

Implementing the EU AI ACT at the national level: models and perspectives

Di Luca Mezzetti

Abstract: The essay analyzes the various models adopted by European Union Member States for the implementation of the EU AI Act, highlighting how the regulation is deeply impacting national systems at the regulatory, organizational, and institutional levels. Through a comparative review of national experiences, the author distinguishes between those states that have already adopted a comprehensive implementing law, those that rely on sector-specific legislation or regulatory acts, those still in the legislative development phase, and those without specific implementing measures. Particular attention is paid to defining the governance structures required by the European regulation, with regard to market surveillance authorities, notification authorities, and bodies responsible for the protection of fundamental rights. The analysis highlights national models characterized by a strong role of independent authorities and specialized agencies. The implementation of the AI Act represents not only a process of regulatory compliance, but also a deep transformation of forms of public governance, destined to redefine the relationship between technological innovation, the protection of fundamental rights, and public powers in European legal systems.

1999

1. Introduction. The impact of the EU AI Act on the regulatory and organizational systems of the Member States. Which models?

The EU AI Act entered into force on 1 August 2024 pursuant to Article 113. Accordingly, the regulation will become fully applicable on 2 August 2026, namely twenty-four months after its entry into force¹.

The implementation and enforcement of the EU AI Act impose numerous new obligations at the national level, many of which are subject to particularly demanding timelines. Overall, 88 responsibilities for Member States can be identified: 18 measures aimed at establishing an AI governance framework, to be implemented between 2 November 2024 and 2 August 2026; 7 measures concerning either the adoption of new national legislation or secondary legislation that Member States may enact or through which they may assist the Commission, some subject to explicit deadlines and others left to national discretion; 55 categories of enforcement-related activities at national level, several of which must already commence from 2

¹ M. Finck, *The EU Artificial Intelligence Act*, Oxford, , 2026; G. Cerrina Feroni, S. Orlando, G. Vettori (cur.), *Il regolamento europeo sull'intelligenza artificiale. Problemi e sistema*, Bologna, 2026; U. Ruffolo (cur.), *AI Act. La regolamentazione europea dell'Intelligenza artificiale*, Rome, 2025.

February 2025 onwards; and 8 tasks relating to the ex-post evaluation of the AI Act, to be carried out between 2025 and at least 2031.

Nevertheless, the AI Act establishes three specific transitional periods for certain categories of provisions. Six months after the entry into force of the AI Act, namely on 2 February 2025, Chapter I (Articles 1–4, concerning introductory provisions) and Chapter II (Article 5, concerning prohibited practices) become applicable. Twelve months after the entry into force, namely on 2 August 2025, Chapter III (Articles 28–39 on notified bodies), Chapter V (Articles 51–56 on GPAI models), Chapter VII (Articles 64–70 on governance), Article 78 on confidentiality, and Articles 99–100 concerning penalties become applicable. Finally, thirty-six months after the entry into force, namely on 2 August 2027, Article 6(1), Annex I, and the related obligations become applicable.

Article 111 establishes specific transitional arrangements for AI systems and GPAI models that had already been placed on the market or put into service prior to the entry into force of the AI Act. Three distinct scenarios are envisaged. First, AI systems forming part of large-scale IT systems listed in Annex X and placed on the market or put into service before 2 August 2027 must comply with the AI Act by 31 December 2030. Second, all other high-risk AI systems placed on the market or put into service before 2 August 2026 are required to comply with the AI Act only once they undergo significant design modifications. However, where the provider or deployer of such a high-risk AI system is a public authority, compliance with the AI Act becomes mandatory by 2 August 2030. Third, GPAI models placed on the market or put into service before 2 August 2025 must comply with the AI Act by 2 August 2027².

On 7 May 2026, the European Parliament and the Council of the European Union reached a provisional agreement on the Digital Omnibus on AI (the “AI Omnibus”), a package of targeted amendments to the EU AI Act. Although the agreement has not yet been formally adopted, it provides greater legal certainty for businesses by indicating, inter alia, that key enforcement deadlines concerning certain rules applicable to high-risk AI systems will be postponed. The AI Omnibus forms part of a broader Digital Omnibus legislative initiative published by the European Commission on 19 November 2025, which seeks to simplify the EU digital regulatory framework. In addition to the EU AI Act, the broader package proposes amendments to several other legislative instruments, including the GDPR, the ePrivacy Directive, the NIS2 Directive, and the Data Act.

The provisional agreement introduces a fixed timeline for the deferred application of the majority of the rules governing high-risk AI systems. Specifically, these rules will apply from 2 December 2027 for stand-alone high-risk AI systems, namely systems deployed in the high-risk sectors identified in Annex III of the EU AI Act, and from 2 August 2028 for high-risk AI systems used as safety components of products or otherwise regulated under EU product safety harmonisation legislation. The postponement is intended to ensure that technical standards and other supporting instruments, many of which remain delayed, can be adequately developed before the relevant obligations become enforceable.

² G. Malgieri et al. (cur.), *The EU Artificial Intelligence Act*, London, 2026.

Furthermore, the provisional agreement expands the list of prohibited AI practices by prohibiting AI systems that generate child sexual abuse material (CSAM) or depict, without consent, the intimate parts of an identifiable person or an identifiable person engaged in sexually explicit conduct. The prohibition applies to images, video, and audio content, with compliance required by 2 December 2026.

