaboration via CONACYT, the LNIA and strategy documents; (3) data governance and information security coordinated through CITICSI and digital strategy initiatives; (4) targeted statutory responses to harms linked to generative AI, including privacy, non-consensual intimate images, intellectual property and labour rights; and (5) governance architecture reform to clarify institutional roles and legislative competence over AI.

Governance Structure

The principal governance actors include federal ministries with ICT and security responsibilities, CONACYT as a research funder and convenor, the Intersecretarial Commission on ICT and Information Security (CITICSI) as a coordination body, and programmatic entities such as the LNIA. The Presidency's digital strategy instruments provide cross-cutting policy direction while individual agencies are expected to operationalise impact assessment guidance. If enacted, the Federal Law on Digital Governance and constitutional reform would reconfigure institutional competencies at the federal level.

Implementation Status

Operational guidance and strategy instruments are already in use to varying degrees: federal agencies have begun integrating impact assessments and aligning procurement with strategy goals, and research consortia and the LNIA are in implementation phases or program announcement stages. Legislative proposals remain under consideration in Congress; their passage is uncertain in timing and substance and will determine whether Mexico moves from a mostly administrative/regulatory stance toward prescriptive statutory regimes that create new offences, rights and obligations.

Future Developments

Watch areas for near-term change include: the outcome of bills criminalising non-consensual deepfake intimate content and amendments to the Criminal Code and Copyright Law addressing generative AI; any passage of a Federal Law on Digital Governance that would centralise rule-making; legal protections for voice and likeness following the dubbing actor proposal; and the constitutional reform that would enable direct congressional competence over AI. Continued development of LNIA outputs, standards and public pilots will also shape practical regulation and standard setting.

International Context

Mexico's documents indicate an intent to align with international best practices on trustworthy AI while accounting for domestic priorities. Strategy documents and research initiatives create opportunities to participate in OECD, G20 and other multilateral dialogues, and proposed statutes reflect global themes such as restriction of harmful deepfakes, transparency obligations and copyright adjustments for AI. Stakeholders should monitor international guidance and bilateral cooperation that may influence standard adoption and regulatory harmonisation.

Primary sources and government portals summarising these initiatives can be found at the official government AI portal: <https://government AI portal> and in official announcements published by CONACYT and relevant ministries: [Official sources and agency pages](#). Date of retrieval for this summary: 2025-11-16T16:57:34.450Z.

Morocco — AI Regulatory Landscape Summary

Overview

Morocco is actively developing a comprehensive AI governance framework through multiple legislative initiatives while building on its established [data protection law](#). The country ranks 4th among African economies in the E-Government Development Index and 57th globally in the Digital Transformation Index. The [Maroc Digital 2030](#) strategy positions AI as central to national modernization, targeting 10% GDP growth through digital initiatives. Key regulatory developments include the proposed Digital X.0 Framework Law and a bill for a National Agency for AI Governance, while Law 09-08 provides the current legal foundation for AI-related data processing.

Definitions

Morocco's regulatory framework adopts internationally recognized terminology. Personal data encompasses any information relating to identified or identifiable individuals. Data processing includes all operations performed on personal data including collection, storage, use, and disclosure. The proposed Digital X.0 framework introduces concepts of data governance, digital identity, and interoperability. Artificial intelligence is understood to encompass systems performing tasks requiring human-like intelligence. The proposed AI Agency bill would establish licensing and standards for AI applications. Consent requirements follow international norms requiring free, specific, informed, and unambiguous indication of data subjects' wishes.

Governance and Institutional Framework

The [National Commission for the Control of Personal Data Protection \(CNDP\)](#) serves as Morocco's autonomous data protection authority under Law 09-08, with responsibilities extending to AI-related data processing. The [Ministry of Digital Transition and Administrative Reform](#) leads digital policy coordination and is advancing the Digital X.0 framework. The House of Councilors is reviewing the National Agency for AI Governance bill. If adopted, this agency would become the primary AI regulatory authority. The [General Directorate of Information Systems Security \(DGSSI\)](#) provides cybersecurity guidance. Sector-specific regulators address AI in financial services, telecommunications, and healthcare.

Key Focus Areas

- **Data Protection:** Law 09-08 requires CNDP declaration for data processing including AI applications.
- **Digital Transformation:** Maroc Digital 2030 strategy targeting 10% GDP growth through digital initiatives.
- **AI Agency Establishment:** Proposed agency to oversee AI activities, licensing, and ethical standards.
- **Digital X.0 Framework:** Comprehensive legislation governing data, AI, and digital services.
- **Data Governance:** Principles for data flow and protection aligned with international standards.
- **Digital Identity:** Sector-specific identity limiting data access to necessary scope.
- **Skills Development:** Training 200,000 young people in digital and AI capabilities.
- **Multilingual AI:** Partnership with Mistral AI for Arabic, Amazigh, and African language models.
- **AI in Government:** Implementation of AI in courts and public services.
- **Cross-Border Data:** CNDP authorization required for international data transfers.

Implementation Framework

Implementation of Morocco's AI governance relies on the established CNDP framework while awaiting legislative developments. Organizations processing personal data must declare activities to CNDP before implementation. The proposed Digital X.0 framework would introduce new requirements for data governance, digital identity, and AI transparency. The AI Agency bill would establish licensing mechanisms for certain AI applications. Sector-specific implementation varies, with AI already deployed in courts for verdict transcription. The Ministry of Digital Transition coordinates implementation of the Maroc Digital 2030 strategy. International partnerships, including with Mistral AI, support technical capacity building.

Monitoring and Evaluation

CNDP maintains oversight through declaration review, complaint investigations, and compliance audits. The Commission has increased enforcement activity in recent years, issuing warnings to major data controllers. Progress toward Maroc Digital 2030 targets is monitored through digital development indicators. Morocco tracks its position in international digital rankings, including the E-Government Development Index (4th in Africa) and Digital Transformation Index (57th globally). Internet penetration statistics (103.45% with 38.3 million subscribers) indicate digital infrastructure readiness. UNESCO's Global AI Ethics Observatory includes Morocco, supporting international benchmarking and knowledge exchange.

Penalties, Liability, and Appeals

Law 09-08 establishes Morocco's current enforcement framework. Administrative fines range from MAD 10,000 to MAD 600,000 (approximately USD 1,000 to USD 60,000). Criminal sanctions include imprisonment of three months to four years for serious violations. CNDP typically issues warnings before pursuing fines or prosecution. The proposed Digital X.0 and AI Agency frameworks would introduce additional enforcement mechanisms. AI-specific liability provisions are expected to address harms from automated decision-making. Appeals against regulatory decisions follow established administrative review procedures. Civil remedies are available for damages from unlawful data processing.

Relationship to Other Instruments

[Law 09-08](#) on data protection provides the foundational legal framework for AI-related data processing. The proposed Digital X.0 Framework Law would extend governance to AI, digital identity, and interoperability. The National Agency for AI Governance bill would create dedicated institutional oversight. The Maroc Digital 2030 strategy provides the overarching policy framework. Sector-specific regulations in financial services, telecommunications, and healthcare interface with data protection requirements. E-commerce and electronic signature laws support the digital ecosystem. Morocco's framework coordinates with regional and international standards.

International Alignment

Morocco's data protection framework was designed to align with European standards, facilitating trade and data flows. Law 09-08 reflects principles consistent with the EU Data Protection Directive. Morocco participates in [UNESCO's Global AI Ethics and Governance Observatory](#). The partnership with [Mistral AI](#) demonstrates engagement with international technology leaders. Morocco is a member of the Council of Europe Convention 108 on data protection. CNDP participates in the Francophone and African networks of data protection authorities. The country's strong digital development rankings position it as a regional leader in North Africa.

Implementation Timeline

Date	Milestone
2009-02-18	Law 09-08 on data protection enacted
2024-04	National Agency for AI Governance bill submitted to Parliament
2024	Morocco ranks 4th in Africa for e-government development
2025-Q1	Digital X.0 Framework Law presented for review
2025-2026	Expected parliamentary consideration of AI legislation
2030	Maroc Digital 2030 strategy targets

Compliance Checklist

Requirement	Details
CNDP Declaration	Declare personal data processing to CNDP before implementation
Cross-Border Authorization	Obtain CNDP approval before transferring data outside Morocco
Consent	Obtain valid consent for data processing where required
Security Measures	Implement appropriate technical and organizational safeguards
Data Subject Rights	Facilitate access, rectification, and objection rights
Purpose Limitation	Process data only for declared legitimate purposes
Monitor Developments	Track Digital X.0 and AI Agency legislative progress

Sources and References

Source	Type
DGSSI - Law 09-08	Primary Source
CNDP Official Website	Regulatory Authority
iAfrica - Digital X.0 Law	News Source
Morocco World News - AI Agency	News Source

Netherlands — AI Regulatory Landscape Summary

Overview

The Netherlands' AI regulatory framework combines strategic national policy, sectoral guidance, public-sector transparency measures and institutional capacity-building. Since the 2018–2019 strategic documents and parliamentary communications, the Dutch approach has emphasized human rights, non-discrimination, accountable public administration and innovation support. The mix includes enacted policy letters and guidance, in-force institutional initiatives, and operational instruments such as impact assessments and a national Algorithm Register. The government also coordinates with EU developments and has published positions in response to European initiatives.

Regulatory Instruments

- [Strategic Action Plan for Artificial Intelligence](#) - National strategy setting research, education and public-sector objectives. Status: Enacted/Published. Type: Strategy/Policy document.
- [AI, Public Values and Human Rights \(Kamerbrief\)](#) - Parliamentary letter articulating human-rights priorities for AI policymaking. Status: Enacted/Published. Type: Parliamentary communication / policy guidance.
- [Safeguards Against Risks of Data Analyses by the Government \(Kamerbrief\)](#) - Focused guidance on safeguarding rights when public entities use data analytics. Status: Enacted/Published. Type: Parliamentary communication / sectoral guidance.
- [Dutch AI Coalition \(Nederlandse AI Coalitie, NL AIC\)](#) - Public–private coalition to coordinate research, skills and standards. Status: In force. Type: Coalition / multi-stakeholder body.
- [Innovation Center for Artificial Intelligence \(ICAI\)](#) - Research and university-consortium hub linking government, industry and academia. Status: In force. Type: Research centre / innovation hub.
- [AiNed \(AiNed National Growth Fund Investment Programme\)](#) - Investment programme to boost AI adoption and capabilities in the economy. Status: In force. Type: Funding / investment programme.
- [Guidelines for the Application of Algorithms and Data Analysis by Governmental Organizations](#) - Practical operational guidance for public bodies on procurement, evaluation and safeguards. Status: Enacted/Published. Type: Guidance / operational framework.
- [Impact Assessment for Human Rights and Algorithms \(IAMA\)](#) - A structured assessment tool to identify human-rights impacts of algorithmic systems. Status: In force. Type: Assessment methodology / procedural requirement.
- [Handbook 'AI-system principles for non-discrimination' \(Non-discrimination by design\)](#) - Technical and organisational measures to prevent discriminatory outcomes. Status: Enacted/Published. Type: Handbook / technical guidance.
- [National Algorithm Register \(Algoritmeregister Nederlandse Overheid\)](#) - Central registry documenting public-sector algorithmic systems to improve transparency and oversight. Status: In force. Type: Registry / transparency instrument.
- [Collective Parliamentary Letter 'Algoritmen reguleren' \(Verzamelbrief\)](#) - Parliamentary coordination document outlining legislative interest and regulatory options. Status: Enacted/Published. Type: Parliamentary coordination / policy letter.

- [Implementation Framework for Responsible Use of Algorithms \(Implementatiekader 'Verantwoorde inzet van algoritmen'\)](#) - Implementation-level framework for risk management and governance within public bodies. Status: Enacted/Published. Type: Implementation framework / guidance.
- [Cabinet Appreciation / Response to the European White Paper on AI \(Kabinetsappreciatie Witboek AI\)](#) - National response framing how EU proposals relate to Dutch policy priorities. Status: Enacted/Published. Type: Government response / policy position.
- [Autoriteit Persoonsgegevens: 'Supervision of Algorithms and AI' \(AP guidance on algorithm supervision\)](#) - AP guidance on how data protection supervision applies to algorithmic systems, including enforcement priorities. Status: Enacted/Published. Type: Supervisory guidance.
- [Final Advice on the Organisation of AI Supervision \(Eindadvies inrichting AI-toezicht\) — AP & RDI](#) - Recommendations for structuring national AI supervision and resourcing of supervisory bodies. Status: Enacted/Published. Type: Advisory / supervisory design.
- [Value-Driven Digitalisation Work Agenda \(Werkagenda Waardengedreven Digitaliseren\)](#) - Cross-government agenda embedding societal values in digital transformation. Status: Enacted/Published. Type: Policy agenda.
- [Government-wide Vision on Generative AI \(Overheidsbrede visie generatieve AI\)](#) - Strategic guidance addressing opportunities, risks and sectoral implications of generative AI. Status: Enacted/Published. Type: Vision / policy guidance.
- [National Innovation Centre for Privacy Enhancing Technologies \(NICPET\)](#) - Centre to accelerate PETs research and adoption. Status: In force. Type: Innovation centre / technology programme.
- [Code 'Good Digital Public Administration' \(Code Goed Digitaal Openbaar Bestuur\)](#) - Principles and practical criteria for trustworthy digital government services. Status: Enacted/Published. Type: Code of conduct / sectoral standards.

Key Themes and Priorities

Across these instruments common themes are evident: (1) human-rights protection and privacy by design, (2) non-discrimination and fairness baked into system development, (3) transparency and public accountability (registers, documentation and impact assessments), (4) risk-based governance emphasising proportional measures relative to societal and individual harm, and (5) an innovation-friendly posture that funds research and private-public partnerships to develop trustworthy technologies, particularly privacy-enhancing technologies (PETs).

Governance Structure

Governance is distributed. Key actors include ministries (policy, procurement and public administration), the Autoriteit Persoonsgegevens (AP) for data-protection oversight, advisory and research bodies (ICAI, NL AIC, NICPET), and cross-government programmes (Werkagenda Waardengedreven Digitaliseren). Parliamentary oversight shapes legislative interest via Kamerbrieven and coordinated letters. AP and RDI collaboration on supervisory design signals movement toward a clearer supervisory architecture with sectoral responsibilities and enhanced technical expertise.

Implementation Status

Most documents exist as enacted guidance, parliamentary letters and operational instruments; several innovation centres and programmes are already in force. Implementation focuses first on public-sector deployments, where the Algorithm Register, IAMA and implementation frameworks are actively used to record systems, conduct impact assessments and integrate safeguards into procurement. Supervision capacity is being strengthened following the 2024 final advice; however, full statutory supervisory powers aligned to an EU AI Act regime will require further legislative and organisational steps.

Future Developments

Primary near-term developments include aligning national rules with the EU AI Act and transposition requirements, expanding capacity and resourcing for AP and cooperating supervisors, refining the Algorithm Register's scope and accessibility, operationalising generative-AI policy into sectoral controls, and scaling PETs development through NICPET. Parliamentary and cabinet activity suggests continued attention to binding safeguards for high-risk public-sector uses and procurement rules that demand transparency and impact assessments.

International Context

The Netherlands positions its framework to be compatible with EU-level instruments (including the EU White Paper response and preparatory steps for the AI Act) and international good-practice (OECD principles, human-rights based approaches). Dutch initiatives emphasise interoperability with European standards and collaborative research across member states, while promoting public-private partnerships to keep pace with technological change.

For official primary sources see [government AI portal](#) and listed official documents. For supervisory perspectives consult the Autoriteit Persoonsgegevens' materials at [Autoriteit Persoonsgegevens](#).

New Zealand — AI Regulatory Landscape Summary

Overview

New Zealand's AI regulatory landscape is defined by a combination of statutory data protection, a statutory trust regime for digital identity, public-sector algorithm governance, and a set of pragmatic guidance instruments for both the public and private sectors. The architecture relies on:

- Privacy law (the [Privacy Act 2020](#)) as the primary legal constraint on AI processing of personal information;
- A statutory accreditation, technical and governance regime for digital identity (the [Digital Identity Services Trust Framework Act 2023](#) and its [Regulations 2024 \(SL 2024/197\)](#) and [Rules 2024](#));
- Sectoral, principle-driven instruments for algorithmic fairness and public sector AI governance (the [Algorithm Charter for Aotearoa New Zealand](#), the [Public Service AI Framework](#) and the [Responsible AI Guidance for the Public Service: GenAI](#)).

These instruments are supported by the Office of the Privacy Commissioner's AI-specific guidance and government strategic statements such as [New Zealand's Strategy for Artificial Intelligence: Investing with Confidence](#), which set policy direction for fostering investment while managing social and economic risk.

Regulatory Instruments

- [Privacy Act 2020](#) - Statutory data protection law setting privacy principles, individual rights, enforcement powers and obligations that apply where AI processes personal information. Status: In force; Type: Primary statute.
- [Algorithm Charter for Aotearoa New Zealand](#) - Policy-level commitments and expectations for government use of algorithms, promoting transparency, human oversight and monitoring. Status: In force; Type: Policy/Charter.
- [Digital Identity Services Trust Framework Bill](#) - Legislative proposal leading to enactment of the Trust Framework; describes accreditation and governance model for identity services. Status: Passed (led to Act); Type: Bill/Legislative history.
- [The Digital Strategy for Aotearoa](#) - National strategy document articulating digital transformation, inclusion and trust principles relevant to AI adoption. Status: Enacted/Published; Type: Strategy/Policy.
- [Digital Identity Services Trust Framework Act 2023](#) - Statute creating accreditation, obligations and enforcement for digital identity service providers interacting with government and regulated services. Status: Enacted/Published; Type: Primary statute.
- [Interim Generative AI guidance for the public service](#) - Rapid guidance issued to address early generative AI risks in government operations; updated as risks emerged. Status: Changed (iterated); Type: Guidance/Interim policy.
- [Office of the Privacy Commissioner — Guidance/Expectations on the use of AI \(privacy guidance\)](#) - AI-specific interpretation of privacy obligations including PIAs, de-identification, lawful bases and transparency. Status: In force; Type: Regulatory guidance.
- [Digital Identity Services Trust Framework Regulations 2024 \(SL 2024/197\)](#) - Prescribed requirements for implementation of the 2023 Act, including accreditation criteria and operational controls. Status: In force; Type: Regulations (secondary legislation).

- [Digital Identity Services Trust Framework Rules 2024](#) - Detailed rules supporting the Regulations and Act, covering technical, assurance and reporting obligations. Status: In force; Type: Rules (regulatory instrument).
- [Public Service AI Framework](#) - Framework establishing governance, assurance, procurement and accountability expectations for AI across public service agencies. Status: Enacted/Published; Type: Framework/Policy.
- [Responsible AI Guidance for the Public Service: GenAI](#) - Specific guidance on managing generative AI risks in public services including data handling and communications. Status: Enacted/Published; Type: Guidance.
- [New Zealand's Strategy for Artificial Intelligence: Investing with Confidence](#) - National-level strategy promoting investment, innovation and public trust. Status: Enacted/Published; Type: Strategy/Policy.
- [Responsible Artificial Intelligence guidance for businesses](#) - Non-binding guidance aimed at private sector adoption of responsible AI practices, including governance and risk management. Status: Enacted/Published; Type: Guidance/Best practice.

Key Themes and Priorities

Across instruments common themes emerge: protection of personal information (privacy-by-design and PIAs); accountability and human oversight (particularly in public sector decision-making); trustworthy digital identity through statutory accreditation and standards; transparency and explainability where feasible; risk-based and proportionate regulation; and alignment with international norms to enable cross-border interoperability and investment.

Governance Structure

Primary agencies and roles include: the Office of the Privacy Commissioner (privacy enforcement and guidance; <https://www.privacy.org.nz>), the Department of Internal Affairs and Government Chief Digital Officer (lead on digital identity and operational frameworks; <https://www.dia.govt.nz>), the Public Service Commission (public service governance and workforce expectations; <https://www.publicservice.govt.nz>), and ministerial/central agencies coordinating strategy and inter-agency controls. Accreditation and compliance mechanisms created under the Trust Framework provide statutory enforcement for identity service providers.

Implementation Status

Most instruments referenced are published, enacted or in force. The Privacy Act remains the enduring legal foundation. The Digital Identity Services Trust Framework Act (2023) and its Regulations and Rules (2024) are in place, enabling accreditation and oversight of identity services. Public service AI frameworks and generative AI guidance have been issued and iteratively updated; the Privacy Commissioner's guidance is actively used in compliance assessments. Enforcement so far is focused through privacy investigations, procurement requirements, accreditation conditions and reputational levers. The landscape is operational but evolving.

Future Developments

Future work is likely to include refinements to public service frameworks, expanded operationalisation of accreditation and certification regimes, strengthened incident reporting and cross-agency coordination, and continued emphasis on international alignment (OECD and comparable jurisdictions). Some stakeholders have signalled interest in considering targeted statutory obligations for high-risk AI applications if gaps in the existing mix of instruments become apparent.

International Context

New Zealand's approach emphasises interoperability with international frameworks, seeking to align privacy, trustworthy identity and responsible AI expectations to support trade, research collaboration and cross-border

services. The model is closer to a principles-and-sectoral approach (similar to several like-minded jurisdictions) rather than prescriptive, broad-based AI prohibition.

For more information and to access primary materials, consult the official agency sites linked above and the listed regulation pages (internal links under "Regulatory Instruments").

Nigeria — AI Regulatory Landscape Summary

Overview

Nigeria's AI regulatory framework is a layered mixture of national digital strategy, data protection law, draft sectoral and technology-specific codes, parliamentary bills proposing statutory institutions, and professional guidance. The framework places strong emphasis on data protection, capacity building and the creation of institutional structures to promote, regulate and materialise an AI-enabled digital economy. Core, in-force instruments such as the [National Digital Economy Policy and Strategy \(NDEPS\) 2020–2030](#) and the [Nigeria Data Protection Act \(NDPA\)](#) (reinforced by the [General Application and Implementation Directive \(GAID\)](#)) establish broad policy goals and substantive privacy obligations that shape permissible uses of AI. Parallel draft instruments from the National Information Technology Development Agency ([NITDA](#)) and active bills before the National Assembly indicate an ongoing shift toward more prescriptive rules and possible statutory regulators.

Regulatory Instruments

- [National Digital Economy Policy and Strategy \(NDEPS\) 2020–2030](#) - A national policy roadmap that positions AI as a cross-cutting driver for digital transformation and economic growth; status: In force; type: National policy/strategy.
- [Draft Code of Practice for Interactive Computer Service Platforms / Internet Intermediaries \(NITDA\)](#) - Draft code aimed at platform liability, content moderation expectations and transparency/reporting duties for intermediaries; status: Draft; type: Agency code of practice.
- [National Artificial Intelligence and Robotic Sciences \(Establishment\) Bill \(HB 601\)](#) - Parliamentary bill proposing the establishment of institutions and regulatory structures for AI and robotics research and oversight; status: Under review; type: Bill/legislation.
- [Control of Usage of Artificial Intelligence Technology in Nigeria Bill \(HB 942\)](#) - Legislative proposal focused on controlling harmful or high-risk AI uses and prescribing sanctions for misuse; status: Under review; type: Bill/legislation.
- [National Artificial Intelligence Policy \(NAIP\)](#) - Draft policy that outlines principles for ethical and beneficial AI development, data governance, and research priorities; status: Draft; type: National policy.
- [Nigeria Data Protection Act \(NDPA\)](#) - Comprehensive data protection statute regulating collection, processing, transfers and data subject rights; foundational for AI compliance; status: In force; type: Statute.
- [Bill on Establishment of the National Institute for Artificial Intelligence and Robotic Studies Regulation Commission](#) - Bill to create an institute/commission for AI research, standard-setting and oversight; status: Under review; type: Bill/legislation.
- [Nigerian Bar Association Guidelines for the Use of Artificial Intelligence in the Legal Profession](#) - Profession-level guidance addressing confidentiality, competence, verification and client consent when lawyers use AI tools; status: Enacted/Published; type: Professional guidelines.
- [National Artificial Intelligence Strategy \(NAIS\)](#) - Draft strategic document aligning national priorities for AI deployment, skills development and public-private cooperation; status: Draft; type: Strategy.
- [General Application and Implementation Directive \(GAID\) of the Nigeria Data Protection Act](#) - Implementation guidance that clarifies compliance obligations under the NDPA; status: In force; type: Directive/implementation guidance.

- [Draft Code of Practice for Artificial Intelligence \(NITDA\)](#) - Draft AI-specific code proposing obligations on transparency, risk assessments, documentation, and algorithmic governance for AI systems; status: Draft; type: Agency code of practice.

Key Themes and Priorities

Across Nigeria's instruments the following themes recur: (1) data protection and individual rights: NDPA/GAID provide the legal backbone for privacy and influence AI practices including lawful bases for training data and automated profiling safeguards; (2) institutional development: multiple bills envision new agencies, institutes or commissions to centralise AI research, standards and oversight; (3) risk-based regulation: draft NITDA codes and legislative proposals favour a graduated approach with tighter controls for high-risk uses; (4) capacity-building and national competitiveness: NDEPS, NAIP and NAIS emphasise skills, research funding, and public-private collaboration to localise benefits; and (5) sectoral tailoring: recognition that health, finance, justice and critical infrastructure need bespoke rules and professional guidance (as illustrated by NBA guidelines).

Governance Structure

Key actors in Nigeria's AI governance include federal ministries (notably the Ministry of Communications and Digital Economy), the National Information Technology Development Agency ([NITDA](#)) which is leading technical codes of practice, the National Assembly (which is considering HB 601, HB 942 and institution-establishing bills), and professional bodies such as the Nigerian Bar Association ([NBA](#)) which issue practice-specific guidance. The NDPA is enforced according to its implementing architecture and the GAID provides clarity on enforcement and compliance. If passed, proposals to establish a National Institute for AI and a dedicated AI regulator would add statutory governance layers responsible for standards, certification and oversight.

Implementation Status

Foundational measures are in force: NDEPS (policy) and NDPA plus GAID (legal/implementation framework). NITDA's instruments (platforms code and AI code) and the NAIP/NAIS remain drafts and are subject to stakeholder review. Parliamentary bills (HB 601, HB 942, and the institute-establishing bill) are under active review and could materially change governance depending on final drafting, scope and institutional design. Professional guidance (NBA) is published and has immediate effect for legal practitioners. Practical enforcement and supervision capacity vary: agencies will need sustained resourcing and technical expertise to operationalise specialised AI supervision.

Future Developments

Near-term developments to monitor include the finalisation or withdrawal of NITDA's draft codes, parliamentary progression of HB 601 and HB 942 (which could create offences, licensing or oversight regimes) and formal adoption of NAIP/NAIS. International cooperation (data transfer frameworks, standards alignment) and domestic capacity-building initiatives are likely to be prioritised. Stakeholders should also watch for sectoral regulations that operationalise NDPA obligations in specific contexts like health, finance and education.

International Context

Nigeria's approach aligns with global trends that pair general-purpose data protection frameworks with AI-specific guidelines and institutional attempts to govern high-risk systems. The emphasis on national strategy and capacity building mirrors approaches elsewhere, while the draft codes echo international risk-based, transparency-focused regulatory models. Nigeria's use of agency-led codes and professional guidance alongside proposed statutory instruments positions it to combine flexibility (through codes) with legal certainty (through

legislation) as the AI policy field matures. For further reference consult government portals such as [Nigeria Official Portal](#), [NITDA](#) and the [Nigerian Bar Association](#).

Norway — AI Regulatory Landscape Summary

Overview

This document summarises Norway's AI regulatory framework as of 14 November 2025. Norway combines strategic national plans, sectoral guidance and innovation tools with alignment efforts toward the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) through EEA processes. The framework prioritises trust, privacy, human-centred design, public-sector transformation and safety-critical controls in health and care services. Governance is distributed across ministries and specialised agencies while practical compliance support is delivered by instruments such as regulatory sandboxes.

Regulatory Instruments

- [One Digital Public Sector: Digital strategy for the public sector 2019–2025](#) - Strategic, published national plan focused on modernising public services through digitalisation and data-driven public administration. Status: Enacted/Published. Type: National digital strategy and policy framework.
- [National Strategy for Artificial Intelligence \(Nasjonal strategi for kunstig intelligens\)](#) - High-level strategy laying out Norway's ambitions for AI development, ethical principles, research, education and public-sector adoption. Status: Enacted/Published. Type: National strategy.
- [Felles plan for kunstig intelligens 2020 \(Common plan for artificial intelligence 2020\)](#) - Coordinated plan between government actors to operationalise AI activities, funding priorities, and cross-sector collaboration. Status: Enacted/Published. Type: Coordinating plan/framework.
- [The Digital Norway of the Future – National digitalisation strategy 2024–2030](#) - Updated national digitalisation strategy emphasising infrastructure, interoperability, digital skills and secure data sharing to underpin safe AI deployment across government and industry. Status: Enacted/Published. Type: National digitalisation strategy.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(AI Act\) \(EEA relevance\)](#) - EU-level horizontal regulation establishing risk-based obligations, prohibited practices, and conformity assessments. Status: Under review for EEA relevance and national implementation. Type: Supranational legal instrument with EEA implications.
- [Datatilsynet Regulatory Sandbox for privacy-friendly innovation and AI \(Sandbox for Responsible AI\)](#) - Practical regulatory sandbox run by the Norwegian Data Protection Authority to enable supervised testing of AI solutions with privacy protections and regulatory feedback. Status: Enacted/Published. Type: Regulatory sandbox/pilot mechanism.
- [Status and proposals for further work with artificial intelligence \(KI\) in the health and care services \(Status og forslag til videre arbeid med kunstig intelligens i helse- og omsorgstjenesten\)](#) - Sectoral report and recommendations focusing on governance, safety, validation and data use in health and care. Status: Enacted/Published. Type: Sectoral status report and recommendations.
- [Joint AI plan for the safe and effective use of AI in the Norwegian health and care services 2024–2025](#) - Operational plan for implementing safe AI in healthcare, emphasising clinical validation, human oversight and interoperability. Status: Enacted/Published. Type: Sectoral implementation plan.

Key Themes and Priorities

Across documents, recurring priorities are: protecting fundamental rights (privacy, nondiscrimination), ensuring safety and clinical robustness in health, enabling trustworthy public-sector AI to improve services, fostering innovation and research, and building technical and organisational capacity within government and health

providers. Transparency, explainability and human oversight are emphasised, alongside the need for secure, interoperable data infrastructures and responsible public procurement to manage vendor risk.

Governance Structure

Norway uses a distributed governance model. Strategic leadership is located with relevant ministries (for example the Ministry of Local Government and Modernisation for public-sector digitalisation and the Ministry of Health and Care Services for healthcare AI). Operational roles are fulfilled by agencies and directorates including the Norwegian Data Protection Authority (Datatilsynet), the Digitalisation Directorate (Digdir), and the Directorate of Health (Helsedirektoratet). These bodies produce sectoral guidance, enforce legal obligations (notably data protection), operate sandboxes, and support procurement and standards work. Research councils, universities and standardisation bodies provide technical expertise, while municipalities and regional health authorities are responsible for on-the-ground implementation.

Implementation Status

Strategic documents listed above are published and inform policy and procurement. The Datatilsynet sandbox has been operationalised to allow supervised testing of privacy-sensitive AI projects and to generate practical guidance. Health-sector work is advanced with status reports and a joint plan for 2024–2025 that sets concrete actions for clinical validation, data governance, and workforce competence building. The EU AI Act (Regulation (EU) 2024/1689) is under active review for EEA incorporation; Norway is preparing for the Act's requirements and potential conformity and enforcement mechanisms. Implementation challenges include capacity gaps among smaller public entities, complexity in procurement and compliance processes, cross-sector data access for safe model training, and the need for more granular guidance for foundation models and generative AI systems.

Future Developments

Key near-term developments include the EEA decision on the AI Act's application and subsequent national implementation measures, publication of additional guidance and technical standards, expansion of sandbox and pilot programmes, and targeted initiatives to strengthen procurement and local government capacity. Expect ongoing sectoral regulations and guidance for health, transport and other safety-critical domains. Norway will likely continue to align closely with EU regulatory milestones while tailoring sectoral operational guidance to national circumstances.

International Context

Norway's approach is closely aligned with EU policy and international standards. The EEA relationship means EU legal instruments such as the AI Act have direct relevance; international cooperation on standards, testing regimes, and cross-border data flows is a practical necessity. Norway's combination of strategic direction, sectoral plans and experimental regulatory tools mirrors broader European trends toward risk-based, rights-sensitive AI governance combined with innovation-friendly measures like sandboxes.

Selected official sources and portals for further reference: [Regjeringen.no \(Norwegian Government\)](https://www.regjeringen.no), [Datatilsynet \(Norwegian Data Protection Authority\)](https://www.datatilsynet.no), [Helsedirektoratet \(Directorate of Health\)](https://www.helsedirektoratet.no), and the EU legal portal for the AI Act at [EUR-Lex](https://eur-lex.europa.eu).

Pakistan — AI Regulatory Landscape Summary

Overview

Pakistan's AI regulatory framework has evolved rapidly since 2018 from a focus on digital transformation and skills development to a more structured combination of cybersecurity, data protection, cloud-first infrastructure and explicit AI governance. The country now has multiple strategic and legal instruments — some enacted, some in force, and others still in draft or under parliamentary review — that together aim to enable AI-driven development while addressing the risks that arise from data-intensive systems. This detailed summary describes the key instruments, their relationships, core themes, governance arrangements and the current implementation picture as of 2025.

Regulatory Instruments

- [Digital Pakistan Policy \(2018\)](#) - Enacted/Published. A foundational national strategy emphasizing digital inclusion, broadband expansion, e-government, skills and institutional modernization. Serves as the enabling policy that situates AI within broader digital transformation goals and public service modernization.
- [Presidential Initiative for Artificial Intelligence and Computing \(PIAIC\)](#) - In force. A presidential-led program focused on upskilling, capacity building, pilot projects and fostering a domestic talent pipeline for AI, data science and related technologies. Functions as an operational and advisory initiative rather than a statute.
- [National Cyber Security Policy 2021](#) - Enacted/Published. Establishes principles, institutional roles and strategic objectives for national cyber resilience, incident response and critical infrastructure protection, which are preconditions for secure AI operations.
- [Pakistan Cloud First Policy](#) - Enacted/Published. Directs public-sector adoption of secure cloud services, standardizes procurement preferences and supports centralized platforms for data and services — a critical infrastructure decision that shapes where and how AI systems are hosted and accessed.
- [Personal Data Protection Bill, 2023](#) - Under review. Draft legislation proposing rules for processing personal data, data subject rights, consent, cross-border transfers, and enforcement mechanisms. Its final form will materially affect algorithmic systems that rely on personal data.
- [Draft National Artificial Intelligence Policy \(2023\)](#) - Draft. An earlier policy draft that articulated principles for trustworthy AI, sectoral use cases, and governance approaches; informed subsequent legislative efforts and the 2025 National AI Policy.
- [Regulation of Artificial Intelligence Bill, 2024](#) - Under review. A bill intended to provide a statutory framework for AI oversight, risk classification, compliance obligations and possibly certification or registry mechanisms. Subject to parliamentary scrutiny and revision at the time of drafting.
- [Digital Nation Pakistan Act, 2025](#) - Enacted/Published. A comprehensive statute advancing digital governance, public-sector digitization, and certain administrative frameworks that enable national-level digital projects including AI deployments.
- [Prevention of Electronic Crimes \(Amendment\) Act, 2025](#) - Enacted/Published. Amendments to Pakistan's electronic crimes law strengthening investigative and prosecutorial powers for cyber offences; has implications for misuse of AI, automated harms and law enforcement access.
- [National Artificial Intelligence Policy \(National AI Policy\) 2025](#) - Enacted/Published. The country's principal AI strategy document in 2025, setting out objectives for trustworthy AI, a risk-based governance approach, public procurement rules for AI, research and capacity priorities, and institutional coordination mechanisms.

Key Themes and Priorities

Across Pakistan's instruments the following themes are prominent: (1) enabling digital infrastructure and cloud-first adoption to create a stable technological base; (2) cybersecurity and resilience to protect AI systems and data assets; (3) data protection and privacy as prerequisites for lawful AI use; (4) human capital development — training, certification and research — to grow local AI capacity; (5) a risk-based regulatory stance emphasizing sectoral calibration rather than blanket prohibitions; and (6) public procurement and service delivery as primary early use-cases for government-led AI projects.

Governance Structure

Implementation relies on a combination of ministries, agencies and initiatives. The Ministry of Information Technology and Telecommunication (MoITT) typically anchors policy coordination, with regulatory and compliance roles for bodies such as the Pakistan Telecommunication Authority (PTA) on communications and intermediate liability matters. Electronic crimes enforcement is led through investigative agencies (including the Federal Investigation Agency and relevant prosecutors) under amendments to the Prevention of Electronic Crimes Act. The Presidential Initiative for Artificial Intelligence and Computing (PIAIC) plays a visible advisory and skills development role. The National AI Policy (2025) envisions or reinforces an apex coordination mechanism to align ministries, provinces and regulators and to set standards, though detailed secondary rules and institutional mandates are required for day-to-day oversight, audit and certification functions.

Implementation Status

Status ranges from operational initiatives to draft laws. The Digital Pakistan Policy (2018), PIAIC and National Cyber Security Policy (2021) are in implementation phases with various projects, trainings and guidelines. The Pakistan Cloud First Policy has influenced public procurement and hosting choices, but technical and procurement reforms remain ongoing. The Personal Data Protection Bill (2023) and the Regulation of Artificial Intelligence Bill (2024) were under review and subject to amendment as of 2024–2025; their final enactment will determine many compliance details for private-sector and government AI systems. The Digital Nation Pakistan Act (2025) and Prevention of Electronic Crimes (Amendment) Act (2025) are enacted statutes that enlarge the statutory toolkit for digital governance and enforcement. The National AI Policy (2025) is the primary strategic document guiding AI priorities, intended to be operationalized through subordinate regulations, standards and institutional actions.

Future Developments

Priority next steps include finalizing data protection legislation, clarifying the Regulation of Artificial Intelligence Bill (if adopted) or equivalent secondary rules with concrete obligations for high-risk systems, and establishing workable certification, audit and oversight mechanisms. Capacity gaps across provinces and agencies will need resourcing, and investment in technical standards, transparency measures and mechanisms for redress will be essential for public trust. Cross-border data transfer rules, procurement rules for AI and alignment with international standards (OECD, ISO) will shape foreign investment and interoperability.

International Context

Pakistan's approach combines elements common to many jurisdictions: an initial phase of national digital strategy and skills development followed by cybersecurity and privacy rules and then AI-specific governance. The 2025 National AI Policy signals an intent to align with global best practices and to participate in international standards development. Practical alignment with multilaterally accepted norms (e.g., risk-based regulation, human rights safeguards, and technical standards for safety and explainability) will help Pakistan attract investment and ensure

cross-border compatibility. For further institutional detail and primary source texts, consult official portals such as <https://www.pakistan.gov.pk> and ministry or regulatory sites referenced in the individual regulations.

Panama — AI Regulatory Landscape Summary

Overview

Panama is developing a comprehensive approach to AI governance through legislative proposals, strategic planning, and institutional coordination. Led by [SENACYT \(National Secretariat of Science, Technology, and Innovation\)](#), the country is working to establish a framework that promotes safe, ethical, and trustworthy AI while respecting democratic principles and human rights. Key developments include the [Draft Bill No. 14 on Artificial Intelligence Regulation](#) under consideration by the National Assembly and the [PENCYT 2025-2029](#) strategic plan with digitalization as a primary focus area.

Regulatory Instruments

- [Draft Bill No. 14 on Artificial Intelligence Regulation](#) - Panama's first comprehensive legislative proposal to establish a legal framework for AI governance, digital rights protections, and citizen safeguards, introduced to the National Assembly in 2023.
- [National Strategic Plan for Science and Technology \(PENCYT\) 2025-2029](#) - Five-year strategic framework establishing AI within the digitalization pillar, coordinating research efforts and positioning Panama as a regional technology hub.

Key Themes and Priorities

- **Digital Rights Protection:** Establishing fundamental protections for citizens in AI contexts through pending legislation.
- **Ethical AI Development:** Commitment to AI that respects human dignity, democratic principles, and individual freedoms.
- **Human Capital Development:** Building AI expertise through training programs and initiatives like Gerencia Panamá.
- **Research Capacity Building:** Developing AI research infrastructure and capabilities through PENCYT objectives.
- **Multi-Stakeholder Participation:** Engaging government, academia, private sector, and civil society in AI governance.
- **Regional Hub Ambitions:** Positioning Panama as a technology and innovation center for Latin America.
- **International Alignment:** Ensuring AI governance aligns with emerging global standards and regional initiatives.
- **Responsible Innovation:** Balancing regulatory protection with support for AI innovation and economic development.

Governance Structure

- [National Secretariat of Science, Technology, and Innovation \(SENACYT\)](#): Primary coordinating body for AI policy, developing the National AI Strategy, and implementing PENCYT objectives.
- [National Assembly \(Asamblea Nacional\)](#): Legislative authority considering Draft Bill No. 14 and responsible for enacting AI legislation.

- **Ministry of Commerce and Industries:** Sector-specific oversight responsibilities for technology and digital economy matters.
- **INDICATIC Initiative:** Program launched in 2022 advancing Panama's technological capabilities including AI.
- **Gerencia Panamá Program:** Initiative strengthening AI literacy and management skills among leaders.

Implementation Status

Panama's AI governance framework is in active development with multiple initiatives progressing in parallel. Draft Bill No. 14 remains under consideration by the National Assembly, with ongoing committee discussions and stakeholder consultations. PENCYT 2025-2029 is in force and being implemented through SENACYT coordination. A National AI Strategy is being developed, with the first draft expected by May 2025. Panama scored 25 on the Latin American Artificial Intelligence Index (ILIA) for regulatory maturity, indicating early-stage development with significant advancement opportunities.

Future Developments

Panama's AI governance is expected to advance through several anticipated developments. The National AI Strategy first draft from SENACYT is expected by May 2025, providing detailed policy direction. Draft Bill No. 14 will continue through the legislative process toward potential passage and implementation. PENCYT 2025-2029 mid-term review in 2027 will assess progress and enable adjustments. Continued development of AI literacy programs and research infrastructure will support workforce preparation. Panama's participation in regional AI governance discussions will inform evolving policy approaches.

International Context

Panama's AI governance approach aligns with emerging international standards and regional best practices. The emphasis on ethical, safe, and trustworthy AI reflects [OECD AI Principles](#) and UNESCO recommendations. Panama participates in hemispheric discussions on responsible AI development and has committed to promoting AI that strengthens democratic principles throughout the Americas. The country's early-stage regulatory maturity, as indicated by the ILIA assessment, presents opportunities for learning from regional leaders while developing an approach suited to Panama's specific context. International cooperation and technology transfer partnerships support knowledge exchange and capacity building.

Peru — AI Regulatory Landscape Summary

Overview

Peru's AI regulatory framework is an evolving, pragmatic mixture of digital-government foundations, targeted promotional law, sectoral bills and penal amendments. The framework places strong emphasis on: (1) enabling the use of AI to modernize public services and catalyze economic development; (2) building operational rules for consular and administrative services; and (3) deterring harmful uses of AI by amending the Penal Code. Multiple draft bills and strategy documents remain active in the policy process, creating a layered regulatory landscape that combines enacted laws with ongoing parliamentary and executive-level rulemaking.

Primary actors in design and implementation include the Presidency of the Council of Ministers (PCM), sectoral ministries (notably Education, Foreign Affairs, Transport and Communications, Justice and Interior), and administrative agencies responsible for identity, data and public services. Peru balances a promotion-first stance (Law No. 31814; National Policy for Digital Transformation to 2030) with enforcement through penal amendments (Law No. 32314) and sectoral safeguards.

Key external reference portals: [Portal del Estado Peruano](#), [Congreso de la República](#), [Presidencia del Consejo de Ministros \(PCM\)](#).

Regulatory Instruments

- [Decree-Law No. 1412 — Law Approving the Digital Government \(Ley de Gobierno Digital\)](#) - Foundational digital-government law that enables electronic procedures, interoperability and the adoption of emerging technologies by public bodies. Status: In force; Type: Decree-Law (digital government).
- [National Artificial Intelligence Strategy — Working Document for Citizen Participation 2021–2026 \(Estrategia Nacional de Inteligencia Artificial, Documento de Trabajo\)](#) - Strategic, consultative working document outlining priorities for inclusive, ethical AI and public participation. Status: Draft/working document; Type: Strategy/working document.
- [Project 2775/2022 — Bill to promote the use of Artificial Intelligence \(project that led to Law 31814\)](#) - Parliamentary bill whose provisions informed and led to Law No. 31814. Status: Ended (led to Law No. 31814); Type: Parliamentary project/bill.
- [Project 6524/2023 — Bill on digital labeling for systems and applications using Artificial Intelligence \(etiquetado digital\)](#) - Proposal to require labeling/disclosure for AI systems that materially affect users, enhancing transparency. Status: Draft; Type: Parliamentary project/bill.
- [Project 6573/2023 — Bill to modify the Penal Code to include AI usage as an aggravating factor](#) - One of several penal amendment projects consolidated into later penal reforms. Status: Ended (consolidated into penal amendments); Type: Parliamentary project/bill (penal reform).
- [Law No. 31814 — Law that promotes the use of Artificial Intelligence in favor of the country's economic and social development](#) - Principal promotion law encouraging AI adoption, establishing policy aims and delegating rulemaking authority. Status: In force; Type: Law (promotion of AI).
- [National Policy for Digital Transformation to 2030 \(Política Nacional de Transformación Digital al 2030\)](#) - Long-term policy framework guiding public-sector digital transformation and recognizing emerging technologies. Status: In force; Type: National policy.

- [Project 6852/2023 \(06852\) — Bill authorizing the use of Artificial Intelligence in Peruvian consulates abroad](#) - Bill to allow consular offices to adopt AI tools for service delivery and efficiency. Status: Ended (elements merged into Law No. 32082 implementation); Type: Parliamentary project/bill.
- [Project 6927/2023 \(06927\) — Bill that would oblige the use of Artificial Intelligence in public entities](#) - Proposed mandatory adoption framework for public entities in specific contexts. Status: Draft; Type: Parliamentary project/bill.
- [Project 7033/2023 \(07033\) — Bill that proposes to regulate the development and use of Artificial Intelligence in Peru](#) - Broader regulatory proposal intending to set rules and obligations for AI systems across sectors. Status: Draft; Type: Parliamentary project/bill.
- [Project 7072/2023 — Bill to modify the Penal Code and related rules to include misuse of AI](#) - Penal-focused bill that was consolidated into broader penal amendments. Status: Ended (consolidated into penal amendments); Type: Parliamentary project/bill (penal reform).
- [Project 7619/2023 \(07619\) — Bill on interoperability and the use of Artificial Intelligence for services of the Ministry of Foreign Affairs](#) - Interoperability-centered bill later merged into consular digital transformation law. Status: Ended (merged into consular transformation law); Type: Parliamentary project/bill.
- [Project 7651/2023 — Bill to regulate use of AI algorithms for license-plate recognition \(reconocimiento de placas vehiculares\)](#) - Sectoral bill proposing rules for vehicle-plate recognition systems, privacy and law-enforcement interfaces. Status: Draft; Type: Parliamentary project/bill (sectoral).
- [Project 7659/2023 — Bill to include programming, robotics and AI education in the school curriculum](#) - Education-focused proposal to integrate digital skills and AI content into basic education. Status: Draft; Type: Parliamentary project/bill (education).
- [Project 8223/2023 \(08223\) — Bill for the promotion and regulation of AI use in Peru](#) - Comprehensive promotion and regulatory bill proposing combined incentives and obligations. Status: Draft; Type: Parliamentary project/bill.
- [Law No. 32082 — Law providing for the progressive implementation of Digital Transformation in Peruvian Consular Offices](#) - Formal legal basis for modernizing consular services and explicitly incorporates emerging technologies including AI. Status: In force; Type: Law (consular/digital transformation).
- [Project 8746/2024 — Bill to modify the Penal Code and related provisions regarding AI](#) - Continuation of penal amendment initiatives addressing misuse of AI; elements consolidated into enacted penal amendments. Status: Ended (consolidated into penal amendments); Type: Parliamentary project/bill.
- [Project 10525/2024 — Bill to modify the Penal Code and related provisions regarding AI](#) - Another penal amendment track that contributed to consolidated penal reform. Status: Ended (consolidated into penal amendments); Type: Parliamentary project/bill.
- [Project 10717/2024 — Bill declaring of national interest the incorporation of AI pedagogy into basic regular education](#) - Policy bill aimed at formalizing AI education as a national interest for primary and secondary education. Status: Draft; Type: Parliamentary project/bill (education policy).
- [Law No. 32314 — Amendment to the Penal Code and related laws to treat malicious use of AI as an aggravating circumstance](#) - Enacted penal amendment creating aggravated penalties for crimes committed through or facilitated by AI. Status: In force; Type: Law (penal amendment).
- [Decree Supreme No. 015-2025-RE — Regulation approving the implementation/regulation of Law No. 32082 \(Reglamento de la Ley N° 32082\)](#) - Regulatory details for the implementation of consular digital transformation and adoption of emerging technologies in consulates. Status: In force; Type: Supreme Decree (regulation).
- [Supreme Decree No. 115-2025-PCM — Regulation of Law No. 31814 \(Reglamento de la Ley N° 31814\)](#) - Executive regulation to operationalize Law No. 31814; described as published but with staged activation

implications. Status: Not yet in force (staged/activation pending); Type: Supreme Decree (regulation).

Key Themes and Priorities

Common themes across Peru's AI instruments include: promotion and economic development; modernization and efficiency of public services; sectoral regulation for high-impact applications (consular services, law enforcement-related recognition systems); transparency and user awareness (digital labeling proposals); education and workforce development (AI/robotics/programming in curricula); interoperability and data-sharing among public entities; and criminal deterrence for malicious AI usage. The policy mix reflects an intent to accelerate adoption while selectively regulating high-risk uses and strengthening criminal law where harms are acute.

Governance Structure

Governance is decentralized and coordination-focused. PCM is central for national policy coordination and has taken the lead in issuing regulatory instruments (e.g., Supreme Decree No. 115-2025-PCM). Sectoral ministries implement and regulate within their competences: Ministry of Foreign Affairs for consular AI use (Law 32082); Ministry of Education for curricular changes; Ministry of Transport and Communications for transport-related AI; and justice and interior authorities for penal enforcement. Administrative bodies and registries contribute to operational deployments and identity/data controls. Inter-agency cooperation mechanisms and technical working groups are a recurring feature in implementing laws.

Implementation Status

As of late 2025, several laws are active and driving implementation: Decree-Law No. 1412, Law No. 31814, Law No. 32082 and Law No. 32314 are in force. Decree Supreme No. 015-2025-RE provides regulatory detail for Law No. 32082 and is in force. Supreme Decree No. 115-2025-PCM (regulating Law No. 31814) exists but has been described as "not yet in force" pending full administrative activation in some domains. Numerous draft bills remain under consideration and will likely produce additional sectoral rules and transparency obligations (labeling, education mandates, license-plate recognition, interoperability). Implementation is therefore ongoing and staged, with PCM and sectoral ministries driving next steps.

Future Developments

Anticipate further clarification through secondary regulation, especially implementing rules for Law No. 31814 and additional sector-specific decrees. Parliamentary activity on labeling, education, and sectoral mandates may produce new obligations. Enforcement activity under Law No. 32314 will shape practical deterrence and compliance. Peru's trajectory favors incremental, sectoral rulemaking and coordination between PCM and ministries rather than a single omnibus regulatory authority.

International Context

Peru's approach — combining digital-government modernization, promotion of adoption, and penal deterrence for misuse — mirrors several jurisdictions that prioritize economic uptake while targeting high-risk uses. Peru will likely continue referencing international best practices and regional initiatives as it develops transparency, data governance and sectoral safeguards. Useful international comparators and cooperation partners can be accessed through global fora and bilateral technical cooperation available via government portals such as [Portal del Estado Peruano](#) and [Congreso de la República](#).

For the individual texts referenced above, see the internal regulation pages listed under "Regulatory Instruments" or visit central government and congressional portals: <https://www.gob.pe>, <https://www.congreso.gob.pe>, and PCM's site at <https://www.pcm.gob.pe>.

Philippines — AI Regulatory Landscape Summary

Overview

The Philippines has developed one of Southeast Asia's most comprehensive and forward-looking artificial intelligence governance frameworks, reflecting the nation's dual imperatives to harness AI for economic development while protecting citizens from AI-related harms. The regulatory approach is characterized by multi-layered governance combining foundational data protection legislation, strategic national roadmaps guiding AI adoption across government and industry, sector-specific regulatory interventions addressing urgent challenges, and pending comprehensive legislation that would establish dedicated AI regulatory authorities and rights frameworks. This layered architecture enables the Philippines to regulate AI incrementally using existing legal tools while developing specialized AI governance capacities through new institutions and frameworks. The Philippine approach emphasizes balancing innovation enablement with rights protection, economic competitiveness with worker welfare, and technological advancement with democratic safeguards. Key themes include human-centered AI ensuring technology serves Filipino society rather than purely commercial interests; responsible AI development incorporating ethics, fairness, transparency, and accountability; inclusive AI ensuring benefits reach all Filipinos including marginalized communities; and sovereign AI capabilities reducing dependence on foreign technologies. The framework positions the Philippines among global AI governance leaders, contributing to international norm development while adapting global best practices to Philippine development priorities, democratic values, and cultural contexts.

Regulatory Instruments

- [Data Privacy Act of 2012 \(Republic Act No. 10173\)](#) - Foundational data protection legislation establishing consent, data minimization, security, and accountability requirements for personal data processing including by AI systems. Enforced by the National Privacy Commission with penalties including imprisonment and substantial fines.
- [NPC Advisory No. 2024-04: Guidelines on the Application of the Data Privacy Act to AI Systems Processing Personal Data](#) - National Privacy Commission guidance (December 2024) extending data privacy protections to AI-specific contexts, addressing automated decision-making rights, algorithmic transparency, bias prevention, and enhanced protections for sensitive personal information processed by AI.
- [National AI Strategy Roadmap \(NAISR 1.0\)](#) - Initial comprehensive national AI strategy (May 2021) led by the Department of Trade and Industry, establishing framework across four dimensions: digitization and infrastructure, research and development, workforce development, and regulation and governance. Set goal of 12% GDP boost (USD 92 billion) by 2030.
- [National AI Strategy Roadmap 2.0 \(NAISR 2.0\)](#) - Updated national strategy (July 2024) expanding to seven strategic imperatives including generative AI focus, accelerated digital infrastructure, enhanced AI R&D, workforce upskilling, regulatory framework strengthening, and international cooperation. Launched with Center for AI Research (CAIR) and updated implementation targets.
- [National AI Strategy for the Philippines \(NAIS-PH\)](#) - Presidential-approved comprehensive AI framework (May 2025) representing government's official strategy across five core areas: AI infrastructure and data (26-fold HPC increase by 2028), workforce development, innovation and entrepreneurship, ethical AI and policy, and strategic AI deployment. Establishes concrete implementation roadmaps and institutional coordination mechanisms.
- [DOST AI National Roadmap](#) - Department of Science and Technology research and development framework (2019-2029) establishing AI research infrastructure, funding priorities (480 million pesos 2017-2021), AI R&D

centers at universities, and focus areas including machine learning, NLP, computer vision applied to health, agriculture, disaster resilience, and smart cities.

- [COMELEC Resolution No. 11064 \(Prohibition of AI-Generated Campaign Content\)](#) - Commission on Elections regulation (September 2024, effective September 26, 2024) for 2025 elections prohibiting deepfakes, mandating disclosure of AI-generated campaign materials, requiring digital platform registration by December 13, 2024, and establishing Task Force KKK sa Halalan for enforcement coordinating with social media platforms.
- [House Bill No. 7396 \(Artificial Intelligence Development and Regulation Act\)](#) - Pending comprehensive AI legislation (filed March 2023) proposing Artificial Intelligence Development Authority (AIDA) under Office of the President to develop national AI strategy, establish technical and ethical standards, create licensing for high-risk AI, ensure Data Privacy Act compliance, and enforce regulations coordinating across government agencies.
- [House Bill No. 7913 \(Artificial Intelligence Regulation Act - AI Bill of Rights\)](#) - Pending rights-based AI legislation (filed May 2023) establishing 'AI Bill of Rights' (safety, non-discrimination, privacy, transparency, remedy), creating Philippine Council on AI (PCAI) for policy coordination and AI Board (AIB) for supervision and enforcement, and establishing code of ethics for AI developers.
- [House Bill No. 9448 \(Protection of Labor Against Artificial Intelligence Automation Act\)](#) - Pending worker protection legislation (filed November 2023) prohibiting AI replacement of workers unless equivalent alternative employment provided, banning solely AI-driven employment decisions, protecting worker rights to object to AI evaluations, and establishing DOLE oversight of workplace AI governance policies.
- [House Bill No. 10567 \(Regulation of AI Use in 2025 Elections\)](#) - Pending deepfake disclosure legislation (filed July 2024) mandating verbal and written disclosures for AI-generated deepfakes, establishing DICT oversight coordinated with COMELEC, imposing penalties up to PHP 5 million for non-compliance, and providing expedited enforcement for electoral deepfakes during 2025 campaign periods.
- [House Bill No. 7983 \(National Center for AI Research Establishment Act\)](#) - Pending research infrastructure legislation proposing National Center for Artificial Intelligence Research (NCAIR) attached to DICT, appropriating dedicated funding for AI research infrastructure, competitive researcher salaries, nationwide research grants, and technology commercialization supporting startup ecosystem and government AI deployment.

Key Themes and Priorities

The Philippine AI regulatory framework is organized around seven interconnected priority themes. **First, human-centered and rights-protective AI:** Multiple instruments emphasize that AI must serve human flourishing rather than enabling exploitation or harm. The Data Privacy Act and NPC Advisory protect privacy and data rights. Pending HB 7913 establishes comprehensive 'AI Bill of Rights' including safety, non-discrimination, transparency, and remedy. HB 9448 protects worker rights and livelihoods. COMELEC Resolution and HB 10567 protect electoral integrity and democratic participation. This rights-first approach distinguishes the Philippines from purely economic or innovation-focused AI strategies. **Second, innovation and economic development:** NAISR 1.0, 2.0, and NAIS-PH emphasize AI as driver of economic growth, productivity, competitiveness, and Fourth Industrial Revolution readiness. DOST AI Roadmap and HB 7983 invest in research infrastructure and talent development. HB 7396 balances regulation with innovation enablement. The Philippines recognizes that AI capabilities are essential for national development and avoiding technological dependency on foreign providers. **Third, inclusive and equitable AI:** Strategic roadmaps emphasize ensuring AI benefits reach all Filipinos including rural populations, marginalized communities, and underserved sectors. Filipino language NLP, tropical agriculture applications, and disaster resilience focus address Philippine-specific needs often neglected in globally dominant AI research. Workforce development programs aim to create opportunities across socioeconomic groups rather than concentrating AI benefits among urban elites. **Fourth, responsible and ethical AI:** NPC Advisory requires bias prevention and fairness in AI systems. NAIS-PH establishes ethical AI as core pillar. HB 7913 creates code of

ethics for developers. DOST Roadmap requires responsible AI research. The framework recognizes that without deliberate ethical design, AI risks perpetuating or exacerbating discrimination, inequality, and social harms. **Fifth, worker protection and just transitions:** HB 9448's focus on preventing unjust displacement and requiring equivalent alternative employment reflects serious concerns about AI's workforce impacts, particularly for Philippines' 1.3 million BPO workers and manufacturing employees vulnerable to automation. The approach emphasizes managing technological transitions humanely rather than allowing market forces to determine outcomes. **Sixth, democratic integrity:** COMELEC Resolution and HB 10567 respond to threats AI poses to free and fair elections through deepfakes, disinformation, and manipulation. The Philippines' vibrant but sometimes contentious democracy requires special protections against AI-enabled electoral interference. **Seventh, institutional capacity and sovereignty:** Proposed AIDA, PCAI/AIB, and NCAIR, along with enhanced roles for DICT, NPC, DOST, and DOLE, reflect recognition that effective AI governance requires dedicated institutional capacity with technical expertise, legal authority, and sustained resources. Building domestic AI capabilities reduces dependence on foreign technologies and enables the Philippines to shape AI evolution according to national values.

Governance Structure

AI governance in the Philippines involves multiple agencies with specialized mandates coordinated through strategic frameworks. The **National Privacy Commission (NPC)** enforces data protection in AI contexts through the Data Privacy Act and Advisory 2024-04, conducting investigations, imposing penalties, and issuing guidance on algorithmic transparency and automated decision-making. The **Department of Information and Communications Technology (DICT)** coordinates digital infrastructure essential for AI, implements aspects of NAIS-PH, and would gain enhanced AI oversight roles under pending legislation including HB 10567 enforcement and NCAIR/AIDA coordination. The **Department of Science and Technology (DOST)** leads AI research and development through its AI National Roadmap, manages research funding via PCIEERD, operates ASTI providing high-performance computing infrastructure, and would coordinate with proposed NCAIR on research priorities. The **Department of Trade and Industry (DTI)** led development of NAISR 1.0 and 2.0, coordinates AI economic development initiatives including startup support and industry partnerships, and implements NAIS-PH economic pillars. The **Department of Labor and Employment (DOLE)** would oversee workplace AI under HB 9448 if enacted, reviewing AI governance policies, investigating worker complaints, and enforcing protections against unjust displacement. The **Commission on Elections (COMELEC)** regulates electoral AI through Resolution 11064 and would coordinate with DICT under HB 10567, operating Task Force KKK sa Halalan for monitoring and enforcement. The **National Economic and Development Authority (NEDA)** integrates AI into national development planning, ensuring alignment with broader economic and social objectives articulated in the Philippine Development Plan. Proposed new institutions include the **Artificial Intelligence Development Authority (AIDA)** under HB 7396, serving as primary AI regulator with broad coordination and enforcement powers; the **Philippine Council on AI (PCAI) and AI Board (AIB)** under HB 7913, providing policy development and enforcement respectively; and the **National Center for AI Research (NCAIR)** under HB 7983, consolidating research capacity. If multiple pending bills are enacted, coordination mechanisms would be essential to prevent fragmentation, duplication, or conflicts—potentially through consolidation during legislative process, memoranda of understanding among agencies, or designation of lead coordinating authority (likely AIDA if HB 7396 passes). The governance structure reflects understanding that AI cuts across all sectors and government functions, necessitating both specialized expertise (in privacy, labor, elections, research) and high-level coordination ensuring coherent national approach.

Implementation Status

The Philippine AI regulatory framework is at a transitional moment between established governance through existing laws and strategic plans, and potential transformation through comprehensive AI-specific legislation if pending bills are enacted. **Fully implemented and operational:** The Data Privacy Act of 2012 has been enforced for over a decade, with NPC conducting investigations, imposing penalties, and issuing guidance. NPC Advisory

2024-04 on AI took effect December 2024 and is being operationalized through agency guidance and stakeholder consultations. COMELEC Resolution 11064 is actively enforced for the May 2025 elections, with digital platform registration completed December 13, 2024, and Task Force KKK monitoring campaign activities. NAISR 1.0 guided AI initiatives from 2021-2024, with measurable progress on infrastructure, research funding, and policy development. DOST AI Roadmap has funded 480 million pesos in AI research 2017-2021, established AI R&D centers at universities, and delivered research outputs in health, agriculture, and disaster management. **Recently launched and scaling:** NAISR 2.0 (July 2024) and NAIS-PH (May 2025) represent current governing strategies, with implementation underway through agency work plans, budget allocations, and multi-stakeholder coordination. NAIS-PH's ambitious infrastructure targets (26-fold HPC increase by 2028) and workforce development goals require sustained multi-year implementation. The Center for AI Research (CAIR) launched with NAISR 2.0 is in operational establishment phase. **Pending legislative consideration:** Five House Bills (7396, 7913, 9448, 10567, 7983) remain in committee review as of early 2025. Legislative observers note that with May 2025 elections approaching and Congress nearing adjournment, passage timeline is uncertain. Bills may be enacted individually, consolidated into comprehensive AI legislation, further amended based on stakeholder input, or delayed to future congressional sessions. The pending legislation represents potential quantum leap in AI governance comprehensiveness, but current governance operates under existing authorities. **Challenges in implementation** include coordination complexity across multiple agencies with overlapping or adjacent AI mandates; resource constraints limiting DICT, NPC, DOLE, and other agencies' capacity to develop specialized AI expertise and enforcement capabilities; technological complexity requiring regulators to keep pace with rapidly evolving AI capabilities; and balancing competing priorities of innovation, rights protection, and economic competitiveness requiring difficult tradeoffs. **International engagement:** The Philippines actively participates in ASEAN digital economy initiatives, UNESCO AI ethics discussions, and engagement with OECD AI governance frameworks, contributing Philippine perspectives while learning from comparative experiences and maintaining regulatory interoperability with major trading partners.

Future Developments

The Philippine AI regulatory landscape will evolve significantly in coming years through multiple anticipated developments. **Legislative enactment decisions (2025-2026):** The fate of five pending House Bills will profoundly shape AI governance. If enacted, HB 7396 would establish AIDA as cross-cutting AI regulator potentially consolidating fragmented authorities. HB 7913's AI Bill of Rights would enshrine fundamental protections likely influencing jurisprudence and cultural norms around AI. HB 9448 would make Philippines among first countries to legislatively protect workers from AI displacement. HB 10567 would formalize deepfake regulation beyond electoral contexts. HB 7983 would create dedicated AI research institution competing with regional AI powerhouses. Legislative outcomes depend on congressional priorities, stakeholder negotiations balancing innovation and protection, budget feasibility particularly for NCAIR and AIDA establishment, and coordination among bills potentially requiring consolidation. **Implementation of NAIS-PH (2025-2028):** The presidential-approved strategy provides roadmap for infrastructure development (HPC expansion, data centers, connectivity), workforce development (AI training programs, curriculum integration, talent retention), innovation ecosystems (startup support, research commercialization, public-private partnerships), ethical AI policy (fairness standards, transparency requirements, accountability frameworks), and strategic deployment across health, education, agriculture, disaster management, and public services. Success requires sustained budget commitments, effective inter-agency coordination, and measurement against concrete targets. **Agency capacity building:** Regardless of new legislation, existing agencies (NPC, DICT, DOST, DOLE, COMELEC) will expand AI-specific capabilities through hiring technical experts, developing specialized training programs, deploying AI detection and analysis tools, and establishing international partnerships with peer regulatory authorities. **2025 elections as proving ground:** The May 2025 elections will test COMELEC Resolution 11064's effectiveness in preventing AI-generated manipulation, potentially informing permanent electoral AI regulations and demonstrating (or challenging) Philippines' capacity to protect democracy from AI threats. **Private sector AI adoption:** As Philippine businesses increasingly deploy AI in customer service, operations, hiring, and decision-making, practical governance challenges will emerge informing regulatory refinement. BPO sector's response to

automation, financial institutions' use of AI credit scoring, and healthcare AI adoption will generate case studies and stakeholder feedback. **Regional and international alignment:** The Philippines will continue engaging with ASEAN on regional AI frameworks, adapting global standards (EU AI Act, OECD principles, UNESCO recommendations) to Philippine context, and potentially influencing regional norm development as Southeast Asian AI governance leader. **Technological evolution:** Advances in generative AI, large language models, autonomous systems, and emerging capabilities will require regulatory adaptation, potentially through AIDA/PCAI if established or through existing agencies' expanded authorities. The framework's flexibility and responsiveness to technological change will be tested. **Public awareness and digital literacy:** Government and civil society initiatives to educate Filipinos about AI opportunities, risks, rights, and literacy will influence public acceptance, participation in governance, and effectiveness of protections. Overall, the Philippines appears committed to comprehensive, rights-protective, innovation-enabling AI governance, with trajectory toward increasingly sophisticated institutional capacity and regulatory frameworks positioning the nation among global AI governance leaders while advancing development objectives.