Additional amendments have also been announced. These include postponing the application of watermarking obligations for AI-generated content until 2 December 2026; clarifying the concept of “safety component,” such that AI systems intended merely to assist users or optimise performance will not automatically qualify as high-risk where their failure or malfunction does not pose risks to health or safety; and addressing overlaps between the EU AI Act and sector-specific legislation, such as rules governing medical devices, toys, lifts, and machinery. In this regard, the agreement clarifies that machinery products are required to comply only with sectoral safety legislation rather than simultaneously with both the AI Act and sector-specific rules, and it also permits the limitation of the AI Act’s application in circumstances where sectoral legislation already contains equivalent AI-related requirements, through the adoption of implementing acts. Moreover, the agreement reinstates the obligation for providers to register AI systems in the EU database for high-risk AI systems where providers consider those systems exempt from high-risk classification pursuant to Article 6(3) of the EU AI Act.

The provisional agreement must now be formally adopted by both the European Parliament and the Council. Formal adoption is expected before 2 August 2026, the date on which the current rules concerning high-risk AI systems would otherwise become applicable. Once adopted, the amendments will be published in the Official Journal of the European Union and will enter into force three days thereafter.

The regulatory implementation models adopted by the various legal systems of the European Union Member States will be analyzed according to a taxonomy of decreasing intensity, structured on the basis of the parameters offered by the adoption by national legal systems of a) a comprehensive implementing law of the EU AI Act, b) partial or sectoral implementing laws, c) implementing acts classifiable as statutory instruments (government regulations, ministerial decrees), d) a comprehensive implementing bill or proposal, or e) the absence of primary or secondary implementing legislation³.

It is also worth emphasizing that in all legal systems, regardless of the specific solution adopted within the various experiences regarding the adoption of strictly regulatory acts adapting the domestic legal system to the EU legal system, plans, programs, guidelines, etc., can be found, under various formal names (soft law) that complements laws, regulations, and ministerial decrees, defining their technical profiles according to quantitative and qualitative criteria of enormous specific weight given the specific nature and peculiarities of the subject matter they cover⁴.

³ OECD, *Progress in Implementing the European Union Coordinated Plan on Artificial Intelligence*, vol. 1, 2025, vol. 2, 2026.

⁴ J. Pötsch, R. Bernnat, *Regulierung von Künstlicher Intelligenz in der EU*, Berlin, 2025.

2. Jurisdictions equipped with an implementing law of the EU AI Act (Denmark, Hungary, Luxembourg, the Netherlands, Slovenia, Italy)

a) Implementing the EU Act in Denmark is the Act on Supplementary Provisions to the Regulation on Artificial Intelligence (*Lov nr. 467 af 14. maj 2025*), the national implementing act that designates *Digitaliseringsstyrelsen* as the central contact point and market surveillance authority, and confers enforcement powers, including the ability to conduct inspections and issue fines. In January 2024 *Digitaliseringsstyrelsen* (the Danish Agency for Digital Government) published short, practical guides for public authorities and private companies on responsible use of generative AI. The documents set out management responsibilities, three-step implementation advice (approach, rules, organisational arrangements), data- and security-related cautions, and recommendations for ongoing updates and risk-based oversight.

The Digital Taskforce for Artificial Intelligence is a cross-governmental, joint-public-sector framework (*Regeringen, KL, Danske Regioner*), created in 2024 to accelerate responsible large-scale deployment of AI across Denmark's public sector. It sets strategic objectives, identifies legal and technical barriers (including GDPR and the EU AI Act), runs pilots, and reports regularly to ministers and stakeholders.

The Strategic Approach for Artificial Intelligence (*Strategisk indsats for kunstig intelligens*) has been published by the Danish Ministry of Digitalisation on 2 December 2024, this strategic approach sets out three guiding principles and four concrete initiatives to accelerate responsible AI development and deployment in Denmark. Key measures include a Digital Taskforce for public-sector roll-out, a new advisory center for responsible AI, a secure platform for Danish language models, and opening Danish text data to spur domestic model development.

Furthermore, the Danish Data Protection Act (*Databeskyttelsesloven*) supplements the GDPR and provides the legal basis for Datatilsynet's oversight of personal data processing within AI systems, including specific provisions for research and public-sector data use. Finally, the Public Administration Act (*Forvaltningsloven*), while technology-neutral, remains critical as it governs how public authorities must ensure transparency, reasoning, and fairness when using automated systems to make decisions affecting citizens. Together, these laws create a comprehensive legal environment that addresses both the technical safety of AI products and the legal rights of the individuals affected by their use.

b) The Hungarian AI legal framework is built upon several foundational instruments that bridge EU requirements with national administrative procedures. The primary legislative act is Act LXXV of 2025 on the domestic implementation of the EU AI Regulation, which establishes the institutional architecture for AI oversight in Hungary. It designates national authorities, defines jurisdictional reach, and sets the legal basis for market surveillance. Complementing this is Government Decree 344/2025, which provides the operational details for the National Accreditation

Authority (NAH) and the Minister for Enterprise Development, specifying the procedures for designating conformity-assessment bodies.

Government Decree 344/2025 (X.31.) implements the domestic procedural and institutional arrangements necessary to apply the EU Artificial Intelligence Regulation ((EU) 2024/1689) in Hungary under Act LXXV of 2025. The Decree designates the *Nemzeti Akkreditáló Hatóság* as the national notifying authority and the minister responsible for enterprise development as the national market surveillance authority and single point of contact; it establishes reporting duties, designation procedures for conformity-assessment organizations, market surveillance powers and sanctioning rules.

The Government Resolution 1406/2025. (XI. 4.) titled "*A mesterséges intelligencia hazai stratégiai megerősítését és kiemelt fejlesztési területeit szolgáló intézkedésekről*" (adopted 4 November 2025) establishes an administrative and strategic package to accelerate Hungary's national artificial intelligence (AI) strategy. The text mandates appointment of AI focal points in ministries and regional government offices, directs the government AI commissioner to prepare an execution framework for the national AI strategy, and instructs several ministries to prepare sectoral plans (notably for healthcare and public administration rollout).

The Government Resolution 1405/2025 (XI. 4.) titled "On measures to increase social awareness of artificial intelligence" is a programmatic *kormányhatározat* adopted on 4 November 2025. It directs multiple ministries and the Government Commissioner for Artificial Intelligence to design, coordinate and launch a series of educational, evaluative and institutional measures to broaden AI awareness and capabilities in Hungary. The resolution complements Hungary's national AI strategy and a cluster of AI-related government decisions issued in November 2025, and establishes concrete deadlines for planning and implementation through 2026.

The Government Resolution 1404/2025 (XI. 4.) — "On measures promoting international cooperation supporting AI development" — establishes a short, targeted set of ministerial instructions to integrate artificial intelligence into Hungary's external policies, foster cooperation with selected partner countries, and evaluate the national environment for attracting AI and data-centre investments. The Resolution was adopted on 4 November 2025 : it assigns lead responsibilities primarily to the Ministry of Foreign Affairs and Trade, jointly with the Ministry of National Economy and the minister responsible for culture and innovation, and directs cooperation with the HIPA investment promotion agency for a specific FDI suitability review to be completed by 31 December 2025.

The National Artificial Intelligence Strategy 2025–2030 serves as the overarching policy document, outlining six pillars of development including infrastructure, education, and the data economy.

c) Luxembourg's AI regulatory landscape is shaped by a combination of national policies and direct implementation of European Union legislation. The key instruments include the Law of 20 December 2024 on implementing rules and penalties related to the EU Artificial Intelligence Act, crucial for transposing the provisions of the EU AI Act (Regulation (EU) 2024/1689) into Luxembourgish law. It designates national competent

authorities, establishes administrative sanctions mirroring EU ceilings, and adapts existing national laws to enable effective enforcement of the AI Act. The law identifies the *Commission nationale pour la protection des données (CNPD)* as the general reference authority and single point of contact for AI Act matters.

The National Artificial Intelligence Strategy (part of 'Accelerating Digital Sovereignty 2030'), adopted in 2025, is a comprehensive policy that defines Luxembourg's vision to become a responsible European hub for AI. It outlines a human-centric approach, focusing on digital sovereignty, fundamental rights, and socio-economic value. The strategy sets out six transversal enablers (talent, infrastructure, service ecosystem, research, governance, international collaboration) and identifies high-impact sectors for AI deployment; the National Data Strategy (aligned with the national AI and quantum strategies — 'Accelerating Digital Sovereignty 2030'), also adopted in 2025, is a strategy that treats data as a strategic national asset, aiming to position Luxembourg as a European center of excellence for data. It outlines a framework for data governance, talent development, secure processing environments, and interoperable services, with a strong emphasis on GDPR compliance and participation in European data spaces; the Artificial Intelligence: A Strategic Vision for Luxembourg, published in 2019, is a foundational paper which outlined Luxembourg's initial human-centric approach to AI. It identified three overarching ambitions: digital leadership, a data-driven sustainable economy, and human-centric AI development, organizing recommendations around focus areas like living laboratories, data as a cornerstone, ethics, investments, public sector AI, skills, and international cooperation.

d) In the Netherlands, to operationalize the EU Act at the national level, the National AI Implementing Act (*Uitvoeringswet AI-verordening*) was enacted. This act is crucial as it designates the Dutch Data Protection Authority (AP) and the Digital Infrastructure Inspectorate (RDI) as the primary oversight bodies, granting them the necessary legal powers to conduct inspections, access source code, and impose sanctions. It also establishes the legal framework for the National Algorithm Register, making it a statutory requirement for government entities to list their impactful algorithmic systems, thereby ensuring public transparency.

In addition to AI-specific laws, the General Data Protection Regulation (AVG/GDPR) remains a cornerstone of the Dutch framework. The Dutch Implementation Act (UAVG) provides specific local nuances, particularly regarding the processing of sensitive data and the rights of individuals to contest automated decisions under Article 22. The *Implementatiekader Verantwoorde inzet van algoritmen* (Implementation Framework for Responsible Use of Algorithms), 2023, further bridges the gap between high-level law and daily administrative practice, providing civil servants with concrete steps for risk management and human oversight.

Finally, the Government-wide Vision on Generative AI (2024) provides the strategic direction for the use of large language models, emphasizing that while generative AI offers immense potential for productivity, its use in the public sector must be governed by principles of accuracy, non-discrimination, and intellectual property respect. These laws

and policies together create a comprehensive net that catches risks at the technical, legal, and ethical levels.

e) The legislative landscape in Slovenia is dominated by the Act on the Implementation of the (EU) Regulation on Harmonised Rules on Artificial Intelligence (ZIUDHPUI), which was passed in 2025 to provide the domestic legal basis for the EU AI Act. This act is comprehensive, detailing the specific powers of the Ministry for Digital Transformation and other market surveillance authorities. It also establishes the procedural rules for notifying bodies—the organizations responsible for assessing the conformity of high-risk AI systems.