International Context

The Philippine AI governance approach demonstrates significant alignment with international frameworks while maintaining distinctive priorities reflecting national context. The framework incorporates principles from the **OECD AI Principles** including human-centered values and fairness, transparency and explainability, robustness and safety, and accountability—evident in NAIS-PH's ethical AI pillar, NPC Advisory's fairness requirements, and HB 7913's rights-based approach. The emphasis on multi-stakeholder governance reflects OECD's participatory model. Alignment with **UNESCO's Recommendation on the Ethics of AI** is visible in commitments to human rights protection (HB 7913's AI Bill of Rights), sustainable development (NAISR/NAIS-PH linking AI to development goals), inclusion and non-discrimination (addressing digital divide, Filipino language technologies), and cultural diversity (adapting global AI to Philippine values and contexts). The Philippines contributed to UNESCO's development of these principles and implements them more comprehensively than many countries. Resonance with the **EU AI Act** appears in risk-based regulatory approaches (high-risk AI facing enhanced requirements in pending legislation), prohibited uses (deepfakes in COMELEC Resolution and HB 10567), transparency requirements (disclosure obligations, algorithmic explainability), and fundamental rights protections (data privacy, non-discrimination). However, the Philippine framework currently lacks the EU's detailed technical specifications and conformity assessment procedures, operating at higher level of principles and strategic direction. The rights-based approach mirrors the **U.S. Blueprint for an AI Bill of Rights** (White House OSTP 2022) in articulating explicit individual protections (safety, non-discrimination, privacy, transparency, remedy) though the Philippine HB 7913 proposes legislative codification rather than voluntary principles. The worker protection focus in HB 9448 reflects concerns prominent in **ILO frameworks on the future of work and just transitions**, positioning the Philippines among countries seriously addressing AI labor impacts legislatively rather than relying on general labor law application. The Philippines' comprehensive strategic approach (NAISR, NAIS-PH) aligns with national AI strategies in **Singapore, South Korea, Japan, UK, France, Canada, and other AI-ambitious nations**, emphasizing infrastructure, talent, research, innovation ecosystems, and governance. The Philippine strategy's explicit development focus (poverty reduction, inclusive growth, sovereign capabilities) reflects emerging economy priorities distinguishing it from advanced economy strategies emphasizing technological leadership or geopolitical competition. The electoral integrity focus (COMELEC Resolution, HB 10567) aligns with democratic protection efforts in **EU, U.S., Taiwan, and other democracies** combating AI-enabled disinformation, though few countries have implemented regulations as rapidly ahead of elections. The Philippines' framework is notably more advanced and comprehensive than most Southeast Asian neighbors, positioning it as potential regional leader influencing **ASEAN AI governance** development. While Singapore leads in AI deployment and economic application, the Philippines may lead in rights-protective and worker-focused regulation, contributing complementary perspectives to regional approaches. The framework's comprehensiveness, rights emphasis, and democratic protection focus position the Philippines among global AI

governance innovators, contributing to international norm development while adapting best practices to national priorities, potentially influencing other emerging democracies facing similar AI opportunities and risks.

Poland — AI Regulatory Landscape Summary

Overview

Poland's AI regulatory framework is currently a hybrid of strategic policy documents, targeted sectoral legislation, and draft primary laws intended to create a coherent domestic regime aligned with wider European rules. Foundational strategic texts (Assumptions to AI Strategy; Memorandum; Roadmap; and the 2019–2027 Policy) established priorities such as digital public services, research & development, workforce reskilling, and open science. At the statutory level, the [Act on Open Data and Re-use of Public Sector Information](#) is in force and functions as a key enabling law for AI access to public datasets. Complementing these are draft bills — notably the Draft Act on Data Management and the Draft Act on Artificial Intelligence Systems — plus horizon strategies (Strategy for the Digitization of Poland to 2035, draft Policy to 2030) that extend strategic planning to mid-century ambitions.

Regulatory Instruments

- [Assumptions to AI Strategy in Poland \(Proposition for an AI Strategy; Plan of activities of the Ministry of Digital Affairs\)](#) - Early strategic/propositional document establishing national AI priorities, proposing institutional responsibilities and a plan of activities. Status: Enacted/Published (strategy paper). Type: Strategic guidance.
- [Memorandum for the Development of Artificial Intelligence in Poland](#) - Memorandum setting out principles for public-private collaboration, investment priorities, and initial coordination mechanisms. Status: Enacted/Published. Type: Policy memorandum.
- [Roadmap for the Development of Artificial Intelligence in Poland \(Mapa drogowa rozwoju sztucznej inteligencji w Polsce\)](#) - Actionable roadmap identifying short- and medium-term tasks, pilot projects, and institutional leads. Status: Enacted/Published. Type: Roadmap/implementation plan.
- [Policy for the Development of Artificial Intelligence in Poland from 2020 – Polityka rozwoju sztucznej inteligencji w Polsce na lata 2019–2027](#) - Comprehensive multi-year policy framing investment, research funding, education and public sector adoption through 2027. Status: Enacted/Published. Type: Multi-year national policy.
- [Act on Open Data and Re-use of Public Sector Information \(Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego\)](#) - Legal framework for publication and reuse of public sector datasets; technical standards, licensing and reuse rules. Status: In force. Type: Statutory law.
- [Draft Act on Data Management \(Projekt ustawy o zarządzaniu danymi\)](#) - Draft legislation proposing national data governance architecture including stewardship, catalogues, supervised access rules and mechanisms for sharing sensitive datasets. Status: Draft. Type: Draft primary legislation.
- [Draft Act on Artificial Intelligence Systems \(Projekt ustawy o systemach sztucznej inteligencji\)](#) - Draft bill that would set provider/deployer obligations, risk classification, transparency and conformity assessment procedures. Status: Draft. Type: Draft primary legislation.
- [Strategy for the Digitization of Poland to 2035 \(Strategia Cyfryzacji Polski do 2035\)](#) - Long-term digital transformation strategy linking infrastructure, public services and economic development goals. Status: Draft. Type: Strategic long-term plan.
- [Policy for the Development of Artificial Intelligence in Poland to 2030 \(Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku\) – draft](#) - Draft update of national AI policy extending goals to 2030 emphasizing EU alignment, skills and trustworthy AI. Status: Draft. Type: Draft national policy.

Key Themes and Priorities

Across documents, common priorities are: 1) data availability and interoperability (publishing public data, creating data catalogues, enabling supervised access); 2) public sector modernization (deploying AI in public administration to improve services and efficiency); 3) research & innovation (supporting R&D, startups and AI clusters); 4) skills and education (reskilling, STEM and vocational programs); 5) trust, ethics and accountability (transparency, human oversight and risk management); and 6) international alignment (with EU rules, OECD recommendations and standards bodies). The draft legislative texts focus on operationalizing these priorities by introducing governance mechanisms, compliance duties and enforcement models.

Governance Structure

Lead responsibility for AI policy is allocated to central digital and economic ministries (historically the Ministry of Digital Affairs / Ministerstwo Cyfryzacji and relevant ministries for innovation, economy and health depending on sectoral use-cases). Coordination is delivered through inter-ministerial working groups, taskforces and partnerships with research agencies and universities. The national data protection authority (Urząd Ochrony Danych Osobowych) retains a critical role in supervising personal data uses in AI systems. Implementation of future conformity assessment and enforcement for AI may involve newly designated bodies or the extension of existing regulator remits.

Implementation Status

As of the retrieval date, strategic documents are published and guiding programmes, while binding legal instruments are mixed: the Open Data Act is in force and operational; the Draft Act on Data Management and Draft Act on Artificial Intelligence Systems are pending and require legislative processes (consultation, amendment and parliamentary adoption). Practical workstreams include pilot programs for public sector AI, the establishment of data catalogues, and stakeholder consultations on draft laws. Administrative capacity and resourcing (for conformity assessment, audits and enforcement) remain priorities identified in policy texts.

Future Developments

Near-term developments to watch include parliamentary progress on the two draft acts, publication of implementing regulations or guidance for the Open Data Act, and finalization of the 2035 digitization strategy and 2030 AI policy. Poland intends to align national law with the EU AI Act and associated delegated/regulatory acts, so legislative drafts are expected to be adjusted for compatibility. Strengthening institutional oversight, investing in conformity assessment infrastructure and further specifying rules for high-risk AI applications are likely next steps.

International Context

Poland frames national AI policy within EU and international frameworks. Policymakers reference the [European approach to AI](#), OECD AI principles and EU data governance initiatives. The country aims for regulatory interoperability to support cross-border services and compliance with the EU AI Act. For official national sources, see the Ministry portal [Ministry of Digitalisation](#) and the legal acts database [ISAP](#).

Sources and further reading: official strategy and policy documents published by the Polish government and draft bills available through government portals and the parliamentary legal acts database.

Portugal — AI Regulatory Landscape Summary

Overview

Portugal's AI policy and regulatory ecosystem in 2025 is characterised by a stacked approach combining strategic national plans, sectoral guidance for the public administration, statutory rights protections, and direct incorporation of the EU Artificial Intelligence Act into national practice. The principal objective of the combined instruments is to accelerate safe AI adoption, build national capacity (including sovereign models), and ensure human-centred and rights-respecting deployment.

Regulatory Instruments

- [AI Portugal 2030 \(Estratégia Nacional para a Inteligência Artificial\)](#) - National strategy setting long-term goals for research, skills, start-ups, public sector modernization and international cooperation. Status: Enacted/Published. Type: Strategy/Policy document.
- [Lei n.º 27/2021 — Portuguese Charter of Human Rights in the Digital Age](#) - Legal framework recognising and protecting digital rights and establishing principles for the use of technologies that affect fundamental rights. Status: In force. Type: Statute / Rights Charter.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(EU\)](#) - EU-wide, directly applicable regulation that sets a risk-based compliance framework, obligations for high-risk systems, transparency rules, market surveillance, and conformity assessment procedures. Status: Enacted/Published (EU Regulation). Type: Supranational regulation (directly applicable).
- [Resolução do Conselho de Ministros n.º 207/2024 — Approval of the Estratégia Digital Nacional](#) - Government resolution formally approving and directing implementation of the national digital strategy. Status: Enacted/Published. Type: Government resolution / policy mandate.
- [Estratégia Digital Nacional \(National Digital Strategy, includes Agenda Nacional de IA\)](#) - Broader national plan to digitalise public services, promote digital skills and include the national AI agenda as a pillar. Status: Enacted/Published. Type: Strategy/Policy document.
- [Resolução do Conselho de Ministros n.º 201/2024 — Approval of the development of a Portuguese LLM \(AMÁLIA\) and mandate to prepare the Agenda Nacional de IA](#) - Authorises development of a national large language model (AMÁLIA) and tasks relevant bodies to draft the national AI agenda. Status: Enacted/Published. Type: Government resolution / operational mandate.
- [Decreto-Lei n.º 49/2024 — Rules on the provision of digital services by the Public Administration \(gov.pt omnichannel\)](#) - Sets obligations for delivery, accessibility, interoperability and continuity of digital public services; relevant to how public bodies procure and operate AI systems. Status: In force. Type: Decree-law / administrative regulation.
- [Agenda Nacional de Inteligência Artificial \(National AI Agenda / ANI\) — planned national AI agenda \(in public consultation/auscultation\)](#) - Draft national AI agenda that translates strategic objectives into operational priorities, governance arrangements and investment plans. Status: Draft (public consultation). Type: Draft policy / national agenda.
- [Guia para uma Inteligência Artificial ética, transparente e responsável na Administração Pública \(AMA Guide\)](#) - Practical guidance for public administrations on procurement, design, deployment, oversight and transparency of AI systems. Status: Enacted/Published. Type: Administrative guidance / best practice.

Key Themes and Priorities

Common themes across instruments include: a risk-based stance aligned with the EU AI Act; emphasis on human rights and digital rights protection (Lei n.º 27/2021); public-sector modernization, service continuity and accessibility (Decreto-Lei n.º 49/2024; AMA Guide); national capacity building and sovereign AI initiatives (AMÁLIA); and stakeholder engagement through public consultation on the Agenda Nacional de IA. Transparency, accountability, safe innovation and fostering an ecosystem for research and industry are constant priorities.

Governance Structure

Governance is cross-cutting: strategic direction is provided by the Governo and Conselho de Ministros through Resoluções (RCM n.º 201/2024 and RCM n.º 207/2024). Operational implementation and public administration transformation are anchored at the Agência para a Modernização Administrativa (AMA) which provides the AMA Guide and leads gov.pt modernization. Data protection and privacy oversight remains with the Comissão Nacional de Proteção de Dados (CNPD). Under the EU AI Act, Portugal will (or has begun to) identify national competent authorities and market surveillance authorities to enforce the Regulation's requirements; the Agenda Nacional de IA is expected to specify national roles, responsibilities and funding mechanisms.

Implementation Status

As of late 2025, foundational statutes and administrative rules (Lei n.º 27/2021; Decreto-Lei n.º 49/2024) are in force and informing public procurement and deployments. The EU AI Act is applicable EU-wide and dictates obligations across sectors; Portugal's national instruments and guidance are being adjusted to ensure compliance and to create coherent enforcement arrangements. The Agenda Nacional de IA remains in public consultation, seeking input to define timelines, institutional remits and operational measures. The AMÁLIA initiative is in active development following the government mandate in RCM n.º 201/2024.

Future Developments

Key near-term developments to monitor include: designation of national competent authorities and market surveillance bodies for the EU AI Act; finalisation and adoption of the Agenda Nacional de IA (moving from draft/auscultation to approved plan); operational roll-out and procurement decisions related to AMÁLIA; and further sectoral guidance or implementing rules to harmonise national legislation and administrative practice with EU requirements. Stakeholder consultation outcomes will shape specific timelines, funding instruments and compliance support programmes.

International Context

Portugal's regulatory posture is closely aligned with EU law as the primary reference framework. The national strategy and public-sector guidance aim to maximise the benefits of the EU single market while safeguarding rights. For further reading, principals sources include the EU text for the AI Act ([Regulation \(EU\) 2024/1689 — AI Act](#)) and national modernization resources such as the Agência para a Modernização Administrativa ([AMA — Agência para a Modernização Administrativa](#)).

Summary conclusion: Portugal combines forward-looking strategic investment in AI capacity and sovereign capability with robust public-sector guidance and rights-based legal safeguards, while relying on the EU AI Act as the decisive legal instrument for market regulation. The Agenda Nacional de IA and implementation choices (including enforcement architecture and operational safeguards for AMÁLIA) will determine the detailed shape of Portuguese AI governance over the next 2–3 years.

Qatar — AI Regulatory Landscape Summary

Overview

Qatar's artificial intelligence (AI) regulatory landscape is a layered mix of a general personal data protection statute, a national strategic roadmap, an inter-ministerial coordinating body, sectoral guidance documents, and ethical principles published by national ministries and agencies. The system emphasizes enabling AI for economic growth and government modernization while managing cybersecurity, privacy and ethical risks. The principal instruments are the Personal Data Privacy Protection Law (Law No. 13 of 2016), the Qatar National Artificial Intelligence Strategy, Cabinet Decision No. (10) of 2021 creating the Artificial Intelligence Committee, the Qatar Digital Agenda 2030, the National Cyber Security Agency's Guidelines for Secure Adoption and Use of Artificial Intelligence, the Qatar Central Bank Artificial Intelligence Guideline for QCB-licensed Entities, and two Ministry of Communications and Information Technology (MCIT) documents on ethical development/deployment and on ethical use. Together these documents form a policy and governance architecture that is strategic, agency-driven, and sectorally differentiated.

Regulatory Instruments

- [Law No. 13 of 2016 Concerning Personal Data Privacy Protection \(Personal Data Protection Law\)](#) - Status: In force. Type: National statute. Description: Provides the legal framework for the lawful processing, collection, storage and transfer of personal data in Qatar. While not AI-specific, it sets binding obligations and data subject rights that govern AI systems processing personal data.
- [Qatar National Artificial Intelligence Strategy \(National AI Strategy\)](#) - Status: Enacted/Published. Type: National strategy/policy document. Description: Sets strategic objectives to harness AI for economic diversification, public sector innovation, talent development, and research; acts as a roadmap rather than prescriptive regulation.
- [Cabinet Decision No. \(10\) of 2021 establishing the Artificial Intelligence Committee](#) - Status: Enacted/Published. Type: Executive decision / governance instrument. Description: Establishes a cabinet-level committee to coordinate AI policy across ministries, align AI initiatives with the national strategy, and supervise implementation efforts.
- [Qatar Digital Agenda 2030](#) - Status: Enacted/Published. Type: National digital transformation agenda. Description: Integrates digital priorities with national development goals and situates AI within broader aims for public service modernization and digital economy growth.
- [Guidelines for Secure Adoption and Use of Artificial Intelligence \(National Cyber Security Agency\)](#) - Status: Enacted/Published. Type: Agency guidance / cybersecurity standard. Description: Provides recommended cybersecurity practices, risk assessments, and operational measures to secure AI systems and reduce attack surface introduced by AI deployments.
- [Qatar Central Bank Artificial Intelligence Guideline for QCB-licensed Entities](#) - Status: Enacted/Published. Type: Regulatory guideline / supervisory standard. Description: Directed at QCB-licensed financial institutions; addresses model governance, risk management, third-party oversight, explainability, audit trails and consumer protection; carries supervisory force for entities under QCB jurisdiction.
- [Principles and Guidelines for Ethical Development and Deployment of Artificial Intelligence \(MCIT\)](#) - Status: Enacted/Published. Type: Ministry-issued ethical framework. Description: Sets out ethical principles (e.g., transparency, fairness, accountability, safety) and recommended implementation practices for developers and deployers of AI in Qatar.

- [Principles and Guidelines for Ethical Use of Artificial Intelligence \(MCIT\)](#) - Status: Enacted/Published. Type: Ministry-issued guidance. Description: Focuses on responsible use by organizations and public bodies, including governance structures, human oversight, rights protection, and public-sector adoption practices.

Key Themes and Priorities

Across Qatar's documents several consistent priorities appear: (1) enabling AI-driven economic diversification and public-sector efficiency; (2) protecting personal data and privacy; (3) securing AI systems against cybersecurity threats; (4) promoting ethical and accountable AI development and use; and (5) building national capacity for research, talent and standards. The state's approach is pragmatic: favor guidance, capacity building and sectoral supervision over comprehensive prescriptive legislation targeted solely at AI (so far), while relying on existing statutes (notably the personal data law) and supervisory powers in sensitive sectors (like finance) to impose specific requirements.

Governance Structure

Institutional roles are distributed across: (a) the Artificial Intelligence Committee (Cabinet level) for overall coordination and strategy alignment; (b) the Ministry of Communications and Information Technology (MCIT) for policy leadership, standards and ethical guidance; (c) the National Cyber Security Agency (NCSA) for technical and security guidance; (d) sectoral regulators such as the Qatar Central Bank (QCB) which issue binding supervisory guidelines for regulated entities; and (e) line ministries, government agencies and state-owned enterprises that operationalize AI in public services. This federated governance model combines top-level strategic steering with agency-specific rulemaking and supervision.

Implementation Status

Most instruments are published and in effect as strategies or guidance. The Personal Data Privacy Protection Law is the main binding statute relevant to AI applications that process personal data. The QCB guideline is supervisory and applies concretely to licensed financial institutions. MCIT and NCSA principles and guidelines are published and promoted across government and industry; they function as authoritative best practices and are expected to inform procurement, audits, and future sectoral rules. Implementation challenges include translating high-level principles into standards, building technical and audit capacity, establishing operational certification or testing regimes, and clarifying the enforceability of ethical guidelines for private actors.

Future Developments

Expected future steps include greater operationalization of strategy through technical standards, incorporation of MCIT/NCSA recommendations into procurement and certification mechanisms, possible sectoral rulemaking by regulators (banking, telecommunications, health), enhancement of data protection enforcement (and potential establishment of a dedicated data protection authority), and iterative updates to reflect international standardization work (ISO, IEEE) and best practices. Stakeholders should monitor announcements from the Artificial Intelligence Committee, MCIT and sectoral regulators for implementation roadmaps and compliance timelines.

International Context

Qatar's approach aligns with many international policy trajectories: a focus on enabling innovation, protecting privacy, securing critical infrastructure, and promoting ethical AI. The emphasis on ethical principles and agency guidance mirrors non-binding international frameworks (OECD principles, G20 discussions) while sectoral supervisory activity (e.g., by QCB) reflects global practice in financial regulation. Qatar is also positioning its national strategy and digital agenda to attract investment and to participate in regional and global standard-setting discussions.

For further reference and primary sources visit official portals such as [Government Communications Office \(GCO\)](#), [Qatar Central Bank \(QCB\)](#), [Ministry of Communications and Information Technology \(MCIT\)](#), and the [National Cyber Security Agency \(NCSA\)](#). Monitoring these agencies will provide the most up-to-date information on binding requirements, supervisory expectations and implementation timelines.

Romania — AI Regulatory Landscape Summary

Overview

Since late 2022 Romania has pursued a coordinated, multi-instrument approach to artificial intelligence, combining high-level strategic documents, interinstitutional coordination (including security council decisions), ministerial orders to stand up governance bodies, targeted draft laws addressing specific harms and broader draft legislation to regulate AI nationally. The architecture prioritizes (1) building institutional capacity for oversight and coordination, (2) aligning national rules and implementation mechanisms with EU developments, (3) enabling research, innovation and public sector adoption, and (4) addressing emergent harms such as deepfakes and cybersecurity risks. The principal published instruments include government memoranda (November 2022 and April 2024), CSAT Decision No. 148/27.09.2022, Ministerial Order No. 20.484/2023, the National Strategy 2024–2027 (HG 832/2024) and multiple draft laws under parliamentary review.

Regulatory Instruments

- Romanian AI Act Implementation Law (candidate title) - Draft national implementing instrument intended to operationalize AI regulatory obligations and align domestic enforcement and procedural rules with EU AI law and national policy. (Status: Draft; Type: Implementation law / regulatory framework)
- [Government Memorandum No. 20D/31781/MN on Artificial Intelligence](#) - Establishes foundational national AI initiatives and initial governance structures to coordinate policy across ministries. (Status: Passed; Type: Government memorandum / coordination instrument)
- [Government Memorandum \(11 November 2022\) regarding the establishment of the Romanian Committee for Artificial Intelligence and related initiatives](#) - Formal decision to create a national committee and launch core initiatives in AI policy and coordination. (Status: Enacted/Published; Type: Government memorandum)
- [Government Memorandum \(11 November 2022\) — Memorandum on establishing the Romanian Committee for Artificial Intelligence](#) - Companion memorandum establishing governance modalities and cross-ministerial engagement. (Status: Enacted/Published; Type: Government memorandum)
- [Decision of the Supreme Council of National Defence \(CSAT\) nr. 148/27.09.2022 — Interinstitutional Commission for National AI Strategy](#) - Security council decision establishing an interinstitutional commission to draft a national AI strategy. (Status: Enacted/Published; Type: National security / interinstitutional decision)
- [Decision of the Supreme Council of National Defence No. 148 \(27 September 2022\) establishing the Interinstitutional Commission for the elaboration of Romania's National Strategy on Artificial Intelligence](#) - Reiterates CSAT mandate to coordinate strategic drafting. (Status: Enacted/Published; Type: National security decision)
- [Cadru Strategic National în domeniul Inteligenței Artificiale \(CSN-IA\)](#) - National Strategic Framework for AI submitted to public consultation (Oct 2023); outlines principles, sectoral objectives and governance approaches. (Status: Draft for consultation; Type: Strategic framework)
- [Order of the Minister of Research, Innovation and Digitalization No. 20484/2023](#) - Establishes, organizes and sets functioning rules for the Romanian Committee for Artificial Intelligence. (Status: Enacted/Published; Type: Ministerial order / administrative instrument)
- [Ordinul nr. 20.484/2023 — Order regarding the establishment, organization and functioning of the Romanian Committee for Artificial Intelligence](#) - Romanian language text of the same ministerial order governing the Committee's role and procedures. (Status: In force; Type: Administrative order)

- [Law on the responsible use of technology in the context of the deepfake phenomenon \(PL-x No. 471/2023\)](#) - Proposed targeted law addressing the manufacture, dissemination and misuse of synthetic media; focuses on responsibility, potential sanctions and protective measures. (Status: Under review; Type: Proposed sectoral law)
- [Law on Artificial Intelligence \(proposed\) \(B154/2024\)](#) - Parliamentary draft law proposing a comprehensive domestic AI regulatory regime; aims to define obligations for developers and deployers, oversight roles and enforcement tools. (Status: Proposed/Under review; Type: Proposed national law)
- [Draft Law B154/2024 — Proposal regarding Artificial Intelligence](#) - Text of the legislative proposal put forward in 2024 containing substantive regulatory measures and definitions. (Status: Under review; Type: Draft legislation)
- [Proposed law regarding Artificial Intelligence — B.154/2024](#) - Alternative reference to the same legislative initiative; stakeholders track this slug for parliamentary debates and amendments. (Status: Proposed; Type: Parliamentary bill)
- [Government Memorandum \(23 April 2024\) — National coordination committee for data, digital services and AI](#) - Establishes cross-cutting coordination to align data policy, digital services and AI governance. (Status: Enacted/Published; Type: Government memorandum)
- [Memorandum of Understanding between the Government of Romania and Google \(15 July 2024\)](#) - Non-binding cooperation agreement on cloud, infrastructure, cybersecurity and advanced technologies to support public sector transformation. (Status: Enacted/Published; Type: MoU / public-private cooperation)
- [National Strategy in the field of Artificial Intelligence 2024–2027](#) - The government's multi-year strategy setting objectives, priority actions, funding lines and governance for AI adoption and risk management. (Status: Enacted/Published; Type: National strategy)
- [Hotărârea Guvernului nr. 832/2024 — National Strategy in the Field of Artificial Intelligence 2024–2027](#) - Government decision formally adopting the National Strategy. (Status: Enacted/Published; Type: Government decision / strategy)
- [National Strategy in the field of Artificial Intelligence 2024–2027 \(Strategia națională în domeniul inteligenței artificiale 2024–2027\)](#) - Romanian language publication of the 2024–2027 strategy text. (Status: In force; Type: Strategy document)

Key Themes and Priorities

Across instruments, Romania emphasizes: institution building (committees, interministerial commissions), EU alignment (preparing to implement EU AI Act obligations), enabling infrastructure (cloud and digital services partnerships), risk management (deepfake controls, cybersecurity), ethical and trustworthy AI principles, public sector adoption and skills development. The strategy sets concrete priorities for research funding, public procurement of AI, data sharing between public bodies, and partnerships with the private sector.

Governance Structure

Principal governance actors include the Romanian Committee for Artificial Intelligence (established by ministerial order), the Interinstitutional Commission created under CSAT Decision No. 148, the national coordination committee for data, digital services and AI (established April 2024), relevant ministries (Research, Innovation and Digitalization; Interior; Justice; Defense; Economy; Education), and sectoral regulators which will hold domain responsibilities. The Committee is the primary advisory and coordination body shaping guidance, standards and public consultations.

Implementation Status

Many strategic and administrative measures are already in force: the Committee (Ordinul nr. 20.484/2023) is operational, and the National Strategy 2024–2027 (HG 832/2024) is enacted. Legislative instruments remain under review: Bill B154/2024 and PL-x No. 471/2023 (deepfake law) are active parliamentary files. The candidate implementation law remains a draft and is expected to be coordinated with EU obligations. Operational rulemaking, secondary guidance and technical standards are expected to be issued by the Committee and relevant ministries as draft laws proceed through parliament.

Future Developments

Key near-term developments to monitor: parliamentary progress and amendments to B154/2024; any national implementing legislation for the EU AI Act; implementing guidance and technical standards produced by the Committee; roll-out of strategy measures (funding calls, cloud procurement, public sector pilots); and potential new rules stemming from deepfake legislation. Bilateral and private-sector partnerships (e.g., the 15 July 2024 MoU with Google) will influence infrastructure and capability timelines.

International Context

Romania's framework is explicitly EU-oriented: strategic and legislative efforts aim to ensure compatibility with EU regulatory developments and to leverage EU funding and cooperation. The government has also pursued bilateral public-private agreements to secure cloud and cybersecurity capabilities. For official texts and further reference see the government's AI portal: [https://\[government AI portal\]](https://[government AI portal]) and other official publications linked in the Regulations section above. Additional authoritative sources and draft texts are published on ministry websites and parliamentary records; practitioners should consult official repositories for the latest enacted texts and committee outputs.

Russia — AI Regulatory Landscape Summary

Overview

Russia's AI regulatory framework reflects a state-led development strategy shaped by geopolitical considerations, Western sanctions, and emphasis on technological sovereignty. The approach combines aspirational national strategies, experimental legal regimes allowing controlled innovation, mandatory liability frameworks, and voluntary ethical principles. Unlike the EU's comprehensive ex-ante regulation, Russia favors experimentation first, then regulation based on observed outcomes. The framework prioritizes domestic technological capabilities, national security applications, and strategic autonomy from Western AI suppliers, with international cooperation focused primarily on BRICS partners rather than Western multilateral frameworks.

Regulatory Instruments

- [National Strategy for the Development of Artificial Intelligence until 2030](#) - Foundational policy document establishing Russia's AI development priorities across healthcare, education, transportation, manufacturing, and defense sectors, with targets for domestic technological capabilities and reduced foreign dependence. Adopted via Presidential Decree No. 490 in October 2019.
- [Federal Law on Experimental Legal Regimes in the Sphere of Digital Innovations \(Federal Law No. 258-FZ\)](#) - Establishes regulatory sandboxes allowing companies to test AI innovations with temporary exemptions from standard regulations. Enables practical deployment of autonomous vehicles, AI diagnostics, and algorithmic trading under controlled conditions with centralized ministerial approval.
- [Code of Ethics in the Field of Artificial Intelligence](#) - Voluntary ethical principles emphasizing human agency, transparency, fairness, and protection of vulnerable populations. Adopted in October 2021, influences corporate AI policies among major Russian technology companies and state-owned enterprises, though legally non-binding.
- [Updated National Strategy for the Development of Artificial Intelligence until 2030 \(Presidential Decree No. 124\)](#) - February 2024 update addressing Western sanctions impacts, prioritizing domestic semiconductor manufacturing, alternative supply chains through friendly nations, defense applications, and BRICS cooperation. Reflects Russia's pivot toward technological sovereignty in response to geopolitical isolation.
- [Federal Law on AI Liability and Updated Experimental Legal Regimes \(Federal Law No. 123-FZ\)](#) - Establishes mandatory civil liability insurance for AI developers in experimental regimes, addresses attribution challenges when AI systems cause harm, and creates risk-scaled insurance requirements. High-risk applications in healthcare, transportation, and financial services face stricter compliance obligations. Adopted July 2024.

Key Themes and Priorities

- **Technological Sovereignty:** Reducing dependence on Western AI technologies, semiconductors, and cloud infrastructure through domestic development and alternative supply chains via BRICS partnerships.
- **State-Led Development:** Centralized government coordination of AI research, development, and deployment, with priority funding for sectors aligned with national security and economic objectives.
- **Experimental Innovation Model:** Regulatory sandboxes allowing controlled testing of AI systems before imposing permanent regulations, favoring practical experimentation over comprehensive ex-ante restrictions.
- **Sanctions Response:** Strategic adaptation to Western export controls on semiconductors and AI hardware, prioritizing algorithms optimized for less advanced hardware and domestic manufacturing capabilities.

- **Defense and Security Applications:** Priority resource allocation for military AI, surveillance systems, autonomous weapons, and intelligence applications over consumer services.
- **Liability and Risk Management:** Mandatory insurance frameworks addressing AI-related harm, with risk-based requirements scaled to application danger levels in healthcare, transportation, and finance.
- **BRICS Cooperation:** Strategic AI partnerships with China, India, Brazil, and South Africa as alternatives to Western multilateral frameworks, including joint standards development and technology transfer.
- **Ethical Principles:** Voluntary commitment to human agency, transparency, fairness, and protection of vulnerable groups, though enforcement remains limited to major companies and state enterprises.
- **Infrastructure Development:** Investment in computing infrastructure, data centers, and high-performance computing capabilities to support domestic AI ecosystem.
- **Talent Development:** Educational initiatives, research funding, and incentives to retain AI talent domestically amid brain drain to Western technology hubs.