Beyond this primary act, the *Digitalna Slovenija 2030* (Digital Slovenia 2030) strategy (2023) serves as the overarching policy framework, aligning national digital goals with the EU's Digital Decade targets. This strategy is not merely a vision document; it sets specific KPIs for AI adoption in the public sector and the economy.

The National Programme for the Promotion of the Development and Use of Artificial Intelligence (NpUI), adopted in 2021, remains a foundational document, focusing on ten strategic goals including research excellence, education, and the ethical deployment of AI in priority sectors.

Additionally, the Strategy for the Digital Transformation of the Economy (2022) provides a roadmap for increasing the adoption of advanced technologies, including AI, IoT, and big data, specifically within the Slovenian business sector.

Finally, the Personal Data Protection Act (ZVOP-2) supplements the GDPR at the national level, providing the necessary privacy protection for data-intensive AI systems. Together, these laws and strategies create a multi-tiered legal environment that addresses everything from high-level ethical principles to granular technical compliance requirements for specific AI applications.

f) The Italian legislative framework for AI is a composite of primary laws, delegated decrees, and strategic policy documents⁵.

The *Legge 23 settembre 2025, n. 132* (National Law on AI) is the primary legislative act establishing the national governance architecture, designating AgID and ACN as authorities, and introducing criminal penalties for AI misuse. It provides the legal basis for the entire national AI ecosystem.

The Agency for Digital Italy, established by Law No. 134 of August 7, 2012, plays a central role in regulating and promoting artificial intelligence: it contributes to the definition of the national strategy, collaborating with other agencies and institutions, promotes the adoption of AI in public administration, ensures ethical and safe use, and facilitates collaboration between the public and private sectors, promoting innovation and the development of digital ecosystems based on this technology. In particular, AgID supports the Coordination Committee for updating the national strategy through the Technical Secretariat established within the

⁵ V. Franceschelli, A. Sirotti Gaudenzi, *La legge italiana sull'Intelligenza Artificiale*, Rimini, 2025; F. Donati et al. (cur.), *La disciplina dell'intelligenza artificiale*, Milan, 2025; R. D'Angiolella, *Legge 23 settembre 2025, n. 132. La tutela della persona nella regolazione dell'Intelligenza Artificiale*, Naples, 2025.

Agency. In fact, together with the Department for Digital Transformation, AgID has updated the Italian Strategy for Artificial Intelligence, publishing the 2024-2026 edition. The document analyzes the global context and Italy's positioning and defines strategic actions grouped into four macro-areas: research, public administration, business, and training. These areas are linked by several important and specific cross-cutting actions. The strategy also includes a monitoring system and an analysis of the regulatory context that defines the framework within which it will be deployed. The field of artificial intelligence is also addressed in the 2024-2026 edition of the Three-Year Plan, which in Chapter 5 provides operational guidelines for the adoption of AI in Public Administration, providing examples, best practices, and a practical handbook containing practical guidelines for the use of Artificial Intelligence in public administration.

The National Cybersecurity Agency (ACN) was established by Legislative Decree No. 82 of June 14, 2021, and redefined the national cybersecurity architecture, with the aim of rationalizing and simplifying the existing system of national competencies, further enhancing cybersecurity and resilience, including for the purposes of protecting national security in cyberspace. The Agency is the national cybersecurity authority for the protection of national interests in the field of cybersecurity and is responsible for safeguarding security and resilience in cyberspace. It is responsible for preventing and mitigating the greatest possible number of cyber attacks and promoting the achievement of technological autonomy. Among the Agency's main tasks is the implementation of the National Cybersecurity Strategy, adopted by the Prime Minister, which contains the objectives to be achieved by 2026.

The *Piano Triennale per l'Informatica nella PA 2024-2026* defines a strategic roadmap for digital transformation that integrates AI adoption standards for all Italian public bodies. It focuses on interoperability and the use of the National Data Platform.

The Digital Administration Code (CAD) is a consolidated text that brings together and organizes the rules regarding the digitalization of Public Administration in its relations with citizens and businesses. Established by Legislative Decree No. 82 of March 7, 2005, it was subsequently amended and supplemented first by Legislative Decree No. 179 of August 22, 2016, and then by Legislative Decree No. 217 of December 13, 2017, to promote and implement digital citizenship rights.

The *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026* is the Italian government's programmatic framework for the digital transformation of the public sector. Approved and published in February 2024, with subsequent updates in 2025 and 2026, it establishes strategic principles ("digital & mobile first", "cloud first", "API-first/interoperability", "digital identity only", "once-only" and "data protection by design") and operational lines for central, regional and local administrations. The document unites high-level direction and granular instruments: it presents strategic components (governance, organisation, skills), technological components (services, platforms, data & AI, infrastructures, security), and a new "tools" section that supplies templates, checklists and case studies to support implementation.

The *Strategia Italiana per l'Intelligenza Artificiale 2024-2026* (2024) contains the national policy document outlining investment priorities in research, training, and industrial adoption. It emphasizes the development of 'Italian' AI models trained on national cultural and linguistic data.

Italia Digitale 2026 is Italy's national digital strategy embedded in the national recovery plan (*PNRR / "Italia Domani"*) and defined in March 2021. It establishes five measurable national targets to be achieved by 2026: 70% digital identity adoption, 70% basic digital skills, 75% of public administrations migrated to cloud services, 80% of essential public services available online, and full ultra-broadband coverage for households and businesses. The strategy brings together investment, regulatory reforms and institutional realignment to speed digital transformation across infrastructure, public administration, health, education and skills. The central coordination role is played by the *Dipartimento per la trasformazione digitale* (Presidency of the Council) and the Minister for Technological Innovation and Digital Transition, with implementing partners including the Ministry/Dipartimento, AgID, the PA Digitale 2026 portal (PA Digitale 2026) and the national cybersecurity authority (ACN).

With Resolution No. 43/2026, AgID adopted the draft "Guidelines for the Development of Artificial Intelligence Systems in Public Administration" and the "Guidelines for AI Procurement in Public Administration," provided for in the Three-Year Plan for Information Technology in Public Administration 2024-2026. These guidelines were submitted for public consultation from March 12 to April 11, 2026.

These guidelines are provided for in the Three-Year Plan for Information Technology in Public Administration 2024-2026, pursuant to the Prime Ministerial Decree of January 12, 2024, and are issued following the procedural process established by art. 71 of the Digital Administration Code (CAD) pursuant to Legislative Decree no. 82/2005. The latter provides that AgID, following a public consultation to be held within thirty days, having consulted the competent administrations, the Personal Data Protection Authority, and obtained the opinion of the Unified Conference, adopts guidelines containing technical and policy rules, which become effective upon their publication in the dedicated area of AgID's institutional website.

In addition to the aforementioned regulations, reference should be made to Legislative Decree no. 196 of June 30, 2003 (Personal Data Protection Code) and Legislative Decree no. 36 of March 31, 2023 (Public Procurement Code), which regulate the entire life cycle of public contracts with comprehensive legislation, and whose articles Articles 19 and 30 lay down general principles applicable to the use of digital tools, including artificial intelligence systems, in the lifecycle of public contracts, imposing requirements for traceability, algorithmic transparency, and accessibility to the source codes of AI systems used in procurement procedures.

3. Jurisdictions with partial or sectoral implementation laws of the EU AI Act (Latvia, Lithuania, Malta)

a) The legislative landscape in Latvia is anchored by several key instruments that work in concert to regulate the AI lifecycle. The Law on the Latvian Artificial Intelligence Centre (2025) is the foundational act, establishing the Centre as a public foundation with the mandate to coordinate national AI policy, manage the regulatory sandbox, and provide expert opinions to other state agencies. This is complemented by the Law on the Development of Artificial Intelligence (2025), which sets out the broader strategic objectives for the national AI ecosystem, including the promotion of AI literacy and the ethical use of automated systems in public administration.

Older but still relevant documents, such as the Digital Transformation Guidelines 2021–2027 (2021) and the 2020 Informative Report, provide the policy context and long-term vision that continue to guide the interpretation and implementation of these newer, binding statutes. Together, these laws form a comprehensive net that captures both the developmental potential and the inherent risks of AI technology.

b) The legislative backbone of Lithuania's AI framework is comprised of several interconnected acts that bridge European mandates with national administrative law. The most significant are the 2025 amendments which provided the necessary legal infrastructure for the EU AI Act's enforcement. These laws are designed to be dynamic, allowing for future updates as the European AI Office issues new guidelines or delegated acts. The primary legislative instruments include Amendments to the Law on Technology and Innovation (Act No. XV-105), adopted in January 2025, that provides the legal basis for the national AI regulatory sandbox and designates the Innovation Agency as the notifying authority for AI conformity assessment bodies. It also outlines the funding mechanisms for AI research and development; Amendments to the Law on Information Society Services (Act No. XV-106), that designates the Communications Regulatory Authority (RRT) as the national market surveillance authority and the single point of contact for the EU AI Act. It establishes the enforcement mechanism for AI systems placed on the Lithuanian market and defines the powers of inspectors.

The Government of Lithuania initiated an update to the national AI strategy in late 2024 to align national policy with the EU Artificial Intelligence Act and to establish a National AI Governance Forum and supporting institutional arrangements (AI sandbox, state data governance coordination). Key implementing bodies include the Ministry of the Economy and Innovation, the Innovation Agency, the State Data Agency and the Communications Regulatory Authority. Official initiatives and legislative amendments were submitted and progressed through the Seimas in 2024–2025 to operationalize the governance forum and pilot regulatory sandbox.

The national update to Lithuania's AI strategy and the parallel plan to establish a National AI Governance Forum were launched by the Ministry of the Economy and Innovation (EIMIN) in late 2024 to align national policy with the European Union's Artificial Intelligence Act and to stimulate controlled innovation domestically. The update packages strategic objectives (competitiveness, secure public services, language and data resource development) with concrete operational measures: a regulated "AI sandbox" to safely test AI systems, funding for language and SME AI

projects, and strengthened state data governance through the State Data Agency's State Data Lake program.

The Seimas Resolution on the Principles of Use of Artificial Intelligence Technologies in the Public Sector (2024) is a policy document setting out the ethical and administrative principles for state and municipal institutions, emphasizing human oversight, transparency, and non-discrimination in automated decision-making; the Action Plan for the Development of Artificial Intelligence Technologies in Lithuania 2023–2026 defines a strategic roadmap that operationalizes the national AI strategy through specific funding measures, infrastructure development, and institutional capacity building, including the development of Lithuanian-specific datasets.

c) In Malta, the national implementation is driven by several key domestic instruments. Legal Notice 226 of 2025 (*Artificial Intelligence Regulations, 2025*) is the primary national instrument that designates the MDIA as the Notifying Authority and Market Surveillance Authority, establishing national enforcement powers and the AI regulatory sandbox.