Governance Structure

- **Ministry of Digital Development, Communications, and Mass Media:** Primary coordinating authority for AI policy implementation since July 2024, responsible for federal AI project execution and international cooperation. Replaced Ministry of Economic Development as lead AI agency.
- **Ministry of Economic Development:** Evaluates experimental legal regime applications, assesses company backgrounds and finances, and coordinates with sectoral ministries before governmental approval of sandboxes. Formerly led AI coordination until 2024 transition.
- **Presidential Administration:** Issues strategic decrees establishing and updating national AI strategy, sets high-level priorities, and coordinates inter-ministerial efforts on AI development.
- **Technical Committee for Standardization No. 164 "Artificial Intelligence":** Brings together over 120 specialized companies and government agencies to develop technical standards for AI systems, ensuring interoperability and establishing baseline requirements.
- **AI Security Research Consortium:** Established May 2024 with Ministry of Digital Development support, includes National Technology Center for Digital Cryptography, Academy of Cryptography of the Russian Federation, and V.P. Ivannikov Institute for System Programming. Focuses on AI technology security research.
- **Sectoral Ministries:** Ministry of Healthcare, Ministry of Transport, Ministry of Finance, and other domain-specific agencies evaluate and approve experimental legal regimes within their jurisdictions, ensuring AI innovations align with sectoral regulations.
- **Federal Assembly (Parliament):** Enacts legislation establishing experimental legal regime frameworks, liability requirements, and other legally binding AI regulations through federal laws.
- **Regional Governments:** Moscow, Tatarstan, and other regions implement AI pilot projects, particularly autonomous vehicle testing zones, within their jurisdictions under federal experimental regime frameworks.

Implementation Status

Russia's AI regulatory framework is at varied stages of implementation across different components. The experimental legal regimes established by Federal Law No. 258-FZ have seen active deployment since 2020, with successful pilot projects including autonomous vehicle testing in Moscow and Tatarstan, AI-powered diagnostic systems in select healthcare facilities, and algorithmic trading platforms in financial markets. These sandboxes have processed applications from dozens of companies, with the Ministry of Economic Development and sectoral ministries establishing standardized evaluation procedures.

The 2024 liability insurance framework (Federal Law No. 123-FZ) remains in early implementation stages. Insurance companies are developing risk assessment methodologies for AI systems, actuarial models for pricing coverage, and claims evaluation procedures for AI-related harm. Only a handful of insurers currently offer AI liability products, primarily for well-established use cases like autonomous vehicles and medical diagnostics. Smaller AI developers report difficulty obtaining affordable coverage, potentially limiting sandbox participation.

The voluntary Code of Ethics has achieved limited adoption beyond major technology companies like Yandex, Sberbank, and VK Group, plus state-owned enterprises in telecommunications and defense sectors. Smaller startups and foreign companies operating in Russia show minimal engagement with ethical principles. No enforcement mechanism exists for non-compliance, and transparency reporting remains inconsistent.

The updated 2024 AI strategy's priorities around domestic semiconductor manufacturing and alternative supply chains face significant technical and economic challenges. Despite government investment, Russia's semiconductor capabilities remain 5-10 years behind leading Western and Asian manufacturers. Alternative supply chains through China and India provide partial solutions but create new dependencies. Defense and surveillance AI applications have received substantial funding and show measurable progress, while consumer AI services lag international standards.

Infrastructure development has progressed unevenly, with Moscow and major cities seeing expansion of data centers and computing resources, while regional areas lack necessary connectivity and hardware. Talent retention remains challenging amid ongoing emigration of AI specialists to Western countries, though increased research funding and salary incentives have slowed the brain drain compared to 2022-2023.

Future Developments

Russia's AI regulatory framework will likely evolve significantly over the next 2-3 years based on current policy signals and strategic priorities. The experimental legal regime framework is expected to expand into additional sectors beyond the current focus on transportation, healthcare, and finance, with manufacturing, agriculture, and energy identified as priority areas. The government has signaled interest in streamlining sandbox approval processes to accelerate innovation cycles, potentially delegating more authority to sectoral ministries rather than requiring centralized Economic Development Ministry review.

The liability and insurance framework will undergo refinement based on initial implementation experience. Early challenges in obtaining affordable coverage for smaller developers may prompt government subsidies, state-backed insurance pools, or tiered requirements based on company size and resources. Attribution mechanisms for distributed AI systems and algorithmic harm remain technically complex, likely requiring updated guidance and potentially new legislation as edge cases emerge.

Domestic semiconductor manufacturing represents a critical strategic priority following Western sanctions. The government has allocated substantial funding for chip fabrication facilities, materials science research, and development of photolithography equipment. Realistically, Russia will require 5-10 years to achieve meaningful production of AI-optimized chips comparable to current Western standards, necessitating continued reliance on alternative supply chains and optimization algorithms for less advanced hardware.

BRICS cooperation on AI governance will likely intensify, with Russia pushing for establishment of BRICS AI standards as alternatives to Western-dominated international frameworks. Joint research initiatives with China on military AI applications, collaboration with India on software development, and potential BRICS AI development bank or funding mechanism are under discussion. Russia seeks to position itself as a bridge between Chinese AI capabilities and other BRICS members seeking technological partnerships independent of Western suppliers.

The voluntary ethics code may transition toward more binding requirements, particularly for high-risk applications in healthcare, criminal justice, and social services. Consumer protection advocates and civil society organizations have called for mandatory transparency requirements and algorithmic accountability mechanisms, though implementation will likely remain limited given Russia's governance priorities and limited regulatory capacity.

International Context

Russia's AI regulatory approach diverges fundamentally from Western frameworks in philosophy, priorities, and implementation mechanisms. Unlike the European Union's comprehensive AI Act with its risk-based classification system, prohibited practices, and extensive compliance requirements, Russia favors experimental regimes allowing innovation first, then regulation based on observed outcomes. This reflects differing political systems, with Russia's centralized state authority enabling rapid deployment of technologies through controlled sandboxes rather than ex-ante regulatory restrictions.

The OECD AI Principles emphasizing human-centered values, transparency, robustness, and accountability find partial reflection in Russia's voluntary Code of Ethics, but enforcement mechanisms and stakeholder participation differ dramatically. Russia's approach prioritizes state interests and national security over individual rights and civil society input, with limited independent oversight of AI deployments in surveillance, law enforcement, and defense applications.

Western sanctions restricting access to advanced semiconductors, AI hardware, and cloud computing services have profoundly shaped Russia's regulatory evolution. While the EU AI Act addresses trustworthiness and fundamental rights, Russia's 2024 strategy update focuses on technological sovereignty, domestic manufacturing, and reducing vulnerability to supply chain disruptions. This geopolitical reality drives regulatory choices that Western frameworks, developed in contexts assuming free technology flows, do not address.

China's AI governance model, combining state-led development with experimental deployment zones and social credit integration, shows stronger parallels to Russia's approach than Western frameworks. Both countries emphasize national security applications, centralized coordination, and strategic competition with Western technology leadership. Russia increasingly looks to Chinese AI regulations as reference points rather than EU or US models, reflected in BRICS discussions about joint AI governance frameworks.

Russia's liability insurance framework for AI developers represents a novel approach not extensively replicated internationally. While the EU AI Act includes insurance-like requirements for high-risk systems and US states are exploring AI liability reforms, Russia's mandatory coverage within experimental regimes creates a unique regulatory model combining innovation flexibility with structured risk management. This may influence other emerging economies seeking balanced approaches between innovation and accountability.

International cooperation on AI governance between Russia and Western nations has largely ceased since 2022, with Russia excluded from OECD working groups, UNESCO AI ethics discussions, and multilateral AI safety initiatives. This isolation reinforces Russia's pivot toward BRICS partnerships and alternative governance frameworks, potentially fragmenting global AI standards into competing Western and non-Western approaches. The long-term implications for AI safety, interoperability, and international coordination remain uncertain as geopolitical tensions persist.

Rwanda — AI Regulatory Landscape Summary

Overview

Rwanda stands as Africa's pioneer in comprehensive AI governance, having become the first country on the continent to adopt a [National Artificial Intelligence Policy](#) in April 2023. This landmark achievement positions Rwanda as a regional leader in responsible and ethical AI development. The regulatory framework combines the AI policy with the [Data Protection and Privacy Law \(Law No. 058/2021\)](#) to create a comprehensive governance ecosystem. Rwanda's vision is to become a global center for AI research and innovation while leveraging AI to power economic growth and improve quality of life for citizens.

Definitions

Rwanda's regulatory framework adopts internationally recognized AI terminology. Artificial intelligence encompasses systems capable of performing tasks requiring human-like intelligence including learning, reasoning, and decision-making. The data protection framework defines personal data as information relating to identified or identifiable individuals, with sensitive personal data receiving enhanced protections. Data controllers determine processing purposes while data processors act on controllers' instructions. The ethical principles framework emphasizes beneficence (doing good), non-maleficence (avoiding harm), autonomy (preserving human control), justice (ensuring fairness), and explicability (maintaining transparency).

Governance and Institutional Framework

The [Ministry of ICT and Innovation \(MINICT\)](#) serves as the lead coordinating body for AI governance with a dedicated AI Office for implementation. The [Rwanda Utilities Regulatory Authority \(RURA\)](#) develops ethical AI guidelines and provides technical regulation. The [National Cyber Security Authority \(NCSA\)](#) enforces data protection law and oversees cybersecurity compliance. The Centre for the Fourth Industrial Revolution Rwanda (C4IR) provides technical expertise and innovation support. Multi-stakeholder coordination involves government agencies, private sector, academia, civil society, and international partners including UNESCO, GIZ FAIR Forward, and The Future Society.

Key Focus Areas

- **AI Skills and Literacy:** Developing 21st-century workforce capabilities through education and training programs.
- **Infrastructure Development:** Building reliable computing capacity and digital infrastructure for AI applications.
- **Data Governance:** Implementing comprehensive frameworks for data collection, management, and utilization.
- **Public Sector AI:** Promoting trustworthy AI deployment in government services and citizen-facing applications.
- **Private Sector Innovation:** Encouraging businesses to leverage AI for sustainable economic growth.
- **Research and Innovation:** Building local AI research capacity through academic and international partnerships.

- **Ethical AI Principles:** Implementing beneficence, non-maleficence, autonomy, justice, and explicability requirements.
- **Data Protection:** Ensuring consent-based processing, data localization, and breach notification compliance.
- **International Alignment:** Coordinating with UNESCO, African Union, and global AI governance initiatives.

Implementation Framework

Implementation follows a phased approach with short-term, medium-term, and long-term objectives. The AI Office coordinates policy implementation through stakeholder consultations and progress monitoring. Organizations must comply with data protection registration requirements and ethical AI principles. Sector-specific guidelines are being developed for healthcare, agriculture, education, and financial services. NCSA conducts compliance monitoring through registration, audits, and breach reporting analysis. The framework emphasizes public-private partnerships for resource mobilization and practical implementation support.

Monitoring and Evaluation

Multiple mechanisms enable ongoing oversight of AI governance. The AI Office tracks implementation progress through defined indicators including AI adoption rates and investment levels. RURA monitors compliance with ethical AI guidelines through audits and stakeholder feedback. NCSA maintains oversight of data protection through mandatory registration, breach reporting, and scheduled inspections. International benchmarking tracks Rwanda's position in global AI readiness indices with a goal of entering the top 50 countries. Annual progress reports document implementation achievements and challenges for continuous policy refinement.

Penalties, Liability, and Appeals

The enforcement framework combines policy guidance with statutory penalties. The AI Policy does not establish direct penalties but operates within Rwanda's broader legal framework. The Data Protection Law provides the primary enforcement mechanism with administrative fines for registration and notification violations, enhanced penalties for security failures, and criminal liability for intentional unauthorized disclosure. Data subjects may pursue civil remedies for damages from unlawful processing. Appeals follow established administrative review procedures. RURA may take regulatory action for ethical AI guideline violations within sectors under its jurisdiction.

Relationship to Other Instruments

Rwanda's AI governance integrates with broader national frameworks including Vision 2050, the National Strategy for Transformation (NST1), and the ICT Sector Strategic Plan. The AI Policy and Data Protection Law complement each other in regulating AI-related data processing. Sector-specific regulations in telecommunications (RURA), financial services (NBR), and healthcare provide additional compliance requirements. The framework aligns with the Electronic Transactions Law and National Cyber Security Policy. Regional alignment includes the African Union Digital Transformation Strategy and Smart Africa initiative commitments.

International Alignment

Rwanda demonstrates strong commitment to international AI governance standards. In September 2023, [UNESCO](#) and Rwanda convened a National Workshop in Kigali to advance implementation of the UNESCO Recommendation on the Ethics of AI. Rwanda contributed to the AI Playbook for Small States published in September 2024. The Data Protection Law aligns with African Union Malabo Convention principles and reflects GDPR-consistent provisions. Rwanda participates in Global Partnership on AI discussions and bilateral partnerships including Germany's GIZ FAIR Forward program. The country's international engagement supports knowledge exchange, capacity building, and positioning as a trusted partner for AI collaboration.

Implementation Timeline

Date	Milestone
2021-10-15	Data Protection and Privacy Law (Law No. 058/2021) enters into force
2023-04-20	Cabinet approves National AI Policy - first in Africa
2023-05	AI Office established within Ministry of ICT and Innovation
2023-09	UNESCO National Workshop on AI Ethics held in Kigali
2024	Development of sector-specific AI implementation guidelines
2024-09	AI Playbook for Small States published with Rwanda contribution

Compliance Checklist

Requirement	Details
Ethical AI Principles	Implement beneficence, non-maleficence, autonomy, justice, and explicability in AI systems
NCSA Registration	Register as data controller or processor with National Cyber Security Authority
Data Consent	Obtain clear, informed consent before processing personal data
Data Localization	Store personal data in Rwanda or obtain NCSA certificate for offshore storage
Breach Notification	Notify NCSA within 48 hours of discovering data breaches
Transparency	Ensure explainability of AI decision-making processes
Bias Prevention	Implement measures to prevent discrimination in AI systems
Security Measures	Deploy appropriate technical and organizational safeguards

Sources and References

Source	Type
Ministry of ICT and Innovation - Policies	Government Source
RwandaLII - Data Protection Law	Primary Source
The Future Society - AI Policy Announcement	Official Partner
UNESCO - Rwanda AI Support	International Organization

Saudi Arabia — AI Regulatory Landscape Summary

Overview

Saudi Arabia's approach to AI regulation is centralized, strategic and implementation-oriented. The Saudi Data & Artificial Intelligence Authority (SDAIA), created by Royal Decree, provides both strategic leadership and operational guidance designed to accelerate adoption while managing risk. The National Strategy for Data & Artificial Intelligence (NSDAI) sets long-term priorities across public service transformation, economic diversification, talent development and international cooperation. Complementary instruments — ranging from binding statutes such as the Personal Data Protection Law (PDPL) to non-binding ethics principles and technical guidance for generative AI — together create a layered governance model that balances adoption with risk controls.

Regulatory Instruments

- [Royal Decree establishing the Saudi Data & Artificial Intelligence Authority \(SDAIA\)](#) - Establishes SDAIA as the national authority for coordinating data and AI strategy and initiatives. Status: Enacted/Published. Type: Royal Decree / Institutional establishment.
- [National Data Governance Interim Regulations \(including Open Data, Data Sharing, Freedom of Information and Personal Data Interim Regulations\)](#) - Interim rules to harmonize government data use, sharing and open data practices; provides baseline governance for public-sector datasets. Status: Enacted/Published. Type: Interim regulation / administrative.
- [National Strategy for Data & Artificial Intelligence \(NSDAI\)](#) - Strategic roadmap establishing national priorities, objectives and implementation levers for data and AI. Status: Enacted/Published. Type: National strategy.
- [Cloud Computing Regulatory Framework \(CCRF\) v3 \(Communications regulator\)](#) - Sectoral framework addressing cloud service provisioning, security, and market rules. Status: Superseded. Type: Sectoral regulatory framework.
- [Personal Data Protection Law \(PDPL\) \(Royal Decree M/19\)](#) - The primary statute governing processing of personal data, setting out rights, lawful bases, controller/processor obligations, and enforcement. Status: In force. Type: National law / statute.
- [Implementing Regulations of the Personal Data Protection Law \(PDPL Implementing Regulations\)](#) - Detailed rules and procedures for compliance with the PDPL, including administrative processes and technical safeguards. Status: In force. Type: Implementing regulations.
- [Principles and Controls of AI Ethics \(SDAIA AI Ethics Principles\)](#) - High-level ethical principles and recommended technical controls for AI systems. Status: Enacted/Published. Type: Non-binding guidance / ethics framework.
- [Generative AI Guidelines for Government \(SDAIA\)](#) - Operational guidance for government agencies on procurement, deployment, risk assessment and mitigation for generative AI technologies. Status: Enacted/Published. Type: Operational guidance.
- [Generative AI Guidelines for the Public \(SDAIA\)](#) - Public-facing guidance aimed at private sector and citizens outlining safe use practices and responsibilities when using generative AI. Status: Enacted/Published. Type: Public guidance.
- [AI Adoption Framework \(SDAIA\)](#) - A structured framework to guide organizations through lifecycle stages of AI adoption, including governance, risk management and capability building. Status: Enacted/Published. Type:

Implementation framework.

- [Deepfakes Guidelines \(SDAIA\)](#) - Guidance on identification, mitigation and public communication strategies related to synthetic media and deepfakes. Status: Enacted/Published. Type: Advisory guidance.
- [Regulation on Personal Data Transfer Outside the Kingdom \(PDPL transfer regulation\)](#) - Rules governing cross-border transfers of personal data, including permitted mechanisms and safeguards. Status: In force. Type: Implementing regulation / transfer control.
- [Draft Global AI Hub Law \(public consultation by Communications, Space and Technology Commission / CST\)](#) - Consultation draft intended to shape future regulatory obligations for AI platforms, hubs and cross-border services. Status: Draft (public consultation). Type: Draft law / sectoral proposal.

Key Themes and Priorities

Across instruments, common themes include: enabling adoption and public-sector modernization; ensuring individual privacy and data protection through the PDPL; promoting ethical AI via SDAIA's principles and practical controls; and securing data flows and digital infrastructure. The Kingdom emphasizes centralized coordination to reduce fragmentation while issuing sectoral instruments where technical or market specifics (e.g., cloud services) require regulator-level detail.

Governance Structure

SDAIA is the primary coordinating agency for data and AI policy, responsible for strategy, standards and ethics advice. The Communications, Space and Technology Commission (CST) addresses communications, infrastructure and market regulation relevant to cloud and platform services. Ministries and sectoral regulators remain responsible for enforcing statutory requirements within their domains; the PDPL creates legal obligations enforceable across sectors. Where instruments are non-binding (ethics, guidance), SDAIA leverages procurement, national program control and technical standards to influence compliance.

Implementation Status

The PDPL and its Implementing Regulations are in effect and constitute the main binding legal obligations regarding personal data processing. SDAIA's ethics and operational guidance documents are published and actively used by government agencies; they are influential even when not legally binding. The CST's Cloud Computing Regulatory Framework has been revised over time and some versions are superseded, while the Draft Global AI Hub Law is under consultation and not yet binding. Organizational readiness varies: public agencies engaged in national AI programs generally follow SDAIA frameworks, whereas private sector compliance efforts continue to evolve in response to PDPL enforcement and contractual requirements from government customers.

Future Developments

Expect continued refinement of AI-specific rules, likely including more prescriptive requirements for high-risk systems, regulatory guidance on model transparency and accountability, certification or audit regimes for AI systems used in critical domains, and potential licensing or registration of certain AI providers. The outcome of CST's draft consultation could introduce sectoral obligations for platforms and hubs, particularly where cross-border services and national security considerations intersect.

International Context

Saudi Arabia's instruments show alignment with global trends — combining data protection law, ethics guidance and sectoral regulatory initiatives. SDAIA and CST engagement with international standards bodies and bilateral initiatives is expected to promote interoperability with privacy frameworks and AI governance best practices while preserving national priorities such as data sovereignty and digital economic objectives.

For authoritative primary documents and current text of instruments, refer to SDAIA's official portal at <https://sdaia.gov.sa>, the Communications, Space and Technology Commission at <https://cst.gov.sa>, and Saudi government legal portals such as <https://www.saudi.gov.sa>.

Senegal — AI Regulatory Landscape Summary

Overview

Senegal has established itself as an emerging leader in AI governance in West Africa and the francophone African region. The country's framework combines comprehensive AI strategy with established data protection foundations, positioning Senegal among Africa's AI pioneers alongside Ghana, Rwanda, and Benin. The [National AI Strategy \(SNDIA\)](#), launched in September 2023 provides the policy foundation, while the [Data Protection Law of 2008](#) establishes legal safeguards for AI applications involving personal data. [UNESCO collaboration](#) on ethical AI assessment has significantly influenced Senegal's approach.

Regulatory Instruments

- [National Strategy for the Development of Artificial Intelligence \(SNDIA\)](#) - Comprehensive national AI framework launched in September 2023, positioning AI as a catalyst for the Plan Senegal Emergent and focusing on socio-economic development, youth employment, and ethical AI.
- [Law No. 2008-12 on the Protection of Personal Data](#) - Foundational data protection legislation providing legal safeguards for AI systems processing personal data, enforced by the Commission de Protection des Données Personnelles.

Key Themes and Priorities

- **Socio-Economic Development:** AI positioned as catalyst for Plan Senegal Emergent and national development objectives.
- **Youth Employment:** Strong focus on creating AI-related job opportunities for young Senegalese.
- **Ethical AI Development:** UNESCO collaboration ensuring ethical principles integrated from strategy inception.
- **Regional Leadership:** Positioning as AI leader in West Africa and francophone region.
- **Public Sector Transformation:** Deploying AI to improve government services and efficiency.
- **Digital Infrastructure:** Addressing connectivity and computing capability development needs.
- **Data Protection:** Strong legal foundations for personal data protection in AI applications.
- **International Cooperation:** Active engagement with UNESCO, francophone organizations, and regional partners.

Governance Structure

- **Ministry of Communication, Telecommunications and Digital Economy (MCTEN):** Lead implementing agency coordinating AI strategy execution.
- [Commission de Protection des Données Personnelles \(CDP\):](#) Data protection authority overseeing AI systems processing personal data.
- [ARTP \(Telecommunications Regulatory Authority\):](#) Telecommunications infrastructure regulation supporting AI deployment.
- **Academic Institutions:** Universities participating in AI research and human capital development.

- **International Partners:** UNESCO, Agence Universitaire de la Francophonie, and development organizations supporting AI advancement.

Implementation Status

Senegal's AI governance framework is in active implementation phase. The [National AI Strategy](#) launched in September 2023 is being operationalized across its strategic pillars. The September 2024 launch of [Afrik'IA](#) at the Agence Universitaire de la Francophonie demonstrates implementation progress and regional leadership. The February 2025 New Technological Deal announced by President Bassirou Diomaye Diakhary Faye provides renewed political commitment and resources. The [Data Protection Law](#) continues to be actively enforced by CDP. No dedicated AI legislation exists yet, though the strategy recommends developing AI-specific regulatory frameworks. Infrastructure challenges including 60% internet penetration rate continue to be addressed.

Future Developments

- **AI-Specific Legislation:** Strategy recommends developing dedicated AI regulatory frameworks.
- **New Technological Deal:** Implementation of the 12-program digital strategy announced February 2025.
- **Infrastructure Development:** Continued investment in data centers, connectivity, and computing capabilities.
- **Regional Cooperation:** Expanded collaboration through Afrik'IA and francophone AI initiatives.
- **Human Capital Development:** Scaling AI education and training programs.
- **Ethical Framework Elaboration:** Further development of ethical AI guidelines building on UNESCO collaboration.

International Context

Senegal demonstrates significant international engagement in AI governance. [UNESCO collaboration](#) on the Readiness Assessment Methodology influenced strategy development with ethical considerations. The country is positioned among African AI pioneers alongside Ghana, Rwanda, and Benin. Active participation in the [Paris Peace Forum](#) demonstrates engagement with global AI governance discussions. Francophone cooperation through the [Agence Universitaire de la Francophonie](#) supports regional collaboration. The framework aligns with [African Union Continental AI Strategy](#) objectives. South-South cooperation enables knowledge sharing with other developing nations advancing AI governance.

Serbia — AI Regulatory Landscape Summary

Overview

Serbia has developed one of the most comprehensive AI governance frameworks in Southeast Europe and the Western Balkans. Beginning with the adoption of its national AI strategy in 2019, the country has progressively built a multi-layered approach encompassing strategic planning, ethical guidelines, and significant international leadership through the [Global Partnership on Artificial Intelligence \(GPAI\)](#). Serbia's approach emphasizes innovation-friendly policies that align with European Union standards while maintaining focus on ethical AI development, human-centric values, and broad international cooperation. The [Office for Artificial Intelligence](#) coordinates this comprehensive framework, supported by dedicated research institutions and substantial infrastructure investments including the National AI Platform.

Regulatory Instruments

- [Strategy for the Development of Artificial Intelligence in the Republic of Serbia 2020-2025](#) - Serbia's foundational national AI framework establishing objectives and measures for AI development across economic, public service, research, and educational sectors. Led to National AI Platform deployment and institutional capacity building.
- [Ethical Guidelines for the Development, Implementation and Use of Reliable and Responsible AI](#) - Comprehensive ethical framework establishing four fundamental principles and seven core conditions for trustworthy AI, with self-assessment tools and high-risk AI system identification criteria.
- [Belgrade Ministerial Declaration on Artificial Intelligence](#) - International ministerial declaration adopted by 44 GPAI member countries, committing to safe, secure, and trustworthy AI development while establishing Serbia's leadership role in global AI governance.

Key Themes and Priorities

- **EU Alignment and Harmonization:** Serbia's AI governance framework explicitly anticipates harmonization with the EU AI Act and European standards, reflecting EU accession aspirations and commitment to European values.
- **Innovation and Economic Development:** AI is positioned as a key driver of economic growth, with support for startups, research commercialization, and public-private partnerships.
- **Human-Centric and Ethical AI:** Strong emphasis on human rights, dignity, transparency, and accountability throughout all regulatory instruments, drawing from UNESCO and European ethical frameworks.
- **Infrastructure and Capacity Building:** Significant investments in supercomputing capabilities, research institutions, and educational programs to build national AI capacity.
- **International Leadership:** Active engagement in multilateral AI governance through GPAI co-chairmanship and participation in global initiatives.
- **Public Sector Innovation:** AI deployment prioritized for improving public administration services and government efficiency.
- **Research Excellence:** Establishment of dedicated AI research institutions and funding programs to advance scientific capabilities.

Governance Structure

- **[Office for Artificial Intelligence](#)**: Primary coordination body for AI policy implementation, strategy oversight, and international engagement including GPAI representation.
- **[Ministry of Science, Technological Development and Innovation](#)**: Oversees AI research funding, strategy development, and innovation policy alignment.
- **[Office for Information Technologies and eGovernment](#)**: Manages National AI Platform infrastructure, data center operations, and technical implementation.
- **[Institute for Artificial Intelligence Research and Development](#)**: National research institution advancing AI science and supporting ecosystem development.
- **Council for Artificial Intelligence**: High-level coordination body established September 2024, providing cross-sectoral policy guidance and strategic direction.
- **[Commissioner for Information and Personal Data Protection](#)**: Enforces data protection requirements relevant to AI systems under GDPR-aligned legislation.

Implementation Status

Serbia has achieved substantial implementation progress across its AI governance framework. The [AI Development Strategy 2020-2025](#) reached its implementation targets, with the National AI Platform operational since 2021 and supercomputing resources available to startups through public calls. The [Institute for Artificial Intelligence Research and Development](#) is actively conducting research and supporting ecosystem development. The successor Strategy 2025-2030 has been adopted, ensuring continuity. The [Ethical Guidelines](#) provide voluntary but influential guidance, with organizations encouraged to complete self-assessments. High-risk AI identification criteria are being applied, particularly in healthcare and critical infrastructure sectors. International implementation through GPAI is advancing, with Serbia fulfilling its co-chairmanship responsibilities. A dedicated AI law is in development, expected by March 2025, which will transition some voluntary provisions to binding requirements.

Future Developments

- **AI Law (Expected March 2025)**: Serbia's first dedicated AI legislation is under development, expected to establish binding requirements aligned with the EU AI Act framework.
- **Strategy 2025-2030 Implementation**: New five-year strategy continuing and expanding initiatives from the first strategy period.
- **GPAI Leadership Continuation**: Serbia continues GPAI co-chairmanship with Slovakia, with ministerial meeting planned for Bratislava in late 2025.
- **Paris AI Action Summit (February 2025)**: Serbia committed to participating in this major international AI governance event.
- **EU Accession Progress**: Continued harmonization with EU AI Act requirements as Serbia advances in accession negotiations.
- **Infrastructure Expansion**: Potential expansion of National AI Platform capabilities and data center resources.

International Context

Serbia's AI governance framework demonstrates strong international alignment and leadership. The country's participation in [GPAI](#) and co-chairmanship following the Belgrade Summit positions it as a significant voice in global AI governance. All Serbian instruments align with the [OECD AI Principles](#), which serve as the foundational international framework. The [Ethical Guidelines](#) explicitly incorporate [UNESCO's Recommendation on AI Ethics](#).

Serbia's framework anticipates harmonization with the [EU AI Act](#), reflecting EU accession aspirations. The [Belgrade Declaration](#) represents Serbia's contribution to international AI governance consensus. Compared to Western Balkans neighbors, Serbia leads in comprehensive AI governance development. Serbia ranks 57th globally in the Government AI Readiness Index, the highest in the Western Balkans, demonstrating effective translation of policy frameworks into implementation capacity.

Singapore — AI Regulatory Landscape Summary

Overview

Singapore's AI regulatory ecosystem combines national strategy, government-supported research translation, cross-agency ethical guidance, sectoral supervisory expectations and practical governance toolkits. The approach is principles-first and risk-based: it emphasizes fairness, ethics, accountability and transparency while facilitating innovation and commercialisation. Implementation relies on collaborative, iterative instruments—model frameworks, advisory guidelines and verification toolkits—supplemented by statutory measures where clear public-interest risks arise (e.g., elections, worker protections, online safety).

Regulatory Instruments

- [AI Singapore \(national AI research and translation programme\)](#) - National programme created to accelerate AI research, build AI talent and translate AI into economic impact. Status: Enacted/Published; Type: National research and translation programme.
- [Advisory Council on the Ethical Use of AI and Data](#) - Cross-sector advisory body providing ethical guidance and high-level recommendations for government and industry adoption. Status: Enacted/Published; Type: Advisory/Ethics council.
- [Principles to Promote Fairness, Ethics, Accountability and Transparency \(FEAT\) in the Use of AI and Data Analytics \(MAS\)](#) - Foundational MAS principles for regulated entities describing expectations around fairness, explainability, accountability and transparency. Status: Enacted/Published; Type: Supervisory principles.
- [Model AI Governance Framework \(First Edition\)](#) - Practical, non-binding governance framework for organisations to operationalise responsible AI practices (governance, risk management, transparency, human oversight). Status: Enacted/Published; Type: Voluntary model framework.
- [National Artificial Intelligence Strategy \(NAIS\)](#) - Government strategy outlining priority sectors, capability targets and public-private partnerships to scale AI adoption. Status: Enacted/Published; Type: National strategy.
- [Model AI Governance Framework \(Second Edition\)](#) - Updated edition refining implementation guidance, assessment templates and industry guidance. Status: Enacted/Published; Type: Voluntary model framework (updated).
- [AI Verify \(AI governance testing framework and toolkit\)](#) - Testing framework and toolkit developed to help organisations validate AI governance controls and assess model behaviour prior to deployment. Status: Enacted/Published; Type: Governance testing toolkit.
- [National Artificial Intelligence Strategy 2.0 \(NAIS 2.0\)](#) - Iteration of the national strategy focused on scaling, international partnerships, talent and trustworthy AI practices. Status: Enacted/Published; Type: National strategy (update).
- [Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems \(PDPC\)](#) - PDPC guidance interpreting data-protection obligations under the PDPA for AI-driven recommendations and decision systems; covers consent, purpose limitation, de-identification and transparency. Status: Enacted/Published; Type: Regulatory advisory guidelines.
- [Model AI Governance Framework for Generative AI](#) - Sector-agnostic operational guidance focused on generative AI risks (hallucination, IP, safety, content provenance and guardrails). Status: Enacted/Published; Type: Voluntary model framework (specialised).

- [Proposed Guide on Synthetic Data Generation \(PDPC\)](#) - PDPC draft guidance on best practices for creating and using synthetic data while managing re-identification and privacy risks. Status: Draft; Type: Proposed advisory guidance.
- [Elections \(Integrity of Online Advertising\) \(Amendment\) Act 2024](#) - Statutory amendment increasing transparency and accountability for online political advertising and related digital campaign activity to protect electoral integrity. Status: In force; Type: Statutory amendment.
- [Guide on the Use of Generative Artificial Intelligence Tools by Court Users \(Registrar's Circular / Singapore Courts\)](#) - Practical guidance for litigants, lawyers and court users on using generative AI tools in proceedings; addresses confidentiality, accuracy and evidentiary implications. Status: Enacted/Published; Type: Judicial guidance circular.
- [Artificial Intelligence Model Risk Management – Observations from a Thematic Review \(MAS information paper\)](#) - MAS observations summarising supervisory findings on model risk management practices and common weaknesses in AI and analytics. Status: Enacted/Published; Type: Supervisory information paper.
- [Workplace Fairness Bill \(Workplace Fairness legislation passed in Parliament\)](#) - Legislation addressing workplace treatment, fairness and dispute resolution mechanisms that may touch on algorithmic management and automated decision-making in employment. Status: Passed; Type: Legislation.
- [Online Safety \(Relief and Accountability\) Bill \(OSRA Bill\)](#) - Proposed legislation aimed at enhancing online safety, platform accountability and user relief mechanisms for online harms that can be amplified by AI systems. Status: Proposed; Type: Proposed legislation.
- [Guidelines on AI Risk Management for Financial Institutions \(MAS consultation paper\)](#) - MAS consultation document proposing more prescriptive AI risk management expectations for financial institutions, including governance, validation and third-party oversight. Status: Proposed/Consultation; Type: Supervisory consultation guidance.