Legal Notice 227 of 2025 (*IDPC Designation Regulations*) designates the Information and Data Protection Commissioner as the MSA for specific high-risk AI systems, particularly those used in biometrics, law enforcement, and the administration of justice.

The *Malta Digital Innovation Authority Act* (Cap. 591) provides the enabling legislation that established the MDIA and was amended in 2024 (Act XIX of 2024) to expand its powers to include market surveillance and conformity assessment for AI.

Malta Digital Strategy 2023–2027 defines Malta's national strategic plan for digital transformation, covering broader digital goals, infrastructure, data governance, and skills, with a focus on ethical and trustworthy AI.

Additionally, the Innovative Technology Arrangements and Services Act (Cap. 592), 2019, provides the legal basis for the voluntary certification of AI systems as 'Innovative Technology Arrangements' (ITAs).

Finally, the Data Protection Act (Cap. 586) remains the cornerstone for privacy, governing the processing of personal data by AI systems and providing the enforcement framework for the IDPC.

4. Jurisdictions equipped with implementing statutory instruments (government regulations, ministerial decrees) (Cyprus, Greece, Ireland, Portugal, Romania, Slovakia)

a) In Cyprus, the EU AI Act is supplemented by the *Governance Framework for the Implementation of Regulation (EU) 2024/1689 in Cyprus* (2024), a national legal framework that designates the specific competent authorities, market surveillance bodies, and the notifying authority responsible for AI Act enforcement. These laws are supported by the National Artificial Intelligence Strategy (2020), which remains the foundational policy

document outlining Cyprus's roadmap for investment, ethics, and data infrastructure development.

In addition to AI-specific laws, the regulatory environment is shaped by broader digital legislation. The Digital Strategy for Cyprus 2020-2025 provides the overarching policy framework for integrating AI into the public sector and the national economy. Data processing, which is central to AI development, is governed by Law 125(I)/2018 (*Protection of Natural Persons with regard to the Processing of Personal Data*), which supplements the GDPR. Furthermore, the *eHealth Law* (Law 59(I)/2019) plays a critical role in regulating AI applications within the healthcare sector, ensuring that patient data used in diagnostic algorithms is handled with the highest levels of confidentiality and security. Together, these legislative pieces create a comprehensive legal net that covers the entire lifecycle of an AI system, from data collection and model training to market deployment and post-market monitoring.

b) On 12 November 2024 the Hellenic Ministry of Digital Governance published the national list of authorities and public bodies designated under Article 77 of the EU Artificial Intelligence Act to supervise and enforce obligations protecting fundamental rights in the use of high-risk AI systems. The publication names four existing independent public authorities and confirms that they will obtain AI-Act related powers where necessary and within their statutory jurisdiction. The Ministry announced the list was notified to the European Commission and indicated that the additional competences will take effect from 2 August 2026.

Law 4961/2022 remains the primary horizontal statute on emerging technologies. It mandates Algorithmic Impact Assessments for the public sector and requires registries for AI systems used in profiling or personnel evaluation in the private sector.

Law 4727/2020, known as the *Code on Digital Governance*, provides the overarching legal framework for Greece's digital transition, transposing EU directives on open data and web accessibility, and providing the legal basis for interoperability across the Greek state.

c) In Ireland, the EU Act is supported by *Statutory Instrument No. 366/2025*, which formally designates the various National Competent Authorities (NCAs) and market surveillance authorities.

Other relevant instruments include the Guidelines for the Responsible Use of AI in the Public Service (2025), which set binding standards for government departments, and the NCSC Cyber Security Guidance (2023), which addresses the technical vulnerabilities inherent in generative AI models. Together, these laws create a multi-layered safety net that addresses technical, ethical, and legal risks associated with AI deployment.

The General Scheme of the Regulation of Artificial Intelligence Bill 2026 is Ireland's primary legislative instrument for the domestic implementation of the EU AI Act, establishing a distributed governance model led by the National AI Office and designating 15 sectoral regulators as Market Surveillance Authorities.

Guidelines (2025) for the Responsible Use of AI in the Public Service are a comprehensive non-binding framework produced by the Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation to guide Irish public servants in the ethical, lawful, and safe adoption of AI.

Data Protection Commission Guidance on AI and Large Language Models (2024) has been created as non-binding practical guidance from the DPC to assist organizations in understanding and mitigating data protection risks associated with generative AI systems and LLMs under GDPR.

Interim Guidelines for Use of AI (Public Service) (2024) are a high-level, practical guidance for Irish public service organizations considering AI adoption, procurement, or experimentation, developed as an interim measure while more detailed frameworks are finalized.

d) In Portugal, the *Lei n.º 27/2021* (Charter of Human Rights in the Digital Era) is a pioneering piece of legislation that grants citizens specific rights against algorithmic bias and the right to human intervention in automated processes. This is further supported by *Resolução do Conselho de Ministros n.º 207/2024*, which adopted the *Estratégia Digital Nacional*, setting the strategic goals for AI adoption through 2030. Another critical instrument is *Resolução do Conselho de Ministros n.º 2/2026*, which specifically approved the creation of the 'Amália' national LLM and the preparation of the National AI Agenda, signaling a move toward technological sovereignty.

In the realm of public administration, *Decreto-Lei n.º 49/2024* established the rules for digital public services, mandating that AI systems used by the state must be interoperable and follow the 'Mosaico' architectural model. Finally, *Lei n.º 58/2019* (Data Protection Act) remains the bedrock for AI data processing, ensuring that the training of models complies with the GDPR. Together, these laws create a multi-layered legal environment that balances the need for innovation with the protection of individual and collective rights.

e) In Romania, Draft Law B154/2024 is a national legislative proposal introduced on 19 March 2024 to regulate artificial intelligence in Romania. The bill aims to create a domestic framework covering AI development, deployment, protection, oversight and sanctions; it adopts a risk-based approach and references the European AI regulatory initiative as a background policy driver.

The National Strategy in the field of Artificial Intelligence 2024–2027 (HG 832/2024) (decree) serves as the foundational policy document, setting strategic objectives for research, skills, infrastructure, and governance. This strategy is complemented by Ministerial Order No. 20.484/2023, which established the Romanian Committee for Artificial Intelligence (CRIA) as the central advisory body for AI policy.

The Memorandum approved by the Government on 23 April 2024 establishes a national Coordination Committee for Data, Digital Services and Artificial Intelligence to provide an inter-institutional framework for implementing and interpreting EU rules in a harmonized way across Romania. The initiative is a response to the incoming and existing European regulatory frameworks — notably the EU AI Act, the Data Governance Act,

and the Digital Services/Markets rules — and aims to ensure that national authorities act consistently, share expertise, coordinate market interventions and produce common guidance.

Historically, CSAT Decision No. 148/2022 played a pivotal role by mandating the creation of the Interinstitutional Commission for the National AI Strategy, signaling that AI is a matter of national security. Additionally, Law No. 190/2018, which implements the GDPR in Romania, remains the primary authority for the processing of personal data within AI training and deployment. These laws work in concert to create a regulated environment that seeks to balance the need for innovation with the protection of individual rights and national interests. The government is also considering a 'National Digital Code' to consolidate these various rules into a single, coherent legislative volume, which would further clarify the legal obligations of AI developers and users in the country.

f) In Slovakia⁶, the EU Act is supplemented by the Draft Act on the Organization of Public Administration in the Field of Artificial Intelligence (LP/2025/401). This national act is crucial as it designates the specific domestic bodies responsible for market surveillance and defines the procedural rules for inspections and penalties. It also establishes the legal basis for the national AI registry, where high-risk systems must be documented before deployment in the Slovak market.

Beyond these primary (draft) act, several other pieces of legislation form the broader regulatory ecosystem. The Statute of the Government Plenipotentiary for AI (2025) (decree) provides the legal mandate for high-level coordination and strategic planning. This governance framework aims to enhance policy coordination, streamline digital transformation efforts, and align Slovakia's regulatory approach with EU digital regulations.

The Institutional and Coordination Framework for Digital Transformation (2024) includes key mechanisms such as the Government Council for Digitalization, the Special Task Force for Digital Governance, and an analysis of the feasibility of establishing a Central Authority for Digital Market Oversight.

The Strategy of Digital Transformation of Slovakia 2030 (2019) remains the guiding policy document, setting the long-term goals for a data-driven economy.

The Action Plan for Digital Transformation of Slovakia 2023–2026 (2022) traced an operational roadmap translating the Strategy for Digital Transformation 2030 and related national and EU commitments into time-bound measures, including fostering the development and responsible deployment of artificial intelligence and other cutting-edge technologies.

National Strategy for Digital Skills of the Slovak Republic and Action Plan 2023–2026 (2022) contains a comprehensive, government-adopted policy document designed to coordinate and accelerate the development of digital competences across public administration, education, the labor market, and civil society, emphasizing AI awareness and digital ethics.

⁶ A. Bröstl, *Artificial Intelligence, Law-Making and Law-Application*, in L. Mezzetti (cur.), *Science, Technology and Law*, Bologna, 2025, 85-95.

National Concept of Informatization of Public Administration (NKIVS) 2021–2026 (2021) describes the government-approved strategic framework for digital transformation of public administration, laying out objectives for user-oriented services, data transformation, shared services, cybersecurity, and the establishment and use of AI/RPA for routine tasks.

National Cybersecurity Strategy 2021–2025 (2021) is a national-level policy instrument enhancing the protection of the national cyber space, improving preparedness and incident response, and strengthening international cooperation, which is crucial for the security and resilience of AI systems.

Research and Innovation Strategy for Smart Specialisation of the Slovak Republic 2021–2027 (SK RIS3 2021+) (2021) aligns the national framework of research, development, and innovation investments and policies with EU cohesion policy, identifying "Digital Transformation of Slovakia" as a key priority domain that includes AI.

5. Jurisdictions equipped with a bill or draft law implementing the EU AI Act (Czech Republic, Germany, Finland, Poland, Spain, Sweden)

a) To support the implementation of the AI Act, the Czech government has introduced the *Draft Adaptation Act* (2025), which designates the national authorities responsible for market surveillance and notification. Another critical piece of legislation is the *Act on Cybersecurity* (No. 264/2025 Sb.), which transposes the EU NIS2 Directive into Czech law. This act imposes strict security and risk management obligations on providers of essential and important services, including AI systems used in critical infrastructure such as energy, transport, and healthcare. The National Artificial Intelligence Strategy 2030 (NAIS 2030) serves as the core policy document, defining the strategic direction for AI development in the country. Furthermore, the Implementational Plan of the Digital Czech Program (Action Plan 2025) provides an annual roadmap for the execution of NAIS 2030, mandating risk assessments for public sector AI deployments and allocating funding for AI-related projects. These legislative and policy instruments work together to create a stable and predictable environment for AI innovation while ensuring the protection of public interests and fundamental rights.

b) Germany's AI regulatory landscape is shaped by a combination of directly applicable EU law and national legislative and policy initiatives⁷.