Key Themes and Priorities

Several consistent themes run across instruments: (1) risk-based proportionality—regulatory intensity scales with potential harm; (2) operationalisation—guidance focuses on implementable controls, checklists and testing (AI Verify, model governance frameworks); (3) sectoral calibration—MAS and PDPC issue sector-specific expectations in finance and data protection respectively; (4) transparency and human oversight—explainability, meaningful human-in-the-loop controls and user-facing disclosures are repeatedly emphasised; (5) iterative governance—documents are designed to be updated and complemented by toolkits and testbeds as technology evolves.

Governance Structure

Responsibility is distributed across agencies: the Monetary Authority of Singapore (MAS) leads financial-sector supervision and sets prudential expectations; the Personal Data Protection Commission (PDPC) interprets data-protection obligations for AI systems; government coordination and strategy are led through national strategy vehicles and Smart Nation initiatives and research translation is supported by AI Singapore. Independent advisory bodies—such as the Advisory Council on the Ethical Use of AI and Data—provide ethical recommendations and public consultation. The courts and election authorities also play defined roles where judicial processes and democratic integrity intersect with AI use.

Implementation Status

By 2025 most foundational documents and toolkits are published and in active use: the Model AI Governance Framework (1st and 2nd editions), FEAT principles, PDPC advisory guidelines and the generative-AI edition of the model framework form the primary governance artefacts used by organisations. AI Verify and government-led testbeds are available for governance testing. MAS has moved from principles to closer supervisory engagement

(information papers and proposed AI risk guidelines). Statutory measures for elections are in force, while workplace fairness and online safety legislation remain recent or proposed and are being operationalised through agency rules and enforcement guidance.

Future Developments

Expect continued refinement and sector-specific prescription where risks are concentrated (finance, healthcare, electoral integrity, employment). Anticipate upgraded supervisory frameworks from MAS following consultation, PDPC finalisation of synthetic-data guidance, and legislative development of OSRA and workplace protections. Singapore is also likely to invest further in verification tooling, standardised impact assessments and cross-border interoperability mechanisms to support trade and data flows.

International Context

Singapore positions itself as pro-innovation but aligned with global norms. The country's principles-first, sectoral approach interoperates with OECD AI principles, aligns with data-protection best practices, and emphasises international cooperation through research partnerships and standards engagement. Singapore's mix of voluntary operational guidance plus targeted statutory intervention provides a credible model for other jurisdictions seeking to balance innovation and protection.

Official sources and further reading include: [AI Singapore](#), [Personal Data Protection Commission \(PDPC\)](#), [Monetary Authority of Singapore \(MAS\)](#), and the Smart Nation / Government portals such as [Smart Nation and Digital Government Office](#).

Slovakia — AI Regulatory Landscape Summary

Overview

As of November 14, 2025, Slovakia's AI regulatory framework is built on three complementary pillars: (1) direct application of EU law — principally Regulation (EU) 2024/1689 (the EU Artificial Intelligence Act); (2) national strategies and action plans that set priorities for digital transformation, skills, research and public-sector digitization; and (3) evolving national implementing legislation and institutional arrangements to operationalize EU obligations at the national level. The combination of strategic planning documents, sectoral guidance, cybersecurity and data governance measures, together with advisory and coordination bodies, shows a coordinated effort to balance risk mitigation, rights protection and innovation support.

Regulatory Instruments

- [Slovak AI Act Implementation Law \(draft\)](#) - Draft national implementing law to align Slovakia's administrative and enforcement architecture with Regulation (EU) 2024/1689; status: Draft; type: National implementing legislation (draft).
- [Action Plan for the Digital Transformation of Slovakia 2019–2022 \(Akčný plán digitálnej transformácie Slovenska na roky 2019–2022\)](#) - First national action plan outlining measures and responsibilities to digitalize public services and build digital capacities; status: Enacted/Published; type: Action Plan.
- [Strategy of Digital Transformation of Slovakia 2030 \(Stratégia digitálnej transformácie Slovenska 2030\)](#) - Long-term strategy setting national priorities for digital transformation to 2030; status: Enacted/Published; type: Strategy.
- [Strategy of Digital Transformation of Slovakia 2030](#) - Alternate reference/version of the 2030 strategy; status: In force; type: Strategy.
- [Strategy of Digital Transformation of Slovakia 2030](#) - Core policy framework for national digital transformation and AI integration; status: In force; type: Strategy.
- [Action Plan for the Digital Transformation of Slovakia 2019–2022](#) - Implementation steps tied to the 2030 strategy; status: Enacted/Published; type: Action Plan.
- [Standing Commission for Ethics and Regulation of Artificial Intelligence \(CERAI\)](#) - Advisory commission focusing on AI ethics, regulatory advice and cross-sector coordination; status: Enacted/Published; type: Advisory body.
- [National Cybersecurity Strategy 2021–2025](#) - National strategy addressing cybersecurity risks relevant to AI systems and infrastructure resilience; status: In force; type: Strategy.
- [National Concept of Informatization of Public Administration \(NKIVS\) 2021 – 2026](#) - Framework for public administration digitization, interoperability and secure data exchange that underpins public-sector AI use; status: In force; type: Policy framework.
- [Strategy and Action Plan to Improve Slovakia's Position in the DESI Index to 2025](#) - Targets digital competitiveness, connectivity and human capital for EU digital performance improvements; status: Enacted/Published; type: Strategy/Action Plan.
- [Research and Innovation Strategy for Smart Specialisation of the Slovak Republic 2021–2027 \(SK RIS3 2021+\)](#) - Research and innovation priorities including AI applications for regional smart specialisation; status: In force; type: Strategy.

- [Action Plan for the Digital Transformation of Slovakia 2023–2026 \(Akčný plán digitálnej transformácie Slovenska na roky 2023–2026\)](#) - Updated operational action plan implementing the 2030 strategy, including AI-relevant projects; status: In force; type: Action Plan.
- [Action Plan for Digital Transformation of Slovakia 2023–2026](#) - Complementary action plan with concrete milestones and institutional leads; status: In force; type: Action Plan.
- [National Strategy of Digital Skills of the Slovak Republic and Action Plan 2023–2026](#) - Strategy and action plan to develop AI-related skills across education and the workforce; status: In force; type: Strategy/Action Plan.
- [National Strategy for Digital Skills of the Slovak Republic and Action Plan 2023–2026 \(Národná stratégia digitálnych zručností SR a Akčný plán 2023–2026\)](#) - Published guidance and funding priorities to support digital and AI skills; status: Enacted/Published; type: Strategy/Action Plan.
- [National Strategy for Digital Skills of the Slovak Republic and Action Plan 2023–2026](#) - Reinforces education and reskilling measures for AI adoption; status: Enacted/Published; type: Strategy.
- [Regulation \(EU\) 2024/1689 - Artificial Intelligence Act \(applies in Slovakia as EU regulation\)](#) - Primary EU-level legal framework regulating AI risk categories, obligations, conformity assessment, transparency and prohibitions; status: Enacted/Published; type: EU Regulation (applies directly).
- [Institutional and Coordination Framework for the Digital Transformation of Slovakia \(government resolution UV-46042/2024\)](#) - Government resolution establishing roles, coordination mechanisms and governance for delivery of digital transformation programs including AI initiatives; status: Enacted/Published; type: Government resolution.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act \(applicable in Slovakia as EU regulation\)](#) - Duplicate/alternate reference confirming the EU AI Act's applicability; status: In force; type: EU Regulation.
- [Government Plenipotentiary for Artificial Intelligence \(appointment and statute establishing the office/splnomocnenec vlády SR pre umelú inteligenciu\)](#) - National focal point tasked with coordination, stakeholder engagement and implementation oversight; status: Enacted/Published; type: Office/Statute.
- [Draft Act on the Organization of Public Administration in the Field of Artificial Intelligence \(government bill submitted to interdepartmental comment procedure\)](#) - Draft law proposing organizational structure for AI governance in public administration; status: Draft (interdepartmental comment); type: Draft bill.
- [AI in Education — Guidance for Educators \(Usmernenie o AI pre pedagógov\)](#) - Practical guidance for schools and teachers on AI use, ethics and risk mitigation in education settings; status: Enacted/Published; type: Guidance document.
- [Draft Act on Artificial Intelligence \(national implementing law to complement the EU AI Act\)](#) - Draft implementing legislation intended to define national enforcement roles and administrative procedures; status: Draft; type: Draft Act.
- [Draft Act on the Organization of State Administration in the Field of Artificial Intelligence \(national bill to establish oversight, notifying authority and regulatory sandbox\)](#) - Draft to set up a notifying authority, regulatory sandbox and administrative competences for AI; status: Under review; type: Draft bill.
- [Draft Act on the Management of Selected Categories of Public Sector Data \(data governance bill supporting AI/data reuse\)](#) - Data governance bill intended to enable secure reuse of public-sector datasets for AI while protecting privacy and rights; status: Under review; type: Draft data governance law.

Key Themes and Priorities

Across strategies, action plans and draft laws, recurring themes surface: (1) EU alignment and transposition — ensuring Slovakia's administrative and enforcement structures can implement the EU AI Act; (2) governance and coordination — establishing focal points (government plenipotentiary), advisory bodies (CERAI) and inter-ministerial coordination (government resolution); (3) data governance and reuse — enabling public data access

under safeguards to spur AI development; (4) skills and innovation — workforce reskilling, research priorities (RIS3), and DESI improvements to boost competitiveness; (5) security and resilience — integrating AI risk into cybersecurity strategy and public administration informatization (NKIVS); and (6) sectoral practical guidance, exemplified by education guidance for teachers.

Governance Structure

Slovakia's governance architecture for AI is a hybrid of advisory and executive elements: CERAI provides ethics and regulatory advice, the Government Plenipotentiary for AI acts as a coordination and implementation focal point, and the government resolution on institutional frameworks clarifies ministerial roles. Draft legislation proposes to formalize the notifying authority and oversight functions (including a sandbox) within state administration. Relevant ministries and agencies responsible for digital transformation, education, research & innovation, public administration informatization and cybersecurity are implicated in the implementation and enforcement roles described in strategy and draft laws.

Implementation Status

The EU AI Act (Regulation (EU) 2024/1689) is applicable in Slovakia. Multiple national strategies and action plans are enacted and in force, providing policy continuity. Institutional measures (CERAI, plenipotentiary, coordination resolution) are established. Key gaps remain in national implementing legislation and administrative structures: draft acts for implementing the EU AI Act, establishing the notifying authority and regulatory sandbox, and for public-sector data governance are at various draft/review stages. Operationalization — including guidance for conformity assessment, notification templates, sanctions, and supervisory capacity — depends on how draft laws progress and on transposition of EU delegated/implementing acts at the EU level.

Future Developments

Near-term priorities should include finalizing the national implementing law and the organizational statute for state administration in AI, approving data governance legislation to enable responsible data reuse, and building operational enforcement and advisory capacity. Slovakia will also need to monitor EU-level delegated acts and guidance under Regulation (EU) 2024/1689 to align national procedures and standards. For authoritative resources see the national government AI portal: [Government AI portal](#) and published official sources: [Official sources](#).

International Context

Slovakia's framework is explicitly EU-centric: direct application of the EU AI Act anchors national obligations while national strategies aim to translate EU priorities into local capacity-building. Slovakia's RIS3 and DESI-related efforts connect national innovation policy to EU competitiveness goals. The country's combination of strategic planning, cybersecurity alignment and emergent national legislation follows a pattern seen across EU Member States: combine EU compliance with national implementation measures that protect rights while promoting innovation.

Slovenia — AI Regulatory Landscape Summary

Overview

Slovenia's AI policy landscape in and through 2025 is defined by a layered, coordinated approach that combines strategic national planning with AI-specific programming and legal implementation of EU harmonised rules. At the strategic level, [Digitalna Slovenija 2030](#) provides a long-term national vision for digital transformation that mainstreams AI across policy areas. Two sectoral strategies—[Strategy for Digital Public Services 2030](#) and [Strategy for the Digital Transformation of the Economy](#)—translate that vision into sectoral objectives and measures. The [National Programme for the Promotion of the Development and Use of Artificial Intelligence in the Republic of Slovenia until 2025 \(NpUI\)](#) functions as the operational AI programme, focused on research, adoption, skills and public-private cooperation through 2025. Finally, the [Act on the Implementation of the \(EU\) Regulation on Harmonised Rules on Artificial Intelligence](#) provides the domestic legal framework to implement and enforce the EU AI Regulation.

Regulatory Instruments

- [National Programme for the Promotion of the Development and Use of Artificial Intelligence in the Republic of Slovenia until 2025 \(NpUI\)](#) - In force. Type: National programme/policy instrument. Description: The NpUI is Slovenia's AI-specific action plan focused on directing public investment, coordinating R&D, building digital skills and ethical guidance, supporting start-ups and SMEs, and facilitating public sector AI pilots and data sharing through 2025.
- [Strategy for Digital Public Services 2030 \(Strategija digitalnih javnih storitev 2030\)](#) - Enacted/Published. Type: Strategic policy document. Description: Sets objectives for digital government transformation, improved service delivery, data-driven public administration and responsible adoption of AI in public services, including interoperability, user-centric design and digital trust measures.
- [Strategy for the Digital Transformation of the Economy \(Strategija digitalne preobrazbe gospodarstva\)](#) - Enacted/Published. Type: Strategic policy document. Description: Focuses on boosting digital capacity and competitiveness in the Slovenian economy, encouraging adoption of digital technologies (including AI) by firms, targeting SME support, digital skills, investment incentives and ecosystem development.
- [Digitalna Slovenija 2030 \(Digital Slovenia 2030\) - National strategy for digital transformation](#) - Enacted/Published. Type: National strategy. Description: A cross-sectoral strategy that outlines Slovenia's digital transformation priorities through 2030, including infrastructure, data governance, digital skills, innovation ecosystems and the principled use of AI across society and the economy.
- [Zakon o izvajanju Uredbe \(EU\) o določitvi harmoniziranih pravil o umetni inteligenci / Act on the Implementation of the \(EU\) Regulation on Harmonised Rules on Artificial Intelligence](#) - Enacted/Published. Type: National implementing act. Description: Implements and operationalises the EU AI Regulation at the national level, defining domestic enforcement, market surveillance, designated supervising authorities, and procedural rules for conformity assessment, notification and sanctions insofar as national law is required.

Key Themes and Priorities

Across these instruments, a consistent set of priorities emerges: (1) fostering innovation and competitiveness by supporting AI research, startups and SME adoption; (2) modernising public services through data-driven and user-centric digital government; (3) investing in digital infrastructure and public data flows to enable trustworthy AI; (4) building human capital through reskilling and education initiatives; (5) emphasising trustworthy and ethical AI,

including risk assessment, transparency and human oversight; (6) aligning national policy with EU rules and standards; and (7) ensuring cybersecurity and privacy protection. The instruments balance measures to stimulate demand for AI with safeguards to manage risk, particularly where AI affects fundamental rights or critical public functions.

Governance Structure

Governance in Slovenia is multi-layered and multi-actor. At the political-administrative level, the Ministry of Public Administration (and equivalent central digital institutions) lead digital government and implementation of public service priorities; the Ministry of Economic Development and Technology and economic development agencies lead business and innovation aspects; ministries responsible for justice, labour, health and education contribute sectoral implementation and regulation. Research institutions and the university sector are central partners under the NpUI. The national implementing act assigns supervisory and market surveillance responsibilities to specified authorities and creates statutory hooks for coordination with EU bodies and for cross-border cooperation where appropriate. Implementation relies on inter-ministerial coordination mechanisms, digital agencies and public procurement frameworks to integrate AI risk assessments into government procurement and service delivery.

Implementation Status

Implementation status as of 2025 is active but evolving. The strategic documents (Digitalna Slovenija 2030 and the two sectoral strategies) have been published and guide policy and funding decisions. The NpUI is in force and has driven targeted measures in research funding, pilot projects and skills programmes up to 2025. The national implementing act has been enacted to give domestic effect to the EU AI Regulation; however, many operational details remain to be fully implemented: establishing supervisory workflows, resourcing market surveillance, consolidating conformity assessment pathways, and integrating risk-based AI controls into procurement and sectoral regulation. Operational readiness of designated authorities, guidance for industry and public bodies, and capacity building for compliance are emphasized as immediate priorities.

Future Developments

Near-term developments likely include: publication of implementing guidance and administrative rules under the national implementing act; the establishment or designation of national supervisory authorities and competence centres; targeted funding calls under national and EU programmes to scale AI adoption safely; measures to ensure transparency, data access and agency for individuals affected by AI systems; and the integration of AI governance into public procurement and sectoral regulatory frameworks. Slovenia will also continue to adapt its strategies to EU-level developments, participate in cross-border regulatory cooperation, and leverage European funding instruments to deliver digital infrastructure and skills programmes.

International Context

Slovenia's framework is explicitly aligned with EU policy and legal frameworks. The national implementing act is the domestic complement to the EU-level AI Regulation, enabling harmonised rules to be applied in Slovenia while preserving coordinated EU enforcement. Slovenia positions itself as a participant in EU digital policy and standardisation efforts, seeking to combine national competitiveness goals with compliance, ethical AI principles and international cooperation. Relevant external resources include the national government portal and EU digital strategy pages, for example <https://www.gov.si> and the European Commission's AI policy pages at <https://ec.europa.eu/digital-strategy/our-policies/artificial-intelligence>.

Overall, Slovenia's regulatory landscape through 2025 shows a pragmatic blend of long-term strategic planning, AI-specific programming through the NpUI, and statutory action to implement EU harmonised rules. The focus now is implementation—resourcing supervision and conformity assessment, integrating AI risk governance into

public procurement and sectoral frameworks, and ensuring SMEs and public bodies have practical guidance and support to comply with and benefit from trustworthy AI.

South Africa — AI Regulatory Landscape Summary

Overview

South Africa's approach to regulating artificial intelligence (AI) is currently a layered mix of statutory data-protection rules, implementing regulations (including a recent amendment), and high-level policy and advisory documents that are still in draft or consultation form. At the center of the legal framework is the Protection of Personal Information Act (POPIA), No. 4 of 2013, which governs the processing of personal information and establishes the Information Regulator as the primary enforcement authority. The Regulations relating to the Protection of Personal Information (Government Notice R1383 of 2018) and their 2025 amendment (Government Notice GN 6126 of 2025) provide subsidiary detail on technical, organisational and procedural aspects of compliance. Complementing these binding instruments are the Report of the Presidential Commission on the Fourth Industrial Revolution (PC4IR Report) and two policy-drafting efforts: "South Africa's Artificial Intelligence (AI) Planning: Adoption of AI by Government" (draft discussion document) and the "National Artificial Intelligence Policy Framework" (draft) developed by the Department of Communications and Digital Technologies. While POPIA and its regulations are enforceable and underpin a rights-focused approach to AI that processes personal information, the PC4IR report and the draft policy documents provide strategic guidance and policy options to shape future regulatory development.

Regulatory Instruments

- [Protection of Personal Information Act \(POPIA\), No. 4 of 2013](#) - Primary statute governing the processing of personal information in South Africa. Status: In force. Type: Primary legislation. POPIA sets out lawful processing grounds, data subject rights (access, correction, deletion and objection), accountability obligations for responsible parties, and enforcement powers for the Information Regulator. Its provisions apply to AI systems to the extent those systems process personal information.
- [Regulations relating to the Protection of Personal Information, 2018 \(Government Notice R1383 of 2018\)](#) - Subordinate regulations that elaborate implementation details for POPIA, including conditions for special personal information, direct marketing rules, cross-border transfer criteria, and technical and organisational security measures. Status: Enacted/Published. Type: Subordinate legislation/regulation.
- [Amendment to the Regulations relating to the Protection of Personal Information \(POPIA Amendment Regulations\) \(Government Notice GN 6126 of 2025\)](#) - 2025 regulatory amendment updating and clarifying certain requirements under the 2018 Regulations. Status: In force. Type: Subordinate legislation/amendment. The amendment adjusts procedural and compliance details to reflect operational realities of digital services and emerging processing practices.
- [Report of the Presidential Commission on the Fourth Industrial Revolution \(PC4IR Report\)](#) - High-level advisory report offering diagnostics, strategy and recommendations for harnessing the Fourth Industrial Revolution, including AI. Status: Enacted/Published (advisory). Type: Advisory/strategic report. The report informs policy-making but does not create binding legal obligations.
- [South Africa's Artificial Intelligence \(AI\) Planning: Adoption of AI by Government \(Draft discussion document\)](#) - Draft document focused on public-sector adoption of AI, procurement principles, risk assessment, and governance for government AI deployments. Status: Draft. Type: Policy discussion document.
- [National Artificial Intelligence Policy Framework \(Draft\) — Department of Communications and Digital Technologies](#) - Draft national policy framework covering principles, governance models, ethical expectations, capacity-building, and implementation pathways for AI across sectors. Status: Draft. Type: Draft national policy/framework.

Key Themes and Priorities

Across instruments and policy documents, common themes emerge: (1) Data protection and privacy as foundational: POPIA principles (lawful processing, data minimisation, purpose limitation, and security) are the primary legal tools governing AI systems that process personal data. (2) Risk-based governance: draft policy documents and the PC4IR Report advocate for proportionate, risk-sensitive oversight rather than a one-size-fits-all ban or permissive regime. (3) Ethical and socio-economic objectives: policy drafts emphasise fairness, non-discrimination, transparency, and the need to align AI deployment with national priorities like job creation, inclusion, and reducing inequality. (4) Public-sector leadership: government aims to pilot and adopt AI in ways that model good governance, ensure public trust, and set procurement standards. (5) Capacity-building and local ecosystem development: promoting research, skills, local data stewardship, and innovation while ensuring consumer and citizen protection.

Governance Structure

Multiple institutions share roles in the governance of AI-related matters. The Information Regulator (established under POPIA) is the primary enforcement body for data protection obligations and is central to oversight where AI intersects with personal information. The Department of Communications and Digital Technologies (DCDT) leads national policy-making on digital transformation and the National AI Policy Framework. The Department of Science and Innovation (DSI) and related agencies support research, standards, and innovation agendas. The Presidency and advisory bodies, including the Presidential Commission on the Fourth Industrial Revolution, provide strategic direction. Sectoral regulators (e.g., financial sector regulators, health regulators) exercise oversight where AI systems pose sector-specific risks. Inter-agency coordination is a developing area, with policy drafts calling for formal mechanisms for cross-cutting governance, ethical review, and procurement oversight.

Implementation Status

Implementation is uneven: data-protection rules (POPIA and associated regulations) are in force and operational, creating immediate compliance obligations for entities processing personal information. The 2025 amendment to the POPIA Regulations is also in force and updates aspects of the regulatory regime. By contrast, AI-specific statutory rules have not yet been enacted; the National AI Policy Framework and the government AI planning document remain draft instruments undergoing consultation and internal alignment. The PC4IR Report's recommendations have influenced policy direction but require translation into binding rules or concrete institutional arrangements to have regulatory effect. Practical implementation issues—such as the operationalisation of algorithmic impact assessments, transparency obligations, standards for auditing, and cross-agency enforcement—are currently being developed through policy work, guidance, and capacity-building initiatives rather than through detailed, AI-specific legislation.

Future Developments

Short- to medium-term developments to watch include finalisation and adoption of the National AI Policy Framework, potential sectoral rulemaking that imposes AI-specific requirements in regulated industries, formal guidance or codes issued by the Information Regulator on algorithmic processing and high-risk automated decision-making, and the expansion of capacity-building programs and testbeds. International alignment efforts and participation in multi-lateral fora may further shape domestic policy choices, while civil-society engagement and litigation under POPIA could clarify legal expectations for transparency, fairness and accountability in AI systems.

International Context

South Africa's model prioritises data-protection compliance and ethical, inclusive policy design, aligning with global trends that blend privacy law with ethical AI principles and risk-based governance. The absence of a single

comprehensive AI statute mirrors approaches in several jurisdictions that prefer to adapt existing legal frameworks while producing policy guidance and sectoral rules. South Africa is positioned to align with international standards on data protection, cross-border transfers, and ethics-driven governance while emphasising local priorities such as socio-economic inclusion, responsible public-sector adoption, and building domestic AI capacity. For official materials and further updates, stakeholders are directed to government portals and the relevant agencies' publications, including the Department of Communications and Digital Technologies and the Information Regulator, and to ongoing consultations on the draft frameworks. For an entry point to government AI resources, see [https://\[government AI portal\]](https://[government AI portal]) and the agencies' official pages listed under "officialSources" of this summary.

South Korea — AI Regulatory Landscape Summary

Overview

South Korea's AI regulatory framework has three distinctive characteristics: (1) a national strategic layer that promotes AI development and sets high-level principles (e.g., the [National Strategy for Artificial Intelligence](#) and the [Digital Strategy of South Korea](#)); (2) a legislative layer that recently culminated in the passage of a dedicated AI Basic Act (Act on the Promotion of AI Development and Establishing a Trustworthy AI Framework) supported by multiple prior bills and proposals; and (3) a dense collection of agency-issued ethics standards, technical guidance, models and notices that operationalize privacy, transparency, safety and consumer-protection obligations. The system is therefore hybrid: statutory anchors + administrative guidance + sectoral instruments.

Regulatory Instruments

- [Act on the Development and Supply \(Distribution\) of Intelligent Robots](#) - (Status: In force; Type: Act). A sector-specific law addressing robotics development, safety standards and distribution obligations; predates modern AI statutes and remains relevant for robot-linked AI deployments.
- [National Strategy for Artificial Intelligence](#) - (Status: Enacted/Published; Type: Strategy). National roadmap (2019) setting long-term priorities for research, talent, data infrastructure, and public-sector adoption; served as a policy foundation for later legislation.
- [Basic Act on AI Technology \(Representative: Min Hyung-bae, proposed Oct 29, 2020\)](#) - (Status: Ended; Type: Bill). An early draft legislative attempt to create a unified AI statute; although it did not pass in this form, it influenced later legislative drafting.
- [Human-Centered Artificial Intelligence Ethics Standards \(National AI Ethics Standards\)](#) - (Status: Enacted/Published; Type: Ethics Standards). Government-published ethics principles focused on human-centered design, fairness, safety and accountability to guide public and private actors.
- [Bill on Artificial Intelligence \(Representative: Lee Yong-bin, proposed July 19, 2021\)](#) - (Status: Ended; Type: Bill). Parliamentary proposal addressing transparency and liability; used as a reference in later debates.
- [AI Promotion and Trust-Building Bill \(Representative: Jeong Pil-mo, proposed July 1, 2021\)](#) - (Status: Ended; Type: Bill). Combined industrial promotion with trust-building measures; did not become law but shaped policy discussions.
- [Act on Algorithms and Artificial Intelligence \(Representative: Yoon Young-chan, proposed Nov 24, 2021\)](#) - (Status: Ended; Type: Bill). Proposed to regulate algorithmic systems and automated decision-making; key concepts migrated into guidance and later statutes.
- [AI Industry Promotion and Trust-Building Bill \(Representative: Yoon Doo-hyun, proposed Dec 7, 2022\)](#) - (Status: Ended; Type: Bill). Continued focus on aligning industrial policy with governance; another legislative input into the final Basic Act.
- [Digital Strategy of South Korea \(national digital transformation strategy\)](#) - (Status: Enacted/Published; Type: National Strategy). Sets objectives for digital transformation across government and industry, including data infrastructure and AI adoption.
- [AI Responsibility Bill \(Representative: Hwang Hee, proposed Feb 28, 2023\)](#) - (Status: Ended; Type: Bill). Parliamentary initiative focused on accountability, transparency and remedies for automated harms.

- [Personal Information Protection Act \(amendment including provisions on automated decision-making/AI\)](#) - (Status: Changed; Type: Amendment). PIPA amendments added AI-relevant obligations, strengthened PIAs, and clarified automated decision-making safeguards.
- [Digital Bill of Rights \(Digital Rights Charter / government proposal\)](#) - (Status: Proposed; Type: Charter/Proposal). A government-level articulation of digital rights including data protection, algorithmic transparency and access to remedy.
- [AI Responsibility and Regulation Bill \(Representative: Ahn Cheol-soo, proposed Aug 8, 2023\)](#) - (Status: Ended; Type: Bill). Another parliamentary attempt to create a rights-and-liability framework for AI systems.
- [Generative AI Ethics Guidebook \(NIA / KCC – sectoral guide for generative AI\)](#) - (Status: Enacted/Published; Type: Sectoral Guidebook). Practical guidance for developers and platforms on generative models addressing safety, content moderation and provenance.
- [Act on the Promotion of AI Development and Establishing a Trustworthy AI Framework \(AI Basic Act\)](#) - (Status: Passed; Type: Act). The central statutory framework establishing objectives for promotion, trust-building obligations, and enabling powers for subordinate rules.
- [AI Privacy Risk Management Model \(안전한 AI-데이터 활용을 위한 AI 프라이버시 리스크 관리 모델\) - Personal Information Protection Commission](#) - (Status: Enacted/Published; Type: Model/Guidelines). Technical model for identifying and managing privacy risks specific to AI systems.
- [Guide on Processing Publicly Available Personal Data for AI Development and Services](#) - (Status: Enacted/Published; Type: Guidance). PIPC guidance addressing when and how publicly available personal data can be used for model training and services.
- [Automated Decision Rights Guide \(자동화된 결정에 대한 정보주체의 권리 안내서\) - Personal Information Protection Commission](#) - (Status: Enacted/Published; Type: Rights Guide). Explains data subject rights and safeguards against opaque automated decision-making.
- [Generative AI Service User Protection Guideline \(생성형 인공지능 서비스 이용자 보호 가이드라인\) - Broadcasting and Communications Commission](#) - (Status: In force; Type: Regulatory Guideline). Sector-focused obligations for user protection, transparency, and redress in generative-AI services in broadcasting and communications.
- [Enforcement Decree \(draft\) of the Act on the Promotion of AI Development and Establishing a Trustworthy AI Framework \(AI Basic Act\) - package of subordinate regulations](#) - (Status: Proposed; Type: Draft Enforcement Decree). Draft subordinate rules intended to operationalize duties and reporting requirements from the Basic Act.
- [Notice on Personal Information Impact Assessment \(개인정보 영향평가에 관한 고시\) - amendment introducing AI-specific/AI-related assessment criteria for public institutions](#) - (Status: In force; Type: Notice). Adds AI-specific assessment criteria for PIAs applicable to public bodies, tightening oversight of government AI use.

Key Themes and Priorities

Several cross-cutting priorities appear consistently across South Korea's instruments: human-centered design and ethics; privacy and data governance; risk-based oversight of high-impact systems; promotion of domestic AI industry and research; transparency and user-protection for generative AI; and inter-agency coordination. The balance between promotion and trust-building is a deliberate policy choice: South Korea seeks to support commercialization while managing reputational, legal and privacy risks.

Governance Structure

South Korea's governance relies on multiple actors. The Ministry of Science and ICT leads broad AI policy and industrial measures; the Personal Information Protection Commission (PIPC) issues privacy rules and technical models; the Broadcasting and Communications Commission (KCC) regulates content, telecom and generative-AI services; other ministries (Ministry of Interior and Safety, Ministry of Trade, Industry and Energy) play sectoral roles. The AI Basic Act creates a statutory coordination framework and authorizes subordinate regulations and agency actions.

Implementation Status

By 2025 the AI Basic Act has been enacted, and numerous PIPC and sectoral guidance documents are published and in force. Several earlier parliamentary bills did not pass but informed the Basic Act. Subordinate legislation (the Enforcement Decree) and rules remain in draft form, meaning that many operational obligations for reporting, classification of high-risk systems, and penalties are set to be clarified. Public sector PIAs are already being updated to include AI-specific criteria, signaling active oversight of government AI deployments.

Future Developments

Key near-term developments to monitor: finalization of the AI Basic Act Enforcement Decree and implementing rules; harmonization between PIPC privacy safeguards and Basic Act obligations; potential expansion of sectoral regulations for financial, healthcare and transport AI; and ongoing publication of technical standards and audit frameworks. Legislative activity may continue as stakeholders refine liability, transparency and redress mechanisms.

International Context

South Korea's approach mirrors international trends toward risk-based, sector-sensitive regulation that pairs national industrial strategy with rights protections. South Korea actively coordinates with international fora and adapts best practices from the OECD, EU and other advanced regulators while tailoring measures to domestic policy aims.

Primary government portals and agency guidance (e.g., PIPC, NIA, KCC) provide source materials and implementation guidance. For consolidated government-level information consult the Korean government AI portal: [Korean Government AI Portal](#).

Spain — AI Regulatory Landscape Summary

Overview

Spain's AI regulatory architecture in 2025 is an intersection of targeted national programmes, administrative instruments and institutional design intended to implement, complement and operationalise EU-level AI policy. The policy mix emphasises: research and university–industry cooperation (Cátedras ENIA), environmental sustainability of AI systems (Programa Nacional de Algoritmos Verdes — PNAV), regulatory experimentation (the National AI Sandbox / Entorno de pruebas de Inteligencia Artificial), institutional supervision and coordination (Agencia Española de Supervisión de la Inteligencia Artificial — AESIA via Royal Decree 729/2023) and an anticipated statutory framework (Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial).

These instruments form a layered approach: promotional and capacity-building measures sit alongside operational testbeds and a statutory supervisory entity, with a draft law intended to formalise substantive obligations and enforcement tools at the national level. Spain positions its instruments to be complementary to the EU AI Act and to use domestic policy levers (research funding, public procurement, regulatory sandboxes) to influence market behaviour and public-sector deployments.

Regulatory Instruments

- [Order ETD/1180/2022 establishing and calling for Cátedras ENIA \(university–industry AI chairs\) \(Cátedras ENIA\)](#) - Administrative order creating a competitive mechanism to fund and structure university–industry chairs focused on AI research, education and technology transfer. Status: In force. Type: Administrative order / programme.
- [Order TDF/304/2025 \(27 March 2025\) modifying Order ETD/1180/2022 on Cátedras ENIA](#) - Modification of the original bases governing Cátedras ENIA to clarify selection criteria, reporting obligations and align chairs with national strategic priorities and EU requirements. Status: Enacted/Published. Type: Administrative amendment.
- [National Programme for Green Algorithms \(Programa Nacional de Algoritmos Verdes - PNAV\)](#) - A national programme setting objectives, funding lines and standards to reduce the environmental footprint of AI systems; it coordinates research grants, incentives and procurement preferences to promote energy-efficient models and best practices. Status: Enacted/Published. Type: National programme / policy initiative.
- [National AI Sandbox \(Entorno de pruebas de Inteligencia Artificial\)](#) - A supervised sandbox environment (first Spanish EU AI sandbox) allowing public and private actors to test AI systems under controlled conditions with regulatory guidance, risk mitigation and monitoring protocols. Status: Enacted/Published. Type: Regulatory sandbox / pilot environment.
- [Royal Decree 729/2023 approving the Statute of the Spanish Agency for AI Supervision \(Agencia Española de Supervisión de la Inteligencia Artificial - AESIA\)](#) - Royal Decree that sets out the mission, structure, competencies and coordination mechanisms for AESIA, Spain's national supervisory body for AI. Status: In force. Type: Royal Decree / agency statute.
- [Draft Bill: Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial](#) - Draft legislative text that proposes comprehensive national rules on AI governance, use by public bodies, user rights, enforcement and coordination with AESIA and other regulators. Status: Draft. Type: Draft national law / anteproyecto de ley.

Key Themes and Priorities

Several recurrent themes emerge across the instruments: (1) risk-based governance and a preference for tailored, sector-sensitive oversight; (2) experimental governance through sandboxes and pilot programmes to balance innovation with safety; (3) sustainability, demonstrated by PNAV's focus on green algorithms and energy-aware model design; (4) capacity-building and knowledge transfer through the Cátedras ENIA; and (5) institutionalisation of supervisory capacity through AESIA, enabling coordination with EU counterparts and national sectoral regulators. Transparency, public-sector accountability and alignment with EU law (notably the EU's AI Act and related guidance) are visible priorities informing the draft law and AESIA's remit.

Governance Structure

At the centre of Spain's governance architecture is AESIA, whose statute (Royal Decree 729/2023) articulates functions such as supervision, market oversight, guidance issuance, coordination with sectoral authorities and international cooperation. AESIA is designed to interact with other national agencies (data protection authorities, competition authorities, sectoral regulators) and to play a role in cross-border cooperation with EU supervisory networks under the EU AI Act. Practical governance of programmes like PNAV and Cátedras ENIA falls to the relevant ministries and government departments responsible for science, digital policy and industry, often in partnership with research funding bodies and regional governments. The National AI Sandbox is operated under protocolised governance combining technical review boards, ethics oversight and AESIA coordination to ensure regulatory alignment during experimentation.

Implementation Status

Implementation is heterogeneous. Royal Decree 729/2023 is in force and provides AESIA with a legal foundation; the agency's operational development (staffing, delegated powers) continues as AESIA assumes responsibilities. The National AI Sandbox and PNAV have been publicly announced and published, enabling calls for participation, pilot projects and funding calls; they are active levers for experimentation and green-AI projects. The Cátedras ENIA initiative had an initial call under Order ETD/1180/2022 and was substantively revised by Order TDF/304/2025 (27 March 2025) to clarify selection, deliverables and monitoring. The Anteproyecto de Ley remains at draft stage: it signals the intent to create a cohesive statutory regime but will not be binding until enacted. Coordination with EU-level rules is an active implementation priority, particularly to ensure that AESIA and sandbox operations are interoperable with the EU's supervisory architecture and any obligations derived from the EU AI Act once fully in force.

Future Developments

Key near-term developments that will shape the landscape include the legislative fate of the Anteproyecto de Ley (its negotiation in parliament, potential amendments, and date of enactment), AESIA's progressive operationalisation (appointments, technical capabilities, supervisory procedures), expansion and results from the National AI Sandbox pilots, and concrete outputs from PNAV (guidelines, procurement criteria, research grants tied to energy-efficient algorithms). Spain will also continue to align domestic instruments with EU rulemaking and guidance documents. Stakeholders should watch publication of AESIA's regulatory guidance, sandbox outcomes, and any parliamentary debates amending the draft law.

International Context

Spain's approach is intentionally compatible with the EU's regulatory trajectory: the emphasis on a supervisory body, risk-based oversight and experimental sandboxes reflects EU priorities. Spain also seeks to contribute to international debates on AI sustainability by piloting green-algorithm standards. AESIA is expected to act as Spain's representative in EU supervisory networks and to coordinate with international partners on technical standards, cross-border supervision and enforcement cooperation. For reference, Spanish legal instruments are

typically published in the [Boletín Oficial del Estado](#) and EU legal instruments and guidance are available via [EUR-Lex](#). Additional Spanish official information and programme pages are published on national portals such as the government's AI pages and agency websites (e.g., [Agencia Española de Supervisión de la Inteligencia Artificial \(AESIA\)](#) where AESIA maintains announcements and guidance).

Overall, Spain combines promotional, experimental and supervisory instruments to create an ecosystem designed to encourage innovation while preparing for the responsibilities of ex post and ex ante supervision under an EU-aligned statutory framework. Stakeholders — industry, academia, civil society and regional governments — should monitor AESIA rulemaking, sandbox outcomes and the parliamentary process for the Anteproyecto to understand evolving compliance obligations and opportunities for participation in national programmes such as PNAV and Cátedras ENIA.

Sweden — AI Regulatory Landscape Summary

Overview

Sweden's artificial intelligence regulatory framework in 2025 is the product of layered instruments: national policy documents and expert reports that set strategy and operational priorities, combined with the direct applicability of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). The national approach paper ("Nationell inriktning för artificiell intelligens") sets high-level objectives: support innovation and research, mainstream trustworthy and human-centric AI in public services, protect fundamental rights, and coordinate implementation across agencies. The AI Commission's Roadmap (SOU 2025:12) translates strategy into a detailed action plan for government agencies, the research community and industry. The expert report "Anpassningar till AI-förordningen — Betänkande av Utredningen om AI-förordningen" (SOU 2025:101), under review, focuses on concrete legal and administrative adjustments required to operationalise the EU AI Act in Sweden.

Regulatory Instruments

- [National approach to artificial intelligence \(Nationell inriktning för artificiell intelligens\)](#) - National policy/strategy document published to set Sweden's long-term priorities for AI. Status: Enacted/Published. Type: Strategic policy guidance.
- [Regulation \(EU\) 2024/1689 — Artificial Intelligence Act](#) - EU-level regulation establishing harmonised, risk-based legal requirements for AI across the European Union. Status: In force. Type: EU regulation (directly applicable in Sweden).
- [AI-kommissionens Färdplan för Sverige \(AI Commission's Roadmap for Sweden, SOU 2025:12\)](#) - Commission report providing a detailed roadmap and operational proposals for public administration and industry. Status: Enacted/Published. Type: Government commission report / SOU.
- [Anpassningar till AI-förordningen — Betänkande av Utredningen om AI-förordningen \(SOU 2025:101\)](#) - Expert inquiry report recommending legal and administrative adaptations to align Swedish rules and enforcement with the EU AI Act. Status: Under review. Type: Government inquiry report / SOU (under consideration).

Key Themes and Priorities

Four themes cut across Swedish documents and the EU Act: (1) a risk-based regulatory approach — consistent with the EU AI Act — targeting the most sensitive/high-risk AI applications with mandatory requirements while avoiding undue burdens on low-risk innovation; (2) trustworthy, human-centric AI that preserves fundamental rights (privacy, non-discrimination, freedom of expression) and ensures human oversight; (3) enabling innovation, research and public-sector digital transformation, with a focus on procurement, testbeds and skills; and (4) building institutional capacity for enforcement, market surveillance and cross-sectoral guidance. The national reports stress transparency and accountability for public-sector AI use and call for clear guidance to support public procurers and civil servants.

Governance Structure

Governance combines EU and national layers. The AI Act establishes EU-level rules and coordination mechanisms among member states while requiring national competent authorities for enforcement and market surveillance. Swedish governance priorities in 2025 include: identifying and resourcing national competent authorities (sectoral agencies for health, transport, finance, consumer protection and data protection), designating a lead coordination body for AI at the national level, and strengthening capabilities within agencies (technical testing, conformity

assessment, inspection). The AI Commission's Roadmap recommends roles for central government ministries, sectoral regulators and research agencies, alongside proposals for inter-agency coordination forums and public-private partnerships to promote safe innovation.

Implementation Status

The AI Act is in force at EU level and therefore applicable in Sweden. National implementation tasks are underway: publication of national strategy and roadmap documents, completion of expert inquiries recommending statutory and administrative changes, and preparatory work by agencies to develop guidance and enforcement capacity. The AI-kommissionens report (SOU 2025:12) contains timelines and milestones to accelerate capacity building. The Anpassningar inquiry (SOU 2025:101) is under review and expected to feed into government proposals for legislative and administrative adaptations (e.g., clarifying competent authorities' mandates, administrative procedures, and procurement rules).

Future Developments

Short- to medium-term developments include: government decisions on the Anpassningar inquiry recommendations, potential bills or ordinances to align national law with the EU AI Act, and formal designation and resourcing of national competent authorities. Sweden will also proceed with guidance and toolkits for public procurement, sector-specific guidance for regulated sectors (healthcare, transport, finance), and initiatives to support research, testbeds and workforce skills. Ongoing EU-level developments, guidance from EU bodies, and cross-border coordination will shape final enforcement practices.

International Context

Sweden's framework sits squarely within the EU regulatory ecosystem. The EU AI Act (Regulation (EU) 2024/1689) provides the primary legal standards; Swedish national strategy documents and inquiry reports focus on how to implement those standards domestically while pursuing national innovation priorities. Sweden also monitors international standardisation and OECD, Council of Europe and other multilateral work on AI to ensure interoperability of rules and to support trade and research collaboration. For further reference: the EU text is available at [EUR-Lex — Regulation \(EU\) 2024/1689](#) and Swedish government materials are accessible via [Government Offices of Sweden](#) and public reports on Swedish inquiries at [regeringen.se](#).

In sum, Sweden in 2025 pursues an approach that combines EU-mandated risk-based regulation with national strategy to secure innovation, public-sector modernisation and rights protection. The immediate focus is practical implementation: aligning agencies, updating sectoral rules where needed, issuing guidance, and ensuring enforcement capacity so that both private and public actors can comply with the new EU rules while continuing to develop AI responsibly.

Switzerland — AI Regulatory Landscape Summary

Overview

Switzerland's approach to regulating artificial intelligence is pragmatic, coordinated and sectorally differentiated. It places a strong emphasis on modernised data protection, public-sector governance, agency-level supervision (particularly in finance and communications), and international alignment with human-rights and safety frameworks. Rather than a single, highly prescriptive AI statute, the Swiss model combines: (1) foundational legislation governing data and rights (the revised Federal Act on Data Protection — FADP — and the Data Protection Ordinance — DPO); (2) interdepartmental policy work and national strategies that set priorities and principles; and (3) sectoral guidance and supervisory instruments such as FINMA's guidance for financial institutions and agency-level operational tools for public administration use.

Regulatory Instruments

- [Challenges of Artificial Intelligence: Report of the Interdepartmental Working Group on Artificial Intelligence to the Federal Council](#) - Comprehensive early assessment identifying legal, economic and social challenges; sets out coordination needs and recommended priorities across departments. Status: Enacted/Published. Type: Policy report.
- [Digital Switzerland Strategy](#) - National digitalisation strategy with objectives for AI research, skills, public-sector digital services, and economic competitiveness. Status: Enacted/Published. Type: Strategy.
- [Guidelines on Artificial Intelligence for the Federal Administration](#) - Operational guidance for federal entities covering transparency, documentation, human oversight and risk assessment for AI deployments. Status: Enacted/Published. Type: Guidelines/Administrative policy.
- [Federal Act on Data Protection \(FADP\) — total revision](#) - Modernised data-protection statute strengthening individual rights, introducing tailored obligations for data controllers and processors, and updating cross-border data-flow rules relevant to AI systems. Status: In force. Type: Primary legislation.
- [Data Protection Ordinance \(DPO\) — implementing ordinance to the revised FADP](#) - Implements technical and procedural details of the revised FADP, clarifying duties such as record-keeping, security measures and DPIA-like processes applicable to AI-related processing. Status: In force. Type: Ordinance/Secondary legislation.
- [Overview of potential regulatory approaches for artificial intelligence \(OFCOM report to the Federal Council\)](#) - Analytical report examining regulatory models (principles-based, risk-based, sectoral, technology-specific), trade-offs and recommendations for federal deliberation. Status: Enacted/Published. Type: Analytical report.
- [FINMA Guidance 08/2024: Governance and risk management when using artificial intelligence](#) - Sector-specific supervisory guidance that integrates AI risk management into prudential governance, model risk controls, outsourcing, and third-party vendor oversight for financial institutions. Status: Enacted/Published. Type: Supervisory guidance.
- [Fact sheet on the use of generative AI tools in the Federal Administration](#) - Practical, short-form controls for staff on confidentiality, IP, data handling and acceptable use when using large language models and other generative tools. Status: Enacted/Published. Type: Fact sheet / operational guidance.
- [Strategy: Use of AI systems in the Federal Administration](#) - Strategic framework for adoption, procurement, governance and accountability for AI across federal agencies, including governance roles and risk management expectations. Status: Enacted/Published. Type: Strategy.

- [Federal Council decision to ratify the Council of Europe Convention on Artificial Intelligence](#) - Political decision to ratify the Council of Europe's AI Convention, signalling formal alignment with rights-based multilateral standards. Status: Passed. Type: Executive decision / international treaty action.
- [Switzerland signs the Council of Europe Convention on Artificial Intelligence \(AI Convention\)](#) - Formal signing step (reported as proposed in national processes) toward treaty accession and international alignment. Status: Proposed. Type: International treaty action.

Key Themes and Priorities

Across instruments, several recurring priorities emerge: (1) data protection and individual rights are central — the revised FADP and DPO anchor privacy obligations for AI systems; (2) risk-based governance — guidance (particularly for the public sector and finance) expects proportionate risk assessments, human oversight and model documentation; (3) operational readiness in the public sector — particular emphasis on procurement, staff guidance and controls for generative AI; (4) sectoral supervision — supervisors such as FINMA translate general principles into sector-appropriate controls; and (5) international alignment — policy documents and the Council of Europe Convention engagement signal a commitment to align Swiss practice with international human-rights and safety norms.

Governance Structure

Coordination is delivered through interdepartmental working groups, the Federal Council's strategic oversight, and agency-level implementation. Key actors include the Federal Council and Federal Chancellery (policy coordination), the Federal Data Protection and Information Commissioner (FDPIC) for data-protection oversight, the Federal Office of Communications (OFCOM / Bakom) for analytical policy inputs and sectoral inquiry, and FINMA for the financial sector. Operational IT and procurement functions inside the Federal Administration (including federal IT steering bodies) implement the administration's AI strategy and guidelines. Interagency reports and working-group outputs provide the cross-cutting glue that links strategy to statutory and supervisory action.

Implementation Status

The revised FADP and its implementing DPO are in force and provide the enforceable privacy framework that applies to AI-driven processing. Guidance for the Federal Administration and targeted instruments (generative-AI fact sheets, the Administration's AI strategy) are published and being integrated into procurement and operational procedures. FINMA's guidance (Guidance 08/2024) is an active supervisory instrument for firms in the financial sector. OFCOM's analytical report has informed federal debate but did not itself impose obligations. The Federal Council's decision to ratify the Council of Europe Convention marks a political decision; formal international steps (signing/ratification deposit) are recorded as proposed or passed in national processes and will trigger further implementation obligations when completed.

Future Developments

Expect continued incremental development rather than a single comprehensive AI statute in the near term: more supervisory guidance, technical standards and sector-specific duties are likely, especially where systemic risks appear (finance, health, critical infrastructure). Formal accession to the Council of Europe's Convention could introduce new treaty-derived obligations requiring domestic adjustments. Switzerland will also monitor and likely align with EU regulatory developments to maintain interoperability with the EU market.

International Context

Switzerland seeks alignment with international frameworks such as the Council of Europe's AI Convention and broader OECD and EU debates while preserving its sectoral, principle-driven model. Supervisory guidance and national strategies reference international best practice and standards. For practical resources and agency portals see the Federal Administration portal at <https://www.admin.ch>, the Federal Data Protection and Information Commissioner's site at <https://www.edoeb.admin.ch/edoeb/en/home.html>, OFCOM (Bakom) at <https://www.bakom.admin.ch/bakom/en/home.html>, and FINMA at <https://www.finma.ch/en/>. For the Council of Europe's work on AI see the Council of Europe AI pages at <https://www.coe.int/en/web/artificial-intelligence>.

In sum, Switzerland's AI policy combines a modernised data-protection foundation, pragmatic administrative governance instruments, and sectoral supervisory action, with ongoing international engagement. This calibrated approach favours flexibility and targeted intervention, with a clear focus on rights protection, operational controls in the public sector, and sector-specific prudential oversight where needed.

Taiwan — AI Regulatory Landscape Summary

Overview

Taiwan has developed one of the Asia-Pacific region's most comprehensive approaches to artificial intelligence governance, combining strategic investment frameworks with emerging AI-specific legislation and product evaluation mechanisms. The country's AI regulatory landscape reflects a balanced approach that promotes innovation while establishing guardrails for trustworthy AI development. Since designating 2017 as "year zero" for Taiwan's AI industry, the government has invested significantly in building an AI ecosystem through talent development, research infrastructure, and regulatory frameworks. Taiwan's unique position as a global semiconductor leader adds strategic importance to its AI governance approach, as the nation seeks to leverage its hardware strengths for generative AI development while establishing itself as a trusted origin for AI products in international markets.

Regulatory Instruments

- [Personal Data Protection Act \(PDPA\)](#) - Comprehensive data protection legislation enacted in 2010 and most recently amended in 2023, establishing foundational privacy requirements for personal data collection, processing, and use that directly impact AI system development. A Constitutional Court ruling mandates establishment of an independent Personal Data Protection Commission by August 2025.
- [Taiwan AI Action Plan 2.0 \(2023-2026\)](#) - The Executive Yuan's strategic framework committing approximately NT\$9-10 billion annually to grow Taiwan's AI industry to over NT\$250 billion by 2026. Focuses on talent development, generative AI advancement, and leveraging semiconductor leadership for AI innovation.
- [AI Basic Act \(Draft\)](#) - Proposed legislation published by NSTC in July 2024 establishing comprehensive AI governance principles including transparency, privacy, autonomy, fairness, cybersecurity, sustainable development, and accountability. Currently under Executive Yuan review pending legislative consideration.
- [AI Product and System Evaluation Centre \(AIEC\)](#) - Institutional framework established by MODA in December 2023 providing certification mechanisms and evaluation guidelines for AI products across ten critical dimensions including safety, fairness, privacy, and transparency, aligned with EU and US standards.

Key Themes and Priorities

- **Semiconductor-AI Integration:** Leveraging Taiwan's world-leading chip manufacturing capabilities to advance AI hardware development, edge computing, and generative AI systems.
- **Trustworthy AI Development:** Establishing evaluation frameworks and certification mechanisms that ensure AI products meet safety, fairness, and transparency standards before deployment.
- **International Alignment:** Aligning regulatory frameworks with EU AI Act requirements and US governance standards to ensure Taiwanese products' competitiveness in global markets.
- **Talent Development:** Investing in AI education across universities and vocational programs to build the skilled workforce needed for AI industry growth.
- **Privacy Protection:** Strengthening personal data protection through PDPA enforcement and the establishment of an independent privacy commission.
- **Innovation Promotion:** Providing computing resources, research funding, and startup support to accelerate responsible AI development and adoption.

- **Cross-Sector Application:** Deploying AI solutions across government, healthcare, finance, manufacturing, and transportation to improve efficiency and services.
- **Linguistic Inclusivity:** Ensuring AI systems work effectively with Taiwan's national languages to reflect the needs and values of diverse populations.

Governance Structure

- **Executive Yuan:** Provides cabinet-level oversight, funding authorization, and policy coordination across government ministries for AI initiatives.
- **National Science and Technology Council (NSTC):** Primary coordinating body for AI policy, research priorities, and development of the draft AI Basic Act. Renamed from Ministry of Science and Technology in 2022.
- **Ministry of Digital Affairs (MODA):** Leads digital governance, operates the AI Evaluation Centre, and develops product certification standards. Established in 2022.
- **Administration for Digital Industries (ADI):** Within MODA, establishes AI evaluation systems and guidelines for product assessment.
- **Taiwan AI Center of Excellence (AICoE):** Platform opened in March 2024 to streamline cross-agency efforts on AI governance rules and coordination.
- **Personal Data Protection Commission:** Independent body mandated by Constitutional Court to be established by August 2025 for dedicated privacy oversight.

Implementation Status

Taiwan's AI governance framework is in active implementation across multiple fronts. The AI Action Plan 2.0 (2023–2026) is fully operational with annual funding allocated through ministerial budgets. The AI Evaluation Centre began accepting AI product submissions for evaluation following its December 2023 inauguration, with initial focus on government agency applications and expansion to private sector systems underway. University AI research centers continue receiving funding for basic research and talent cultivation programs. International partnerships with Google, Microsoft, and Synopsys remain active, bringing investment and expertise. The draft AI Basic Act completed its 60-day public consultation period following July 2024 publication and was submitted to the Executive Yuan for review in early 2025, pending legislative consideration. The Personal Data Protection Commission establishment is on track for the August 2025 Constitutional Court deadline. Free GPU computing resources are available to AI startups for model training, reducing development costs and accelerating adoption.

Future Developments

Taiwan's AI governance landscape is poised for significant evolution in 2025 and beyond. The AI Basic Act represents the most consequential pending development—upon legislative enactment, it would establish binding legal requirements for AI governance including the seven foundational principles. The Personal Data Protection Commission's establishment by August 2025 will add dedicated independent oversight for privacy matters affecting AI systems. The AI Evaluation Centre continues developing specialized assessment protocols for generative AI and expanding certification services to additional sector applications. The AI Action Plan 2.0's 2026 target of NT\$250 billion AI industry value will drive continued investment and policy attention. International alignment efforts are expected to intensify as the EU AI Act enters full enforcement, with Taiwan seeking mutual recognition arrangements to reduce duplicative certification burdens for exporting companies. The government is also exploring enhanced mechanisms for public participation in AI governance, building on citizens' deliberative assembly initiatives launched by MODA.

International Context

Taiwan's AI governance approach explicitly positions the nation within global regulatory frameworks while leveraging its unique strengths. The AI Evaluation Centre's criteria incorporate EU AI Act requirements, enabling Taiwanese products to demonstrate compliance with the world's most comprehensive AI regulation—a strategic advantage for companies exporting to European markets. Alignment with US frameworks including the NIST AI Risk Management Framework informs technical assessment methodologies. The draft AI Basic Act draws on OECD AI Principles for its ethical foundation. Taiwan's semiconductor leadership adds a distinctive dimension to its international AI role—the nation's hardware capabilities are essential to global AI development, providing leverage in international discussions on AI governance standards. Partnerships with major technology companies including Google's Smart Taiwan Initiative, Microsoft's R&D center, and Synopsys' AI design center in Hsinchu demonstrate Taiwan's attractiveness for international AI investment. Participation in international forums on AI governance enables Taiwan to contribute perspectives on semiconductor-enabled AI development while learning from global experiences. This international orientation supports export competitiveness while enabling regulatory interoperability with major trading partners.

Thailand — AI Regulatory Landscape Summary

Overview

Thailand's approach to regulating artificial intelligence (AI) in 2025 is characterized by a layered, pragmatic architecture that combines existing binding law (notably the Personal Data Protection Act B.E. 2562 (2019) or PDPA), national strategy and ethics documents, sectoral supervisory guidance, and a set of draft instruments intended to enable innovation while managing risk. The government has prioritized both adoption and safeguards: it promotes AI-driven economic development through the Thailand National AI Strategy and Action Plan (2022-2027) while addressing privacy, financial stability and consumer protection via the PDPA and sectoral guidance. Multiple drafts (royal decree, promotion act, ETDA notifications, Bank of Thailand guidance and draft legislative principles) indicate an iterative regulatory process, balancing regulatory certainty and policy experimentation.

Regulatory Instruments

- [Personal Data Protection Act B.E. 2562 \(2019\) \(PDPA\)](#) - In force; Act. The PDPA is Thailand's primary binding privacy statute and affects most AI systems that process personal data. It sets lawful bases for processing, data subject rights, security obligations, data breach notification, cross-border transfer rules and enforcement by the Personal Data Protection Commission.
- [Draft Royal Decree on Business Operations Using Artificial Intelligence Systems](#) - Draft; Royal Decree. A proposed instrument to regulate business operations that deploy AI systems at scale. The Decree (still at draft stage) is designed to set operational requirements and supervisory powers for regulated AI use-cases.
- [Artificial Intelligence \(AI\) Ethics Guidelines for Digital Thailand](#) - Enacted/Published; Guidance. National-level ethics principles promoting fairness, transparency, accountability, safety and human-centric design to guide public and private AI deployment.
- [NSTDA AI Ethics Guideline](#) - Enacted/Published; Guidance. Technical and ethical recommendations issued by the National Science and Technology Development Agency to guide researchers, developers and implementers on responsible AI practices.
- [Draft Act on the Promotion and Support of Artificial Intelligence Innovation \(AI Innovation Promotion Act\)](#) - Draft; Act. A proposed law to promote AI innovation through incentives, institutional support, and potentially a governance body for AI innovation policy. Currently under drafting/consultation.
- [Draft ETDA Notification regarding Artificial Intelligence Sandbox \(AI Innovation Testing Center\)](#) - Draft; Administrative Notification. ETDA's intended framework for controlled testing environments (sandboxes) to reconcile experimentation and consumer protection.
- [Draft ETDA Notification regarding AI Risk Assessment](#) - Draft; Administrative Notification. Proposes requirements for AI risk assessments, documentation and mitigation measures for operators of high-risk AI systems.
- [Draft Principles for AI Legislation \(Draft Principles of the AI Law\)](#) - Draft; Principles/Consultation document. High-level legislative principles under review to inform future comprehensive AI law design.
- [Bank of Thailand Draft Policy on Risk Management of the Use of Artificial Intelligence Systems \(Financial Sector AI Risk Guidelines\)](#) - Draft; Supervisory guidance. Sector-specific risk and governance expectations for AI use in the financial sector, covering model risk, explainability, governance and auditability.

- Thailand National AI Strategy and Action Plan (2022-2027) - In force; Strategy/Action Plan. Strategic priorities to accelerate AI adoption, capacity building, data stewardship and R&D while aligning ethical and regulatory considerations.

Key Themes and Priorities

Common themes across Thailand's instruments include:

- Privacy and data protection as foundational constraints (PDPA).
- Enabling innovation through sandboxes, promotion acts and strategy-oriented instruments.
- Sectoral risk management (Bank of Thailand guidance for financial institutions; ETDA draft notifications for digital services).
- Ethics and human-centered design as normative requirements (national and NSTDA ethics guidelines).
- Incrementalism: preference for guidance, pilot sandboxes and supervisory expectations rather than immediate sweeping prohibitions.

These priorities reflect a policy trade-off: support economic adoption and experimentation while reducing privacy, safety and financial stability risks.

Governance Structure

Key agencies and bodies include:

- Office of the Personal Data Protection Commission (PDPC) — enforcement and interpretation of the PDPA. Official portal: <https://www.pdpc.go.th>.
- Electronic Transactions Development Agency (ETDA) — digital economy regulator coordinating sandbox frameworks, draft notifications and technical standards. Official portal: <https://www.eta.or.th>.
- National Science and Technology Development Agency (NSTDA) — provides technical and ethics guidance. Official portal: <https://www.nstda.or.th>.
- Bank of Thailand — prudential regulator issuing AI risk management expectations for financial institutions. Official portal: <https://www.bot.or.th>.
- National AI strategy coordination bodies and relevant ministries (e.g., Ministry of Digital Economy and Society) — cross-cutting policy leadership and strategy implementation.

These actors coordinate through consultations, joint working groups and public comment processes for draft instruments.

Implementation Status

The PDPA and the National AI Strategy are active and constitute the immediate legal and policy framework. Ethics guidelines are published and actively promoted. Many AI-specific instruments remain draft: Royal Decree on Business Operations Using AI, AI Innovation Promotion Act, ETDA sandbox and risk assessment notifications, Bank of Thailand draft policy and the Draft Principles for AI Legislation. As such, enforceable, AI-specific statutory obligations remain limited to PDPA and sectoral supervisory powers; other measures are preparatory or advisory. Implementation emphasis is currently on establishing sandboxes, piloting rules, stakeholder consultations and producing sectoral supervisory expectations prior to broad mandatory rules.

Future Developments

Watch for several likely developments in the near term: enactment or revision of ETDA notifications to operationalize sandboxes and risk assessment duties; potential passage or reworking of the AI Innovation Promotion Act or Royal Decree; finalization of Bank of Thailand supervisory rules for AI in finance; and possible movement from draft principles toward a consolidated AI law in the medium term. Stakeholders should expect continued consultation-led evolution and targeted regulation for high-risk sectors first (finance, health, public procurement).

International Context

Thailand's approach aligns with international trends favoring data protection as a core constraint, the use of ethics guidelines, sandbox-based innovation regimes and sectoral supervisory guidance. Its strategy mirrors OECD and ASEAN dialogues that promote trustworthy AI while enabling innovation. Thailand also participates in regional and multilateral forums to harmonize standards and to attract investment while preserving domestic policy objectives.

For further authoritative information, consult the PDPA and agency portals: [PDPC](#), [ETDA](#), [NSTDA](#) and [Bank of Thailand](#).

Tunisia — AI Regulatory Landscape Summary

Overview

Tunisia has established an emerging AI governance framework that combines foundational personal data protection with strategic AI development planning and recent cybersecurity regulation. As an early mover in the Arab world and Africa for data protection, Tunisia enacted the [Organic Act No. 2004-63 on the Protection of Personal Data](#) in 2004, predating the AI era but establishing essential privacy principles. The [National AI Strategy and Roadmap \(2021-2025\)](#) provides strategic direction for AI development, while [Decree-Law No. 2022-54](#) addresses cybersecurity and digital crimes. While no dedicated AI-specific law exists, Tunisia's multi-instrument approach covers key aspects of AI governance from data protection to strategic development and digital security.

Regulatory Instruments

- [Organic Act No. 2004-63 on the Protection of Personal Data](#) - Tunisia's comprehensive data protection legislation establishing the National Authority for the Protection of Personal Data (INPDP) and introducing principles for lawful data collection, processing, and cross-border transfer. Provides foundational privacy framework affecting AI system development and deployment.
- [National AI Strategy and Roadmap \(2021-2025\)](#) - Strategic framework overseen by the Ministry of Industry, Mines, and Energy setting objectives for AI development through five pillars: talent development, infrastructure, data governance, networking, and awareness building. Aims to position Tunisia as a regional AI innovation leader.
- [Decree-Law No. 2022-54 on Combating Offenses Related to Information and Communication Systems](#) - September 2022 legislation addressing cybersecurity and digital crimes with provisions affecting AI applications, including data retention requirements and penalties for misinformation that impact AI-enabled content systems.

Key Themes and Priorities

- **Data Protection Foundation:** Early adoption of comprehensive personal data legislation provides baseline privacy protections for AI applications, including consent requirements and data processing principles.
- **Talent Development:** The National AI Strategy prioritizes developing AI skills through education programs, training initiatives, and building a skilled workforce for the AI industry.
- **Infrastructure Investment:** Strategic focus on establishing computing infrastructure necessary for AI development, including data centers and connectivity.
- **Data Governance:** Emphasis on data policies that enable AI development while protecting privacy and ensuring data quality for training and deployment.
- **Public Sector AI Adoption:** Deployment of AI applications in government services, particularly financial management systems for fraud detection and budget optimization.
- **Startup Ecosystem:** The 2018 Startup Act demonstrates commitment to fostering AI entrepreneurship as Africa's first AI startup legislation.
- **Cybersecurity Enhancement:** Integration of digital security measures addressing AI-related risks including misinformation and data breaches.

- **International Alignment:** Engagement with European data protection standards through Council of Europe Convention 108 and participation in international AI governance discussions.

Governance Structure

- **Ministry of Industry, Mines, and Energy:** Primary oversight authority for the National AI Strategy, coordinating AI development across government and industry.
- **National Authority for the Protection of Personal Data (INPDP):** Independent body established under the 2004 Data Protection Act responsible for privacy enforcement and data protection oversight affecting AI systems.
- **National Research and Innovation Programme:** Supports AI research initiatives and innovation ecosystem development under the National AI Strategy.
- **High Authority for Public Procurement:** Involved in AI strategy implementation, particularly regarding government AI adoption and procurement standards.
- **Ministry of Communication Technologies:** Oversees telecommunications and digital infrastructure supporting AI development.

Implementation Status

Tunisia's AI governance implementation reflects both achievements and challenges. The 2004 Data Protection Act remains fully operational with INPDP providing ongoing oversight. The National AI Strategy (2021-2025) is in mid-implementation, with progress on awareness building and initial infrastructure investments. AI applications have been successfully deployed in public finance management, demonstrating practical value. However, Tunisia's Government AI Readiness Index ranking dropped from 53rd (2020) to 56th (2023), indicating implementation challenges. Investment levels reached approximately \$14 million in 2024 with 88 AI publications in 2025, showing growing but still modest ecosystem development. Brain drain remains a significant challenge as startups seek better investment climates abroad. Decree-Law 54's implementation has raised concerns regarding its impact on innovation and freedom of expression.

Future Developments

Tunisia's AI governance landscape is poised for evolution as the 2021-2025 National AI Strategy reaches its conclusion. Assessment of strategy outcomes will inform the next phase of AI development planning. The lack of a dedicated AI law creates both uncertainty and flexibility, allowing Tunisia to observe international developments before crafting comprehensive AI legislation. Potential developments include updated data protection provisions addressing AI-specific concerns, clearer guidelines for AI in public sector applications, and frameworks for addressing AI-generated content and deepfakes. The government has signaled interest in building on the Startup Act's success to further support AI entrepreneurship. International partnerships and capacity-building initiatives continue, with stakeholder consultation workshops informing policy development. Addressing the innovation-restriction balance in cybersecurity legislation may be necessary to prevent further talent exodus.

International Context

Tunisia's AI governance approach reflects significant international engagement while maintaining regional distinctiveness. Tunisia signed the [Council of Europe Convention 108](#) for the Protection of Individuals regarding Automatic Processing of Personal Data in 2017, aligning with European data protection standards before AI-specific regulations emerged. The National AI Strategy incorporates international best practices and OECD AI Principles in its ethical framework. Tunisia participates in pan-African AI governance discussions and benefits from international stakeholder consultation workshops. However, Tunisia has not adopted AI-specific legislation comparable to the EU AI Act, maintaining a more flexible approach. The country's position as a francophone

North African nation provides bridges to both European and African AI governance communities. Regional competition from Morocco, Egypt, and other emerging AI hubs influences Tunisia's strategic priorities and urgency in AI development.

Turkey — AI Regulatory Landscape Summary

Overview

Turkey's AI regulatory framework as of November 14, 2025 combines a central national strategy, targeted action plans, agency-level guidance and draft legislation under parliamentary review. The foundational policy is the [National Artificial Intelligence Strategy \(Ulusal Yapay Zekâ Stratejisi\) 2021-2025](#), which sets strategic priorities in R&D, workforce development, data and infrastructure, sectoral deployment and standards. A 2024–2025 Action Plan updates implementation tasks and assigns responsibilities across ministries.

The Presidency reinforced the Strategy through [Presidential Circular No. 2021/18](#), instructing cross-ministerial coordination and emphasising public-sector uptake. Regulatory detail to date is delivered largely through non-binding guidance (KVKK notes, YÖK ethics guide) and sectoral policy instruments (MEB education policy), while two parliamentary bills seek to create binding statutory rules.

Regulatory Instruments

- [National Artificial Intelligence Strategy \(Ulusal Yapay Zekâ Stratejisi\) 2021-2025](#) - National roadmap setting priorities (R&D, talent, infrastructure, standards, public adoption). Status: Enacted/Published. Type: Strategy/Policy.
- [Presidential Circular No. 2021/18 on the National Artificial Intelligence Strategy](#) - Executive directive assigning responsibilities to central bodies for implementing the Strategy. Status: Enacted/Published. Type: Presidential Circular/Administrative Directive.
- [Recommendations Guide on the Protection of Personal Data in the Field of Artificial Intelligence \(KVKK\)](#) - Practical guidance interpreting Law No. 6698 (KVKK) for AI contexts: lawful basis, minimisation, transparency, DPIAs and security measures. Status: Enacted/Published. Type: Regulator Guidance (KVKK).
- [Deepfake Information Note \(Deepfake Bilgi Notu\)](#) - KVKK thematic note addressing deepfakes, synthetic media risks to privacy and reputation, and mitigation measures. Status: Enacted/Published. Type: Regulator Thematic Note.
- [Grand National Assembly of Turkey \(TBMM\) Decision Establishing an AI Research Commission](#) - Parliamentary commission to examine AI policy, legal gaps and propose reforms. Status: Passed. Type: Parliamentary Commission Decision.
- [Explanatory Note on Chatbots \(ChatGPT Example\)](#) - KVKK explanatory note clarifying personal data issues, disclosure and accountability in conversational AI deployments. Status: Enacted/Published. Type: Regulator Note.
- [Ethics Guide for Generative Artificial Intelligence Use in Scientific Research and Publication in Higher Education Institutions \(YÖK Ethical Guide\)](#) - Ethics-focused guidance for universities on generative models in research and academic publishing. Status: Enacted/Published. Type: Sectoral Ethics Guidance (YÖK).
- [Yapay Zeka Kanun Teklifi \(Artificial Intelligence Law Bill\) — TBMM Esas No. 2/2234](#) - Draft comprehensive AI law proposing obligations, liability frameworks and enforcement; currently under parliamentary review. Status: Under review. Type: Parliamentary Bill.
- [National Artificial Intelligence Strategy 2024-2025 Action Plan](#) - Detailed implementation timetable and assigned agency tasks to operationalise the Strategy. Status: Enacted/Published. Type: Action Plan/Implementation Roadmap.

- [Bill on Amendments to Certain Laws Regarding Artificial Intelligence \(Kanun Teklifi — Esas No. 2/3358\)](#) - Legislative proposal to amend existing statutes for AI compatibility (e.g. liability, administrative law); under review in TBMM. Status: Under review. Type: Parliamentary Bill/Amendment Package.
- [Policy Document and Action Plan on Artificial Intelligence in Education \(Eğitimde Yapay Zekâ Politika Belgesi ve Eylem Planı 2025-2029\)](#) - MEB's sectoral strategy for AI in education: curricula, teacher training, pilot deployments, and safeguards. Status: In force. Type: Sectoral Policy & Action Plan.
- [Yapay Zeka ve Eğitim: Öğretmenler İçin Uygulamalı Prompt Mühendisliği ve Üretken Araçlarla Yenilikçi Öğrenme Stratejileri \(Teacher Guide\)](#) - Practical handbook for educators on safe, pedagogically sound use of generative AI tools. Status: Enacted/Published. Type: Practical Guidance/Capacity Building.
- [National Artificial Intelligence Strategy 2021-2025 \(Updated 2024-2025 Action Plan\)](#) - Consolidated public-facing strategy document reflecting the original strategy and the updated action plan. Status: In force. Type: Consolidated Strategy & Action Plan.

Key Themes and Priorities

Common themes across Turkey's instruments include: human-centred AI and ethics (YÖK guidance, Strategy principles), alignment with data protection (KVKK guidance, chatbots/deepfake notes), capacity building (education policy, teacher guide, national R&D priorities), coordinated implementation (Presidential Circular and Action Plans) and legislative harmonisation (TBMM bills). Risk management, transparency and human oversight recur as operational priorities. Sectoral focus — particularly on education and higher education — reflects an early-stage, capacity-development approach to mainstreaming AI while protecting academic integrity and student welfare.

Governance Structure

Lead and coordinating bodies include the Presidency (political direction and Presidential Circular implementation), the Ministry of Industry and Technology (strategy implementation and industrial policy interface), KVKK (personal data guidance and enforcement under Law No. 6698), YÖK (higher education policy and ethics), MEB (education deployment and teacher training), TÜBİTAK (science, R&D funding and standards), and TBMM via its AI Research Commission (legislative review). Sectoral regulators such as BTK may exercise domain-specific oversight where communications, consumer protection or cybersecurity intersect with AI systems.

Implementation Status

Policy documents, KVKK guidance and education-sector plans are active and being implemented through training programmes, guidance dissemination and pilot projects. The TBMM bills remain under parliamentary review and therefore do not yet impose statutory AI-specific obligations. As a result, enforcement is principally through existing legal regimes (data protection, consumer law, administrative procurement rules) and through reputational/compliance incentives tied to public funding and procurement.

Future Developments

Expect adoption of at least some legislative measures if political and parliamentary consensus forms around a risk-based approach. Potential future developments include: clarified liability rules, mandatory risk assessments for high-risk systems, transparency obligations, formal supervisory powers for a designated agency, and sectoral standards for government procurement. Continued alignment with EU/ OECD/UNESCO frameworks is indicated in strategy documents and will shape legislative drafting.

International Context

Turkey positions its approach in dialogue with international standards and multilateral fora, citing OECD and UNESCO principles and aiming for interoperability with EU regulatory trends while tailoring measures to national priorities such as digital sovereignty, workforce development and public-service transformation. For primary source materials consult the online government AI portal: [https://government AI portal](https://government-ai.portal/) and regulator pages such as the KVKK website for the AI guidance and thematic notes.

Ukraine — AI Regulatory Landscape Summary

Overview

Ukraine has developed a comprehensive AI regulatory framework distinguished by its phased voluntary-to-mandatory implementation approach, development during unprecedented wartime circumstances, and strategic alignment with European and international democratic standards. The country's journey from strategic vision to operational governance spans five years, beginning with the [Concept of Artificial Intelligence Development in Ukraine](#) approved in December 2020, progressing through the [Roadmap for AI Regulation](#) in October 2023 and [White Paper](#) in June 2024, implementing sector-specific [media](#) and [marketing](#) guidelines throughout 2024, and achieving international dimension through signing the [Council of Europe Framework Convention on AI](#) in May 2025. This regulatory architecture reflects Ukraine's position as country simultaneously confronting Russia's invasion, pursuing European Union candidacy, building democratic institutions, and fostering thriving technology sector with approximately 150 AI development companies representing Eastern Europe's largest concentration. The framework emphasizes human rights protection, democratic values preservation, and rule of law maintenance as foundational principles, implemented through "bottom-up" methodology where voluntary compliance and self-regulation during Stage One (2023-2025) prepare for binding legislation during Stage Two (2026 onwards). Coordination centers on the [Ministry of Digital Transformation](#) working with the [Expert Committee on the Development of Artificial Intelligence](#), engaging multiple stakeholders including civil society, industry, and international partners. Ukraine's approach serves multiple strategic objectives: demonstrating European alignment supporting EU candidacy, building institutional capacity for accession, attracting investment, countering Russian disinformation, and positioning Ukraine as responsible innovation leader. The regulatory development during wartime, with AI technologies playing crucial defense roles while civilian governance maintains human rights standards, exemplifies Ukraine's commitment to democratic institution building despite extraordinary pressures.

Regulatory Instruments

- [Concept of Artificial Intelligence Development in Ukraine](#) (December 2020) - Strategic framework establishing 2020-2030 objectives including increasing competitiveness through AI deployment, harmonizing legislation with international standards, and ensuring compliance with human rights and democratic values, approved by Cabinet of Ministers as foundational vision document.
- [Roadmap for the Regulation of Artificial Intelligence in Ukraine](#) (October 2023) - Operational framework translating Concept's strategic vision into two-stage implementation: Stage One voluntary preparatory tools (2023-2025) including regulatory sandbox, assessment methodologies, and sectoral guidelines, followed by Stage Two binding legislation aligned with EU AI Act (2026 onwards).
- [White Paper on Artificial Intelligence Regulation in Ukraine](#) (June 2024) - Comprehensive policy document elaborating Stage One implementation in detail, providing businesses with assessment frameworks, labeling standards, voluntary code guidance, and timeline specifications for transitioning to binding requirements.
- [Guidelines for the Responsible Use of Artificial Intelligence in Media](#) (March 2024) - Sector-specific voluntary standards implementing Council of Europe journalism principles, addressing editorial accountability, transparency, disinformation counter-measures, and press freedom protection in AI-enabled journalism contexts.
- [Guidelines for the Responsible Use of AI in Advertising and Marketing](#) (August 2024) - Sector-specific voluntary recommendations addressing consumer protection, data privacy, manipulation prevention, and transparency in AI-driven advertising and commercial communications.

- [Council of Europe Framework Convention on AI, Human Rights, Democracy, and Rule of Law](#) (signed May 2025) - World's first legally binding international AI treaty ensuring systems respect human rights, democratic values, and rule of law, requiring Verkhovna Rada ratification before creating binding domestic obligations and connecting national frameworks to international accountability mechanisms.

Key Themes and Priorities

Human Rights Protection represents Ukraine's paramount AI governance priority, with all instruments emphasizing dignity, privacy, non-discrimination, free expression, and democratic participation as non-negotiable requirements transcending commercial or efficiency considerations. **European Integration** pervades the regulatory framework, with explicit commitments to EU AI Act alignment, Council of Europe standards implementation, and OECD principles operationalization, serving both technical governance and geopolitical objectives of anchoring Ukraine within European institutions. **Phased Implementation** through voluntary Stage One before mandatory Stage Two reflects pragmatic recognition that effective governance requires business readiness, regulatory capacity building, and self-regulation culture rather than immediate comprehensive legislation risking non-compliance or innovation chilling. **Multi-Stakeholder Collaboration** ensures regulatory development engages government, industry, civil society, and international partners, building legitimacy and practical feasibility through inclusive processes rather than top-down imposition. **Sector-Specific Adaptation** recognizes that media, marketing, healthcare, finance, and other domains face unique AI governance challenges requiring tailored approaches beyond general principles, demonstrated through dedicated sectoral guidelines. **International Accountability** through Council of Europe Convention signature creates external oversight reinforcing domestic democratic institutions and providing civil society additional tools for ensuring government and industry accountability. **Innovation and Competitiveness Balance** seeks to protect rights and democracy while supporting Ukraine's significant AI sector, enabling responsible development rather than hindering technological advancement through premature or excessive regulation. **Transparency and Explainability** across all instruments mandate understandable disclosure of AI presence, capabilities, and decision-making, enabling informed engagement by affected individuals and democratic oversight by civil society. **Defense-Civilian Distinction** maintains that military AI applications remain outside civilian governance frameworks, addressing national security imperatives while preserving democratic standards for non-military uses. **Wartime Governance Resilience** demonstrates Ukraine's determination to continue democratic institution building despite Russia's invasion, using regulatory development as concrete domain showcasing commitment to European values distinguishing country from authoritarian alternatives. **Post-War Reconstruction Framework** positions AI governance as foundation for Ukraine's recovery supported by international partners expecting adherence to democratic standards and human rights protections. **Regional Leadership** establishes Ukraine as AI governance pioneer among Eastern European, post-Soviet, and EU candidate countries, creating diplomatic capital and enhanced international influence.

Governance Structure

Ukraine's AI governance centers on the [Ministry of Digital Transformation](#) serving as primary policy coordinator across sectors, established under Vice Prime Minister Mykhailo Fedorov's leadership and responsible for overall regulatory framework development, international engagement, and Stage Two legislative preparation. The [Expert Committee on the Development of Artificial Intelligence in Ukraine](#), established December 21, 2019, provides specialized technical guidance through four working groups: **AI + Public Administration** (headed by Andriy Zablovskiy) addressing government service applications, **AI + Education/Science** (headed by Dmytro Chumachenko) focusing on educational and research contexts, **AI + Security/Defense** examining national security applications, and **AI + Regulation** (co-chaired by Timofiy Milovanov) developing governance frameworks. The Committee operates under Chairman Oleksiy Molchanovskiy with Deputy Minister Oleksandr Boryakov representing governmental interests. The [Cabinet of Ministers of Ukraine](#) provides strategic oversight, approving major policy decisions including the Concept, Roadmap endorsement, and eventual Stage Two legislative proposals. **Sector-Specific Regulators** implement domain governance including the National Council

of Ukraine on Television and Radio Broadcasting for media guidelines, State Service of Ukraine on Food Safety and Consumer Protection for advertising standards, and various other agencies for their respective domains. The [Verkhovna Rada](#) (Parliament) will enact Stage Two binding legislation and ratify the Council of Europe Convention, exercising legislative authority over binding requirements. **Civil Society Organizations** championed human rights considerations throughout regulatory development, maintain ongoing monitoring of implementation, and provide accountability oversight ensuring governance protects public interests. **Industry Associations** including IT Ukraine Association, Interactive Advertising Bureau, marketing organizations, and media groups contribute sector expertise, promote voluntary compliance, and provide business perspective ensuring feasibility.

International Partners including [USAID](#) through Cybersecurity for Critical Infrastructure and Digital Transformation activities, UK Aid, [Council of Europe Office in Ukraine](#), and EU institutions provide capacity-building support, comparative insights, and technical assistance. **Academic Institutions** contribute research, professional education integration, and expert analysis supporting evidence-based governance development. This distributed governance model ensures regulatory approaches are adapted to sector contexts while maintaining alignment with overarching principles and international standards, reflecting Ukraine's commitment to collaborative rather than authoritarian governance philosophies.

Implementation Status

Stage One Voluntary Phase (2023-2025) is currently operational with multiple tools deployed: the **regulatory sandbox** framework established for testing AI systems with medium or high human rights impact, though specific operational details continue refinement; **assessment methodologies** published enabling businesses to self-evaluate systems against future requirements; **labeling mechanisms** developed for transparent AI identification in media and advertising contexts; **voluntary codes of conduct** in development with industry associations promoting self-regulatory standards; and **sectoral guidelines** actively implemented in media (March 2024) and marketing (August 2024) with additional domains anticipated. **Adoption rates** for voluntary tools vary by sector, with media and technology industries showing relatively high engagement while some domains require additional outreach and support. **Business readiness assessments** conducted periodically evaluate Ukrainian AI companies' understanding of future requirements and compliance capability, informing Stage Two transition timing. **Council of Europe Convention ratification** proceeds toward Verkhovna Rada submission, estimated for late 2025 or early 2026 parliamentary approval, following signature in May 2025. **Stage Two Legislative Drafting** is underway with Ministry of Digital Transformation developing binding legislation mirroring EU AI Act provisions, informed by Stage One implementation experiences and stakeholder consultations. **International Alignment Activities** maintain ongoing dialogue with EU institutions regarding AI Act implementation, Council of Europe regarding Convention monitoring preparation, OECD regarding AI principles operationalization, and UNESCO regarding ethics framework integration. **Capacity Building** strengthens regulatory authority expertise through training programs, international exchanges, and technical assistance from partners, preparing government for eventual enforcement responsibilities. **Stakeholder Engagement** continues through regular convenings of multi-stakeholder forums, industry association dialogues, civil society consultations, and public awareness campaigns building societal understanding of AI governance. **Wartime Adaptations** recognize that Russia's ongoing invasion affects implementation capacity, resources, and timelines, with flexibility maintained while core commitments to rights protection and democratic governance preserved. **Monitoring and Evaluation** tracks voluntary tool adoption, implementation challenges, effectiveness at achieving objectives, and readiness for binding requirement transition, providing evidence base for adaptive management. **EU Integration Progress** demonstrates concrete advancement on accession criteria including rule of law, human rights protection, and regulatory approximation through AI governance development. **Future Timeline Projections** anticipate Stage One completion by late 2025 or early 2026, followed by Stage Two legislative enactment during 2026, Convention entry into force after ratification, and full transition to binding requirements during 2026-2027, though exact timelines remain subject to EU AI Act finalization, business readiness, and Ukraine's evolving circumstances.

Future Developments

Stage Two Binding Legislation represents the most significant forthcoming development, with draft AI law anticipated for Verkhovna Rada submission in 2026, establishing comprehensive legal requirements mirroring EU AI Act provisions including risk classifications, conformity assessments, transparency obligations, and enforcement mechanisms with proportionate penalties. **Additional Sectoral Guidelines** will expand beyond media and marketing to education (incorporating AI literacy and pedagogical ethics), healthcare (addressing clinical decision support and patient data protection), public administration (governing automated administrative decisions), finance (covering algorithmic trading and credit decisioning), and other domains requiring specialized governance approaches. **Regulatory Sandbox Expansion** will accommodate additional AI system testing as capacity develops, potentially expanding eligibility beyond systems with medium or high human rights impact to broader applications as experience accumulates and resources permit. **Assessment Methodology Refinement** will update evaluation frameworks as AI technologies evolve, new capabilities emerge, and implementation experiences reveal needed improvements or additional considerations. **Council of Europe Convention Entry Into Force** following Verkhovna Rada ratification will create binding international legal obligations, trigger domestic implementing legislation requirements, establish periodic reporting to Conference of the Parties, and enable international monitoring of Ukraine's compliance. **EU AI Act Harmonization** requires continuous alignment with European regulatory developments, necessitating Ukrainian legislative updates matching EU requirements as they evolve through implementation guidance, case law interpretation, and potential amendments. **Enforcement Capacity Development** will build regulatory authority capabilities for complaint investigation, compliance auditing, penalty imposition, and corrective action ordering when binding requirements take effect, including technical expertise acquisition and procedural framework establishment. **International Cooperation Expansion** through bilateral agreements, multilateral initiatives, and regional partnerships will address transnational AI governance challenges including cross-border data flows, jurisdictional enforcement coordination, and shared standard development. **Post-War Reconstruction Integration** will incorporate AI governance into Ukraine's recovery planning supported by international partners, potentially accelerating implementation through reconstruction funding conditionality and technical assistance programs. **Technology Evolution Responses** will adapt regulatory approaches to emerging AI capabilities not fully anticipated during initial framework development, including advanced generative systems, autonomous technologies, and novel application domains. **Liability Regime Establishment** in Stage Two legislation will clarify developer, deployer, and user responsibilities when AI causes harm, establishing compensatory mechanisms, insurance requirements potentially, and clear accountability chains. **Judicial Capacity Building** will prepare courts to interpret AI regulations, adjudicate disputes involving automated systems, and provide authoritative precedents guiding implementation across sectors. **Democratic Participation Enhancement** will expand civil society engagement mechanisms, public consultation processes, and transparent governance enabling continued multi-stakeholder input as frameworks mature. **Economic Impact Assessment** will measure regulatory effects on Ukrainian AI sector competitiveness, innovation rates, investment attraction, and international market access, informing refinements balancing protection with development objectives.

International Context

Ukraine's AI regulatory approach aligns extensively with international frameworks while reflecting unique national circumstances. **EU AI Act Convergence** represents the centerpiece of international alignment, with Stage Two explicitly designed to mirror European comprehensive regulatory framework, facilitating Ukrainian companies' seamless EU market access and supporting EU candidacy by demonstrating regulatory approximation progress. The convergence reflects both technical governance needs and strategic European integration objectives, with Ukraine participating in EU implementation dialogues despite non-membership status. **Council of Europe Framework Convention** signature positions Ukraine within first wave of countries embracing legally binding international AI treaty emphasizing human rights, democracy, and rule of law, demonstrating commitment to democratic governance distinguishing Ukraine from authoritarian regional alternatives including Russia. **OECD AI Principles** inform Ukrainian approaches to human-centered values, transparency, robustness, accountability, and fundamental rights respect, with Ukraine's framework operationalizing these voluntary commitments through binding domestic instruments. **UNESCO Recommendations on AI Ethics** shape approaches to cultural diversity,

inclusion, transparency, responsibility, and monitoring, particularly influencing sectoral guidelines for media and education. **Comparative Positioning** places Ukraine among proactive AI governance countries alongside EU members, United Kingdom, United States, Canada, Singapore, and other jurisdictions developing comprehensive frameworks, rather than reactive countries awaiting international consensus before acting. **Regional Leadership** establishes Ukraine as pioneer among Eastern European, post-Soviet, and EU candidate countries, with neighboring states observing Ukrainian experiences and potentially modeling approaches on Ukraine's frameworks. **Transatlantic Partnerships** through USAID support and North American engagement diversify Ukraine's international alignment beyond purely European focus, strengthening connections to democratic alliance supporting sovereignty and security. **Differentiation from Authoritarian Models** represented by China's state-centric AI governance and Russia's minimal rights protections emphasizes Ukraine's democratic values through concrete regulatory commitments, reinforcing geopolitical positioning and civilizational choice narrative. **Global South Perspectives** potentially gain representation through Ukraine's participation as developing country balancing innovation promotion with rights protection, offering model distinct from both Western regulatory strictness and authoritarian permissiveness. **Standards Harmonization** through ISO/IEC AI standards adoption, technical specifications alignment, and interoperability requirements enables Ukrainian AI companies to participate in global supply chains and markets with regulatory compatibility confidence. **Multi-lateral Governance Forums** including G7, NATO, and democratic partnership initiatives on AI provide Ukraine venues for contributing to evolving international norms, sharing implementation experiences, and learning from other countries' approaches. **Investment Signaling** through credible governance commitment demonstrates to international investors that Ukraine provides predictable regulatory environment respecting international standards despite wartime circumstances, potentially accelerating foreign direct investment in AI sector. **Post-War International Support** positions AI governance as domain demonstrating Ukraine's readiness for European integration and democratic reconstruction supported by Western partners, potentially influencing aid allocation and partnership depth during recovery phase. Ukraine's international alignment serves technical governance purposes while advancing broader strategic objectives of European integration acceleration, transatlantic partnership deepening, democratic resilience demonstration, and post-war reconstruction framework establishment, using AI regulation as concrete domain showcasing institutional capacity and values alignment essential for achieving foreign policy and security objectives in context of ongoing Russian aggression and European Union candidacy.

United Arab Emirates — AI Regulatory Landscape Summary

Overview

The United Arab Emirates pursues a deliberate, innovation-first approach to AI governance that balances national ambition with incremental risk management. The national ambition is explicit in the [UAE National Strategy for Artificial Intelligence 2031](#), which aims to position the UAE as a global AI leader by 2031 through rapid government adoption, skills development, and enabling infrastructure. Rather than a single, comprehensive AI statute, the UAE relies on a portfolio of instruments: enabling legislation (notably [Federal Decree-Law No. \(25\) of 2018 on the Projects of Future Nature](#)), national ethics guidance and toolkits, sectoral rules (especially in finance and health), and emirate/city level toolkits (Smart Dubai). This layered model supports fast-track pilots and sandboxes while encouraging voluntary compliance with ethical norms.

Regulatory Instruments

- [UAE National Strategy for Artificial Intelligence \(AI\) 2031](#) - High-level national ambitions, cross-sector priorities and government adoption targets. Status: Enacted/Published. Type: National strategy.
- [Federal Decree-Law No. \(25\) of 2018 on the Projects of Future Nature](#) - Enables interim licensing and temporary exemptions for innovative future technologies where no existing law applies; provides legal flexibility for early pilots. Status: In force. Type: Federal decree-law (enabling/interim licensing mechanism). For text and articles see the federal legislation portal at [uaelegislation.gov.ae](#).
- [Ethical AI Toolkit / AI Principles and Guidelines for the Emirate of Dubai \(Smart Dubai\)](#) - Practical ethical principles, implementation guidance and the Smart Dubai AI System Ethics Self-Assessment Tool. Status: Enacted/Published. Type: Regional/city ethical toolkit and self-assessment (non-binding). See [Smart Dubai](#) for resources.
- [Deepfake Guide \(UAE National Programme for Artificial Intelligence\)](#) - Public awareness guidance on risks, detection and reporting channels for synthetic audio/video (deepfakes). Status: Enacted/Published. Type: Awareness and risk mitigation guide. Announcements available via national press and the AI Office.
- [Guidelines for Financial Institutions Adopting Enabling Technologies \(joint UAE regulators\)](#) - Cross-regulatory supervisory guidance (CBUAE, SCA, DFSA, FSRA) describing expectations when financial firms adopt AI, cloud, DLT, biometrics and APIs. Status: Enacted/Published (consultation launched 2021, guidance subsequently issued). Type: Sectoral regulatory guidelines. See regulator portals: [Central Bank of the UAE](#), [SCA](#), [DFSA](#).
- [AI Ethics Principles and Guidelines \(UAE national AI ethics guide\)](#) - National, non-binding principles setting out fairness, transparency, accountability, human-centred design, and safety expectations for AI systems. Status: Enacted/Published (Dec 2022). Type: National ethics guidelines. Host: UAE AI Office at [ai.gov.ae](#).
- [AI Ethics Self-Assessment Tool \(beta\)](#) - A practical, web-based self-assessment for AI developers/operators to score AI systems against the UAE ethics guidelines. Status: Enacted/Published (beta). Type: Operational assessment tool (non-binding). Live at the AI Office and Digital Dubai portals, e.g. [ai.gov.ae/aiethics-self-assessment](#).
- [AI Adoption Guideline in Government Services \(UAE AI Office\)](#) - Lifecycle guidance for procurement, risk assessment, documentation, monitoring and public communication for AI in government services. Status: Enacted/Published (2023). Type: Implementation guidance for public sector adoption.

Key Themes and Priorities

Across these instruments the UAE emphasizes: (1) enabling public sector adoption and setting ambitious national targets; (2) ethics-by-design (fairness, accountability, human-centredness, explainability); (3) practical operationalisation through self-assessment tools and procurement guidance; (4) sectoral risk management (notably financial services); (5) experimentation and rapid piloting backed by legal flexibility (Decree-Law 25/2018 and sandboxes); and (6) public awareness and safety relating to misinformation risks (Deepfake Guide). The approach prioritizes guidance and governance processes over burdensome prescriptive rules so long as adequate documentation, oversight and mitigation controls are in place.

Governance Structure

Governance is distributed and collaborative: the AI Office (Minister/Office for Artificial Intelligence, Digital Economy and Remote Work Applications) leads national strategy and toolkits. Smart Dubai and Digital Dubai produce city-level toolkits and operational self-assessment instruments. Sectoral regulators (Central Bank, SCA, DFSA, FSRA) produce tailored supervisory guidance for regulated firms. The Cabinet and Council bodies (e.g. Council for Digital Wellbeing) coordinate cross-ministerial public-interest initiatives such as the Deepfake Guide. Free-zone regulators (DIFC, ADGM) operate parallel frameworks for data and autonomous systems in their jurisdictions, sometimes supplementing UAE mainland guidance.

Implementation Status

By 2025, the majority of national AI instruments are non-binding published guidance, widely used for public sector rollout and industry best practice. The AI Ethics Principles and Guidelines and the AI Ethics Self-Assessment Tool are published and available online; Smart Dubai's toolkit is implemented across Dubai entities; the Deepfake Guide has been used for public awareness campaigns; and financial regulators have issued enabling-technology guidelines and supervisory expectations. Enforcement mechanisms specific to AI remain limited; existing laws (data protection, cybercrime, consumer protection) are the primary enforcement levers where harms emerge. Interim licensing under Decree-Law 25/2018 has been used to permit novel projects where existing law is silent, enabling controlled real-world testing.

Future Developments

Expect incremental tightening in risk-sensitive sectors, ongoing alignment efforts between mainland and free-zone regimes, and the publication of additional sector-specific guidance (health, transport, defence, and consumer-facing services). The UAE may also progressively codify procedural requirements (record-keeping, audit trails, reporting obligations) for high-risk AI use cases. International engagement and adoption of global standards will likely continue to shape domestic updates.

International Context

The UAE's model follows other jurisdictions that favor a principles-based, sectoral approach while enabling experimentation (e.g., those using sandboxes and flexible licensing). The UAE actively engages international partners and benchmarks its guidance against global best practices; many national toolkits are published under Creative Commons to encourage reuse. For primary sources consult the UAE AI Office at <https://ai.gov.ae>, the federal legislation portal at <https://uaelegislation.gov.ae>, Smart Dubai at <https://www.smartdubai.ae>, and regulator websites such as the [Central Bank of the UAE](#), the [Securities & Commodities Authority](#), and the [Dubai Financial Services Authority](#).

Summary conclusion: The UAE's AI regulation landscape in 2025 is characterized by strategic ambition, operational toolkits and sectoral guidance, underpinned by a legal mechanism for experimentation (Decree-Law

No. 25/2018). Stakeholders should treat national ethics guidelines and self-assessment tools as de facto expectations while preparing for more prescriptive sector rules in high-risk domains.

United Kingdom — AI Regulatory Landscape

Summary

Overview

The United Kingdom's AI regulatory framework blends a pro-innovation philosophy with targeted risk management, sector-specific regulation, and institutional strengthening. Since the publication of the [National AI Strategy](#), the government has moved from strategic vision to operational instruments: white papers, departmental playbooks, statutory reforms affecting data and online harms, and the creation of central coordination bodies. The overall objective is to support AI-driven economic growth while managing privacy, safety, competition and national security risks. Central elements include policy documents that set direction, regulator-led guidance that interprets existing law for AI use, and newly established bodies and assurance roadmaps that aim to standardise risk management and verification.

Regulatory Instruments

- [AI Energy Council - Grid Reform and AI Growth Zones Initiative](#) - Initiative to coordinate AI deployment in energy sector and create local growth zones linking grid reform and AI innovation. Status: In force. Type: Initiative / policy programme.
- [A guide to good practice for digital and data-driven health technologies \(NHSX / DHSC\)](#) - Sector-specific guidance covering clinical evaluation, safety, data governance and adoption pathways for health AI. Status: Enacted/Published. Type: Sector guidance.
- [National AI Strategy](#) - Foundational strategic document establishing priorities across skills, research, governance and adoption. Status: In force. Type: Strategy.
- [Defence Artificial Intelligence Strategy](#) - Ministry of Defence strategy for safe and effective use of AI in defence capabilities, procurement and doctrine. Status: Enacted/Published. Type: Sector strategy.
- [National AI Strategy - AI Action Plan](#) - Operational plan to implement the National AI Strategy across government departments, funding and milestones. Status: Enacted/Published. Type: Action plan.
- [A Pro-Innovation Approach to AI Regulation \(White Paper\)](#) - Central government proposal setting a principles-based regulatory approach, focusing on harm-based interventions and regulatory sandboxes. Status: Enacted/Published. Type: White paper / policy framework.
- [Data Protection and Digital Information Bill](#) - Legislative proposal that aimed to reform data protection; this instrument is noted here as ended. Status: Ended. Type: Bill (withdrawn/ended).
- [ICO guidance: AI and data protection \(updated guidance and AI risk toolkit\)](#) - Practical guidance on lawful AI processing, DPIAs and risk-based safeguards, accompanied by an AI risk toolkit for practitioners. Status: Enacted/Published. Type: Regulatory guidance.
- [Guidance to civil servants on use of generative AI](#) - Operational rules and risk controls for public servants using large language models and generative systems. Status: Enacted/Published. Type: Internal government guidance.
- [Competition and Markets Authority - Initial report on foundation models](#) - Analysis of competition, market structure and consumer protection concerns posed by foundation models and platform power. Status: Enacted/Published. Type: Regulator report.

- [Central AI Risk Function \(CAIRF\)](#) - Cross-government risk coordination unit to identify systemic AI risks, provide guidance and escalate policy responses. Status: In force. Type: Institutional mechanism.
- [MHRA guidance: Software and AI as a Medical Device \(updated guidance\)](#) - Updated regulatory approach for software and AI used in clinical contexts, including conformity and safety expectations. Status: Enacted/Published. Type: Sector regulator guidance.
- [Online Safety Act 2023](#) - Comprehensive statute addressing online harms, platform duties and safety requirements which intersect with AI-generated content and moderation. Status: Enacted/Published. Type: Statute.
- [AI Safety Institute \(establishment following AI Safety Summit\)](#) - Institution founded to coordinate research, assurance and best practice on AI safety following the 2023 summit. Status: In force. Type: Institutional body.
- [Bletchley Declaration \(outcome of 2023 AI Safety Summit\)](#) - International outcome document emphasising multilateral cooperation on AI safety and responsible innovation. Status: Enacted/Published. Type: International declaration.
- [Generative AI Framework for HMG](#) - Framework specifying protective measures, procurement controls and acceptable uses of generative AI within central government. Status: Enacted/Published. Type: Government framework.
- [Government response to the AI regulation white paper \(AI regulation: government response\)](#) - Official response setting next steps, timelines and commitments following the White Paper consultation. Status: Enacted/Published. Type: Government response.
- [Information Commissioner's Office - Strategic approach to AI](#) - The ICO's strategic priorities for regulating AI-related data protection and privacy issues. Status: Enacted/Published. Type: Regulator strategy.
- [AI Opportunities Action Plan \(Matt Clifford\) and Government acceptance/response](#) - Recommendations and government commitments to accelerate commercial opportunities and regional AI ecosystems. Status: Enacted/Published. Type: Action plan/report.
- [Artificial Intelligence Playbook for the UK Government](#) - Practical playbook for procurement, risk assessment and deployment of AI across public bodies. Status: Enacted/Published. Type: Operational playbook.
- [AI Security Institute \(renaming / rebrand of AI Safety Institute\)](#) - Rebranding and refocus of the safety institute to emphasise security, resilience and assurance. Status: Changed. Type: Institutional rebrand.
- [Data \(Use and Access\) Act 2025](#) - Statute modernising rules on public sector data sharing and access for research, including safeguards for privacy and national interest. Status: Enacted/Published. Type: Statute.
- [Trusted Third-Party AI Assurance Roadmap \(DSIT\)](#) - Roadmap setting out steps to establish accredited third-party assurance services for high-risk AI systems. Status: Enacted/Published. Type: Roadmap / assurance framework.

Key Themes and Priorities

Across the instruments several consistent themes appear: (1) risk-based, outcomes-focused regulation rather than prescriptive rules for all systems; (2) sectoral application of existing statutory frameworks (health, defence, online safety) rather than a single monolithic AI law; (3) emphasis on assurance, transparency and third-party validation for higher-risk systems; (4) capacity-building in government through playbooks, CAIRF and central institutes; and (5) continued support for innovation through targeted action plans, growth zones and procurement incentives. Privacy and data protection remain central, shaped by ICO guidance and the Data (Use and Access) Act, while competition and market concerns are addressed by CMA analysis.

Governance Structure

Governance is distributed. Central policy and strategy come from the Department for Science, Innovation and Technology (DSIT) and the Cabinet Office; sectoral oversight is performed by established regulators such as the ICO, MHRA and CMA; operational risk coordination is provided by the Central AI Risk Function; and specialist capability and assurance are built via the AI Safety/AI Security Institute. Departments maintain their own guidance and playbooks (for example NHSX/DHSC for health and MOD for defence), with cross-government coordination through CAIRF and interdepartmental committees. International engagement is reflected in outcomes such as the Bletchley Declaration and Summit follow-ups.

Implementation Status

By 2025, many instruments are published and operational: statutory acts (Online Safety Act 2023, Data (Use and Access) Act 2025) are in force, central bodies (CAIRF, AI Security Institute) have been established, and multiple guidance documents and sectoral standards are being applied in procurement and regulatory decision-making. The Trusted Third-Party Assurance Roadmap sets an implementation pathway, but accreditation processes and market-scale assurance services are still maturing. The government remains focused on converting the White Paper principles into practical, enforceable measures for specific high-risk uses.

Future Developments

Upcoming work includes operationalising the assurance ecosystem, publishing detailed guidance and conformity assessment criteria for high-risk systems, strengthening public sector procurement controls, and continuing international alignment on safety standards. Watch areas include potential further statutory interventions if voluntary and guidance-based approaches prove insufficient for systemic risks, and the evolution of data-sharing rules as research and public policy demands increase.

International Context

The UK's approach intentionally balances alignment with international partners (G7, summit declarations such as the [Bletchley Declaration](#)) and domestic competitiveness. The emphasis on third-party assurance and coordination functions positions the UK to engage with international standard-setting bodies while maintaining regulatory flexibility to adapt to domestic industrial priorities.

For further reference, key regulator pages include the Information Commissioner's Office at <https://ico.org.uk>, the Medicines and Healthcare products Regulatory Agency at <https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency>, and the DSIT homepage at <https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology>.

United States — AI Regulatory Landscape Summary

Overview

The United States follows a distributed, sectorally oriented approach to AI regulation that mixes federal strategy and funding with state-level operational rules and agency enforcement. Federal instruments (executive orders, memoranda, funding statutes, and R&D strategic plans) set national priorities—innovation, leadership, national security, and responsible use—while states and agencies implement concrete obligations focused on transparency, consumer protection, public-sector governance, employment, and biometric/identity harms. This summary synthesizes federal and state instruments, describes relationships between them, and identifies likely implementation and enforcement paths.

Regulatory Instruments

- [Arizona HB 2175 — Healthcare AI Insurance Claim Denial Restrictions](#) - Restricts use of automated systems to deny certain insurance claims without human review; status: Enacted/Published; type: State statute.
- [Arkansas HB 1876 — Generative AI Content Ownership \(Act 927\)](#) - Clarifies ownership/attribution rules for generative content and addresses contractual presumptions; status: Enacted/Published; type: State statute.
- [Arkansas HB 1958 — Public Entity AI Policy Requirements \(Act 848\)](#) - Requires public entities to adopt AI policies and conduct risk assessments; status: Enacted/Published; type: State statute.
- [California AB 2013 — Generative Artificial Intelligence: Training Data Transparency](#) - Imposes disclosure obligations for training datasets and model provenance for certain deployed generative systems; status: Enacted/Published; type: State statute/transparency obligations.
- [California AB 2885 — Artificial Intelligence: Unified Definition and State Agency Inventory](#) - Creates unified state definition of AI and requires agency inventories of AI systems in use; status: Enacted/Published; type: State statute/agency inventory.
- [California SB 53 — Transparency in Frontier Artificial Intelligence Act \(TFAIA\)](#) - Establishes reporting, risk assessment, and disclosure requirements for frontier models and operators; status: Enacted/Published; type: State statute focused on high-capability models.
- [California SB 942 — California AI Transparency Act](#) - Requires documentation and disclosures for automated decision-making systems used by businesses and state entities; status: Enacted/Published; type: State statute/transparency and accountability.
- [Colorado SB24-205 — Consumer Protections for Artificial Intelligence Act](#) - Consumer-facing disclosure and safeguard requirements, emphasizing transparency and mitigation of consumer harms; status: Enacted/Published; type: State consumer protection statute.
- [Illinois HB 3773 — Amendment to Human Rights Act \(AI in Employment\)](#) - Extends protections and imposes obligations to prevent algorithmic discrimination in hiring and employment; status: Enacted/Published; type: State anti-discrimination amendment.
- [Kentucky SB 4 — AI Governance Framework and Election Integrity Act](#) - Sets governance standards for state AI use and includes measures to protect electoral processes; status: Enacted/Published; type: State statute on governance/election integrity.
- [Maryland HB 956 — Workgroup on Artificial Intelligence Implementation](#) - Establishes a workgroup to study AI adoption and governance for state agencies; status: Enacted/Published; type: State study/workgroup

statute.

- [Tennessee ELVIS Act — Ensuring Likeness Voice and Image Security Act](#) - Protects individuals from unauthorized use of biometric likeness, voice, and image in generative systems; status: Enacted/Published; type: State biometric/identity statute.
- [Texas HB 149 — Texas Responsible Artificial Intelligence Governance Act \(TRAIGA\)](#) - Establishes state procurement, governance, and transparency requirements for AI used by state agencies and contractors; status: Enacted/Published; type: State governance/procurement statute.
- [Executive Order on Maintaining American Leadership in Artificial Intelligence \(American AI Initiative, EO 13859\)](#) - Early executive-level directive prioritizing AI leadership and R&D coordination; status: Changed; type: Executive Order.
- [AI in Government Act of 2019](#) - Requires agency inventories, modernization, and coordination for AI use in the federal government; status: Enacted/Published; type: Federal statute.
- [National Artificial Intelligence Initiative Act of 2020](#) - Establishes National AI Initiative for R&D coordination, workforce development, and public-private partnerships; status: Enacted/Published; type: Federal statute.
- [National Artificial Intelligence Research and Development \(R&D\) Strategic Plan \(2021 update\)](#) - Sets R&D priorities and strategic objectives; status: Enacted/Published; type: Federal strategic plan.
- [Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People \(OSTP\)](#) - Nonbinding framework outlining principles to protect civil rights, safety, and equity; status: Enacted/Published; type: Executive/OSTP guidance.
- [CHIPS and Science Act \(contains multiple AI-related authorizations and provisions\)](#) - Authorizes funding for semiconductor capacity, research, and AI-related infrastructure; status: Enacted/Published; type: Federal appropriations/authorization statute.
- [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence \(EO 14110\)](#) - Directed agency actions on safety and security; status: Ended; type: Executive Order (superseded/changed by later EO).
- [Algorithmic Accountability Act \(H.R. 5628, House version\)](#) - Proposed legislation to require impact assessments and oversight for high-risk automated systems; status: Proposed; type: Federal bill.
- [Algorithmic Accountability Act \(S. 2892, Senate version\)](#) - Senate companion/proposed text with similar aims on audits and accountability; status: Proposed; type: Federal bill.
- [DEEPFAKES Accountability Act \(H.R. 5586\)](#) - Proposed federal restrictions and labeling for manipulated media and deepfakes; status: Proposed; type: Federal bill.
- [National AI Research Resource \(NAIRR\) pilot \(NSF program launched as pilot\)](#) - Pilot to provide compute, data, and tools for researchers; status: In force (pilot); type: Federal research program.
- [National Security Memorandum on Artificial Intelligence \(NSM on AI, Oct 24, 2024\)](#) - Directs national-security-focused actions including model and data protections; status: Changed; type: National security directive.
- [Federal A.I. Governance and Transparency Act \(H.R. 7532\)](#) - Proposed federal bill to strengthen agency governance, transparency, and procurement rules; status: Proposed; type: Federal bill.
- [OMB Memorandum M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence](#) - Operational guidance to federal agencies on AI governance and risk management; status: Changed; type: Executive branch memorandum.
- [Preventing Algorithmic Collusion Act \(S. 232, 2025\)](#) - Proposed bill addressing antitrust risks from algorithmic coordination; status: Proposed; type: Federal bill.
- [Executive Order: Removing Barriers to American Leadership in Artificial Intelligence \(EO 14179\)](#) - Executive action emphasizing removal of regulatory barriers while maintaining safety priorities; status: In force; type:

Executive Order.

- [Creating Resources for Every American To Experiment with Artificial Intelligence \(CREATE AI Act / H.R. 2385\)](#) - Proposed legislation to codify and fund NAIRR and public experimentation resources; status: Proposed; type: Federal bill.
- [Content Origin Protection and Integrity from Edited and Deepfaked Media Act \(S. 1396, 2025\)](#) - Proposed federal requirements for content provenance and labeling to combat manipulated media; status: Proposed; type: Federal bill.
- [OMB Memorandum M-25-21: Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust](#) - Directs agencies to accelerate AI adoption with governance guardrails; status: In force; type: Executive branch memorandum.
- [OMB Memorandum M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government](#) - Guidance to streamline federal AI acquisition while managing risk; status: In force; type: Executive branch memorandum.
- [Coalition of 42 State Attorneys General Letter to AI Companies on Chatbot Safety](#) - Multi-state enforcement and outreach initiative urging safety, guardrails, and consumer protections; status: In force; type: Multi-state enforcement letter/initiative.
- [DOE Request for Information: Partnerships for Transformational Artificial Intelligence Models](#) - DOE solicitation seeking input on public-private partnerships for large models; status: Under review; type: Federal RFI.
- [Utah SB 149 — Artificial Intelligence Policy Act](#) - Requires transparency and reporting for state agency AI use and sets guidance for public-sector governance; status: Enacted/Published; type: State statute.

Key Themes and Priorities

Common themes appear across federal and state instruments: transparency (training-data and content provenance disclosures), accountable procurement and agency inventories, protection of civil rights and employment equality, biometric privacy and likeness protections, targeted consumer protections, national-security-oriented controls for frontier systems, and investments in research and compute to preserve U.S. competitiveness. There is a strong emphasis on documentation, human oversight, and impact assessments for high-risk systems.

Governance Structure

Governance is distributed across the Executive Branch (White House, OSTP, OMB), independent agencies (NSF for NAIRR pilot), sectoral regulators (HHS, FTC, EEOC, DOJ, SEC), and state governments (legislatures, attorneys general, and state procurement offices). OMB memoranda implement binding requirements for federal agencies. States create binding statutes that apply to private-sector actors and public entities within their borders. Multi-state coalitions of attorneys general supplement this by coordinated enforcement actions and guidance.

Implementation Status

Implementation varies: many state laws are enacted and operational or being phased in; federal statutes focus on funding and coordination while executive orders and OMB memos require agency-level rulemaking, inventories, and procurement changes. Several federal bills remain proposed and reflect an appetite in Congress for more prescriptive, nationwide rules. Agencies are increasingly using existing consumer-protection, civil-rights, and sector-specific authorities to enforce AI-related harms while preparing for potential new legislative mandates.

Future Developments

Expect continued state-level experimentation and gradual federal consolidation via a combination of agency rulemaking, enforcement precedents, targeted legislation addressing deepfakes, algorithmic collusion, and

accountability, and further investment in public research infrastructure. Harmonization pressure will come from industry demands for national standards and from international alignment efforts.

International Context

The U.S. model contrasts with comprehensive EU-style regulation by favoring sectoral and risk-based measures and strong investments in research and industry competitiveness. However, U.S. instruments increasingly converge with international priorities—transparency, safety, and human rights—and will interact with global regimes on model provenance, export controls, and cross-border data flows.

Key references and entry points for further review include official White House and OSTP materials (e.g., [OSTP](#)), OMB memoranda pages (e.g., [OMB](#)), the NSF NAIRR pilot information (e.g., [NSF](#)), and state legislative repositories for the specific acts listed above.

Uruguay — AI Regulatory Landscape Summary

Overview

Uruguay has positioned itself as a Latin American leader in artificial intelligence governance, developing a comprehensive framework that combines legal mandates, strategic planning, and international treaty commitments. The country made history in September 2024 by becoming the [first Latin American nation](#) to sign the Council of Europe Framework Convention on AI—the world's first legally binding international AI treaty. Uruguay's approach is coordinated by [AGESIC](#) (Agency for Electronic Government and Information Society), balancing innovation promotion with responsible AI development, human rights protection, and democratic safeguards.

Regulatory Instruments

- [Law No. 20.212 Article 74 - AI and Data Strategy Mandate](#) - Enacted November 2023, this law mandates AGESIC to develop a national AI and data strategy based on international standards. It establishes 180-day deadline for regulatory recommendations and requires coordination with URCDP on data protection matters.
- [Uruguay National Artificial Intelligence Strategy 2024-2030](#) - Approved November 2024, this comprehensive strategy is built on 10 guiding principles and organized into 3 pillars (Governance, Capabilities, Monitoring) with 12 lines of action. Promotes safe, responsible AI for inclusive growth and sustainable development.
- [Council of Europe Framework Convention on AI and Human Rights](#) - Signed September 2024, Uruguay became the first Latin American country to join this first-ever internationally binding AI treaty. Establishes obligations for AI systems to respect human rights, democracy, and rule of law.

Key Themes and Priorities

Uruguay's AI governance framework reflects consistent priorities across all instruments:

- **Human Rights Protection:** Central focus on ensuring AI systems respect fundamental rights, with international treaty commitment reinforcing domestic protections.
- **Responsible AI Development:** Emphasis on safe, ethical AI use benefiting all sectors of society.
- **Inclusive Growth:** Leveraging AI for economic development that benefits all population segments.
- **Public Service Improvement:** AI-enabled enhancement of government services through digital transformation.
- **Sustainable Development:** Aligning AI with environmental sustainability goals.
- **International Alignment:** Strong commitment to OECD AI Principles, UNESCO recommendations, and Council of Europe standards.
- **Multi-Stakeholder Collaboration:** Engaging government, private sector, academia, and civil society in AI governance.
- **Risk Management:** Explicit acknowledgment and management of AI risks to society, democracy, and human rights.
- **Data Governance Integration:** Coordination between AI and data strategies, including personal data protection.

Governance Structure

Uruguay's AI governance operates through a coordinated institutional framework:

- **AGESIC:** The Agency for Electronic Government and Information Society serves as the primary coordinating body for AI strategy development, implementation oversight, and recommendations.
- **Strategic Committee of the Public Sector for AI and Data:** Established under Article 74 of Law No. 20.212, this apex governance body approves major AI policy initiatives and monitors implementation progress.
- **Personal Data Regulatory and Control Unit (URCDP):** Collaborates with AGESIC on data protection aspects of AI systems, ensuring compliance with Law No. 18.331.
- **International Engagement:** Uruguay participates in Council of Europe AI Convention governance and regional initiatives like fAIrLAC.

Implementation Status

Uruguay has made significant progress in implementing its AI governance framework. Article 74 of Law No. 20.212 established the legal mandate in November 2023. AGESIC submitted regulatory recommendations to the legislature within the 180-day deadline. The National AI Strategy 2024-2030 was approved by the Strategic Committee on November 21, 2024, following development with technical support from CAF and UNESCO. The National Data Strategy 2030 was published on December 26, 2024, complementing AI governance with data governance foundations. Uruguay's signature of the Council of Europe AI Convention in September 2024 demonstrates international commitment. Comprehensive AI regulation with specific enforcement mechanisms is anticipated in 2025.

Future Developments

Uruguay's AI regulatory landscape continues to evolve with several key developments anticipated:

- **Comprehensive AI Regulation (2025):** AGESIC's regulatory recommendations are expected to inform new legislation establishing specific AI requirements and enforcement mechanisms.
- **Council of Europe Convention Ratification:** Following signature, Uruguay is expected to pursue ratification through domestic constitutional processes.
- **Strategy Implementation:** Full implementation of the National AI Strategy 2024-2030 across all 12 lines of action and 3 pillars.
- **Data Strategy Implementation:** Continued rollout of National Data Strategy 2030 supporting AI governance.
- **Regional Leadership:** Continued engagement in regional AI initiatives and potential influence on other Latin American countries' approaches.

International Context

Uruguay demonstrates exceptional international alignment in AI governance. The country's signature of the [Council of Europe Framework Convention on AI](#) as the first Latin American nation positions it as a regional pioneer. Uruguay adheres to [OECD AI Principles](#) and UNESCO's Recommendation on Ethics of AI. The National AI Strategy was developed with technical support from [CAF](#) and [UNESCO](#), ensuring international best practice integration. Uruguay participates in the [fAIrLAC network](#) coordinated by the Inter-American Development Bank for responsible AI in Latin America. The country's approach serves as a model for other Latin American nations developing AI governance frameworks.

Uzbekistan — AI Regulatory Landscape Summary

Overview

Uzbekistan is rapidly emerging as a leader in AI governance within Central Asia, developing a comprehensive regulatory framework that balances innovation promotion with citizen protection. The country's approach is anchored by the [Strategy for the Development of Artificial Intelligence Technologies until 2030](#), approved in October 2024, and the [Draft Law on Artificial Intelligence](#), which passed its first parliamentary reading in April 2025. These instruments reflect Uzbekistan's commitment to positioning itself as a regional AI hub while establishing appropriate safeguards against misuse.

Regulatory Instruments

- [Strategy for the Development of Artificial Intelligence Technologies until 2030](#) - Presidential strategy establishing the legal, technological, and economic foundations for AI adoption across all sectors, with ambitious targets including \$1.5 billion in AI-based services revenue by 2030.
- [Draft Law on Artificial Intelligence](#) - Comprehensive legislation introducing mandatory AI content labeling, personal data protection requirements, prohibition of rights-violating AI systems, and requirements for human oversight in consequential decisions.

Key Themes and Priorities

- **Economic Development:** Targeting \$1.5 billion in AI-based services and establishing 10 AI research laboratories by 2030.
- **Fundamental Rights Protection:** Explicit prohibition of AI systems that violate rights to life, health, freedom, and dignity.
- **Transparency and Labeling:** Mandatory labeling of all AI-generated content with uploader accountability.
- **Human Oversight:** Requirement that decisions affecting citizens' rights cannot rely solely on AI conclusions.
- **Personal Data Protection:** Administrative liability for unlawful AI-based processing and distribution of personal data.
- **Sectoral Implementation:** Priority deployment in banking, healthcare, agriculture, energy, taxation, and public services.
- **International Alignment:** Commitment to aligning with OECD AI Principles and international best practices.
- **Digital Transformation:** Integration with the broader Digital Uzbekistan 2030 national initiative.

Governance Structure

- [Ministry of Digital Technologies](#): Lead implementing agency responsible for strategy execution, policy coordination, and technical monitoring of AI governance.
- **Center for Development of Artificial Intelligence and Digital Economy**: Coordinates AI research, development, and deployment activities under Ministry oversight.
- **Coordination Commission for Digital Uzbekistan 2030**: Provides high-level oversight and monitors implementation progress across government agencies.

- **[Oliy Majlis \(Parliament\)](#)**: Legislative authority responsible for enacting AI legislation and overseeing law implementation.
- **Reconstruction and Development Fund**: Provides financial support through a \$50 million interest-free loan facility for AI development.

Implementation Status

Uzbekistan's AI regulatory framework is in active development. The Strategy for AI Development is fully in force since October 2024, with implementation milestones underway. The priority projects list was due by December 1, 2024. The Big Data database is scheduled to become operational by May 1, 2025, with high-performance computing infrastructure launching by May 1, 2026. The Draft AI Law passed its first reading in April 2025 with 150 votes in favor and is proceeding through the legislative process, with full entry into force anticipated in 2026 following development of implementing regulations for labeling procedures and compliance requirements.

Future Developments

Uzbekistan's AI governance landscape will continue evolving with several key developments expected. The Draft AI Law will undergo second and third readings before final passage, followed by development of detailed implementing regulations specifying AI content labeling procedures. Sector-specific guidelines for AI deployment in healthcare, finance, and other priority areas are anticipated. The country aims to achieve a top 50 ranking in the Government AI Readiness Index, up from its current 70th position. Continued investment in AI research infrastructure and workforce development will support the 2030 revenue targets. Enhanced international cooperation and standards harmonization efforts are planned to position Uzbekistan as a regional AI hub.

International Context

Uzbekistan's AI regulatory approach reflects alignment with international standards while addressing domestic priorities. The strategy explicitly references the [OECD AI Principles](#) as a foundation for ethical AI development. The Draft AI Law's mandatory labeling requirements mirror provisions emerging under the [EU AI Act](#), while the prohibition on rights-violating AI systems aligns with UNESCO recommendations. Uzbekistan participates in regional AI cooperation initiatives within Central Asia and broader international frameworks. The country's integration of AI oversight into existing regulatory structures rather than creating new specialized agencies follows models adopted by many jurisdictions during early phases of AI regulation. The ambitious Government AI Readiness Index targets demonstrate commitment to achieving international recognition for AI governance maturity.

Vietnam — AI Regulatory Landscape Summary

Overview

Vietnam has established one of the most comprehensive and ambitious AI regulatory frameworks in Southeast Asia, positioning itself as a global pioneer by becoming the first country to enact a standalone law exclusively for the digital technology industry. The Vietnamese approach combines strategic vision from the Communist Party's highest leadership with binding legal requirements, reflecting the nation's commitment to becoming a regional technology hub while ensuring responsible AI development. With five complementary instruments spanning Politburo resolutions to enforceable legislation, Vietnam targets achieving top 4 status in ASEAN and top 50 globally in AI by 2030. The framework emphasizes human-centric AI principles, risk-based classification similar to the EU AI Act, and innovation-enabling governance that explicitly rejects overly restrictive regulatory approaches.

Regulatory Instruments

- [Resolution on Breakthrough Development of Science, Technology, Innovation and National Digital Transformation](#) - The Politburo's landmark December 2024 resolution establishing Vietnam's strategic vision for technology leadership, targeting 2% GDP R&D investment by 2030 and 50% digital economy contribution by 2045.
- [Law on Digital Technology Industry](#) - The world's first standalone law for digital technology industry, enacted June 2025, adopting EU-style risk-based AI classification with binding requirements effective January 2026.
- [National Strategy on Research, Development and Application of Artificial Intelligence to 2030](#) - Comprehensive 2021 roadmap for AI ecosystem development, workforce building, and sectoral deployment across healthcare, education, finance, and public administration.
- [Principles on Research and Development of Responsible AI Systems](#) - June 2024 voluntary ethical framework establishing nine fundamental principles: cooperation, transparency, controllability, safety, security, privacy, human rights, user support, and accountability.
- [Cybersecurity Law](#) - Foundational 2018 legislation requiring data localization (minimum 24 months local storage), security standards, and authority cooperation for online services including AI systems.

Key Themes and Priorities

- **Innovation-Enabling Governance:** Resolution 57 explicitly mandates eliminating the "if you can't stop it, then ban it" mindset, prioritizing regulatory approaches that enable innovation while managing risks.
- **Human-Centric AI Development:** All instruments emphasize AI systems must be ethical, transparent, explainable, and under human control with accountability throughout the lifecycle.
- **Risk-Based Classification:** The Law on Digital Technology Industry adopts EU AI Act-style categorization of high-risk and high-impact AI systems with corresponding compliance requirements.
- **Strategic Technology Investment:** Aggressive targets for R&D investment (2% GDP), national AI innovation centers, and special mechanisms to attract global talent and investment.
- **Data Sovereignty:** Strong data localization requirements ensuring government access to data powering AI systems operating in Vietnam.
- **International Competitiveness:** Clear benchmarks targeting top 4 ASEAN and top 50 global rankings in AI development and innovation.

- **Sectoral Application:** Prioritized AI deployment across healthcare, education, finance, public administration, and national defense.

Governance Structure

- **Ministry of Science and Technology (MOST):** Lead agency for AI research and development standards, implementation of Responsible AI Principles, and coordination of National AI Strategy.
- **Ministry of Information and Communications (MIC):** Primary authority for digital transformation initiatives, Law on Digital Technology Industry implementation, and telecommunications infrastructure.
- **Ministry of Public Security (MPS):** Enforcement authority for Cybersecurity Law, data localization compliance, and cybersecurity incident response.
- **Ministry of National Defense:** Oversees AI applications in defense and national security contexts.
- **Provincial People's Committees:** Responsible for local implementation of digital transformation and AI development initiatives.

Implementation Status

Vietnam's AI regulatory framework is transitioning from strategic and voluntary guidance to binding legal requirements. The Cybersecurity Law (2018) is fully operational with data localization provisions enforced through Decrees 53/2022 and 13/2023. The National AI Strategy (2021) is in Phase 1 implementation building foundational infrastructure and workforce. The Responsible AI Principles (June 2024) are in effect as voluntary guidance with growing adoption. Resolution 57-NQ/TW (December 2024) is being implemented across Party organs and government agencies. The Law on Digital Technology Industry was enacted June 2025 and will take full effect January 1, 2026, with implementing decrees due within 12 months. Businesses currently have a transition period to assess AI system compliance with the forthcoming binding requirements.

Future Developments

Vietnam's AI regulatory landscape continues evolving with several significant developments expected. A dedicated AI Law is being developed to provide more detailed AI-specific regulations beyond the Digital Technology Law's framework, potentially by end of 2025. The [Law on Data \(No. 60/2024/QH15\)](#) takes effect July 1, 2025, introducing "digital data," "important data," and "core data" concepts with new governance requirements. Implementing decrees for the Law on Digital Technology Industry will detail high-risk AI system requirements, conformity assessment procedures, and sector-specific obligations. The government is establishing regulatory sandboxes to enable controlled testing of innovative AI products. Provincial digital transformation plans are being developed to implement national objectives at local levels. International cooperation agreements on AI development with advanced technology partners are expanding.

International Context

Vietnam's AI governance approach represents a unique hybrid model combining elements from multiple international frameworks. The [Law on Digital Technology Industry](#) explicitly aligns its AI definition and risk-based classification with [OECD AI Principles](#) and the [EU AI Act](#) framework, facilitating interoperability with European regulatory standards. Human-centric principles mirror [UNESCO's Recommendation on AI Ethics](#). However, the data localization requirements and government oversight emphasis reflect approaches similar to China's Cybersecurity Law model, prioritizing state sovereignty over data flows. Vietnam participates in ASEAN digital cooperation frameworks including the ASEAN Guide on AI Governance and Ethics while maintaining national

regulatory authority. This balanced approach positions Vietnam to engage with both Western and Asian technology partners while developing domestic AI capabilities under sovereign governance structures.

About This Report

This report has been generated using Regulations.AI, a public information platform developed and operated by Smitteck GmbH, Switzerland. The platform aggregates, summarizes, and structures publicly available laws, policies, and regulatory developments related to artificial intelligence across jurisdictions.

Purpose and Intended Use

The content of this report is provided for informational and educational purposes only. It is intended to support general understanding, comparison, and high-level analysis of AI-related regulatory developments worldwide. The report does not constitute legal advice, regulatory guidance, or compliance recommendations and should not be relied upon as a substitute for advice from qualified legal or regulatory professionals.

Methodology and Sources

The report is based on summaries and references derived from publicly accessible regulatory texts, official government publications, and related policy materials. While care is taken to reflect the substance of relevant laws and initiatives, regulatory environments evolve rapidly and interpretations may vary across jurisdictions.

Readers are encouraged to consult original legislative texts, official government sources, or professional advisors when accuracy, completeness, or legal interpretation is critical.

Accuracy and Limitations

Although reasonable efforts are made to ensure accuracy and timeliness, no guarantee is given that the information contained in this report is complete, current, or free from errors. Limitations may arise due to:

- subsequent legal or policy changes after publication,
- differences in translation or legal interpretation,
- incomplete or unavailable source material.

Smitteck GmbH assumes no responsibility for decisions, actions, or outcomes resulting from reliance on this report.

No Professional Relationship

Use of this report does not create any advisory, legal, fiduciary, or client relationship with Smitteck GmbH or its contributors. Any communications or feedback related to the report should be considered non-confidential unless explicitly agreed otherwise.

Intellectual Property and Use

The structure, compilation, and original summaries contained in this report are protected under Swiss and international intellectual property laws. Brief quotations or references are permitted with appropriate attribution to Regulations.AI. Systematic reproduction, redistribution, scraping, or commercial reuse of the content requires prior written permission from Smitteck GmbH.

Third-Party References

This report may reference or link to third-party sources for contextual or informational purposes. Such references do not imply endorsement, and Smitteck GmbH does not assume responsibility for the accuracy, availability, or content of external materials.

Governing Law

This report and its use are governed by the laws of Switzerland, with jurisdiction vested exclusively in the courts of Zurich, Canton of Zurich.