The Draft Act for the Implementation of the EU AI Regulation, 2025, (*Gesetz zur Durchführung der KI-Verordnung - KI-MIG*), is a federal government draft bill (*Referentenentwurf*) to implement the EU AI Act in Germany. It designates national competent authorities (e.g., Bundesnetzagentur, BaFin), establishes a coordination center (KoKIVO),

⁷ D.H. Wendt et al., *Digitalisierung und Recht*, Baden-Baden, 2026; M. Ebers, C. Heinze, B. Steinrötter (cur.), *Künstliche Intelligenz und Robotik*, München, 2026.

and creates provisions for innovation measures and national enforcement procedures.

The BMBF AI Action Plan 2023 (*Aktionsplan Künstliche Intelligenz 2023*) works as a targeted update and operational program by the Federal Ministry of Education and Research to accelerate Germany's AI ecosystem, focusing on strengthening research, infrastructure, human capital, and promoting European and international cooperation.

The German Standardization Roadmap on Artificial Intelligence (2023) is a DIN/DKE strategic framework that identifies priority standardization needs, recommendations and implementation steps to support trustworthy, interoperable and certifiable AI in line with the German government's AI strategy and the EU AI Act. Commissioned by the Federal Ministry for Economic Affairs and Climate Action (BMWK), it catalogs over 100 standardization needs and six high-level recommendations and provides an implementation plan for national and international standardization work.

The Data Strategy of the Federal Government (*Datenstrategie der Bundesregierung*), 2021 provides for a comprehensive, non-binding policy framework to unlock the social and economic value of data in Germany, focusing on data infrastructures, responsible data use, data skills, and public administration as a model user.

The National AI Strategy — Update (*Fortschreibung der KI-Strategie/ National AI Strategy: Update 2020*) is the mid-term revision to the 2018 National AI Strategy, increasing federal financial commitment to AI and sharpening priorities to strengthen Germany's position in AI research, development, and application, while embedding ethical and social considerations.

The Strategy for Artificial Intelligence of the Federal Government (*Strategie Künstliche Intelligenz/ 'AI Made in Germany'*), 2018 depicts the foundational national policy framework defining Germany's strategic objectives for AI research, development, application, and governance, emphasizing excellence, talent, transfer, and ethical principles.

c) To complement the EU ai act, the Finnish government has introduced Government Proposal HE 46/2025 (*Hallituksen esitys*), which provides the necessary national legal framework for the Act's implementation. This proposal clarifies the roles of national authorities, establishes the procedures for market surveillance, and sets out the administrative penalty system. Another critical piece of legislation is the Finnish Data Protection Act (1050/2018), which supplements the GDPR and governs the processing of personal data in AI systems.

In the public sector, the Administrative Procedure Act (434/2003) is increasingly relevant as it contains provisions on automated decision-making, ensuring that citizens' rights to transparency and appeal are protected when public authorities use AI. Additionally, the Act on the Secondary Use of Health and Social Data (552/2019) is a pioneering piece of legislation that enables the use of high-quality Finnish health data for AI research and development, provided that strict security and privacy conditions are met. Together, these laws create a comprehensive, multi-layered legal framework that addresses the technical, ethical, and

administrative aspects of AI. The foundational horizontal regulation establishing a risk-based framework for AI systems across the EU, prohibiting certain practices and imposing strict requirements on high-risk systems.

AuroraAI (2020) was initiated by Finland's Ministry of Finance as a national artificial intelligence program to prepare public administration for a human-centric and ethically sustainable society in the age of AI. The programme published an implementation plan for 2019–2023 and carried out preparatory studies, pilots and reference implementations that demonstrated a life-event oriented service ecosystem enabled by an "AuroraAI Network." For the Ministry of Finance overview and official description see Implementation of the national AuroraAI program (Ministry of Finance). AuroraAI emphasized cross-sector collaboration, user control, privacy safeguards and open models for interoperability while also producing documentation on architecture, ethical guidelines and data protection impact assessment work. The program's coordinated implementation phase concluded by the end of 2022 and subsequent decisions in 2023 led to decommissioning of active maintenance for some components; independent analyses and academic reviews summarizing the results and lessons are available from research and advisory bodies.

The Artificial Intelligence 4.0 Program (AI 4.0) is a national strategy-led programme launched by the Ministry of Economic Affairs and Employment to accelerate the introduction and diffusion of AI and related digital technologies across Finnish industry, with a particular focus on SMEs and the twin (digital + green) transition. A steering group was appointed in November 2020; interim reports were published in 2021 and the programme's final report was published by the Ministry in 2022.

The Well-being and Health Sector's Artificial Intelligence and Robotics Program (*Hyteairo*, or *Hyvinvoinnin tekoäly ja robotiikka*) is a Finnish Government sector program led by the Ministry of Social Affairs and Health (STM) and coordinated operationally with the Finnish Institute for Health and Welfare (THL). The program was initiated in 2018 to accelerate the safe, ethical and evidence-based use of AI and robotics across social and health services, with an emphasis on practical implementation in home care, conversational AI and analytics. *Hyteairo* operated as a national coordination and facilitation platform — convening public authorities, regional wellbeing service counties, research organizations, testbeds and private sector actors — and produced strategic deliverables, operating models (including the KATI model for tech-enabled home living), and a final program report.

d) The Polish AI legal framework is composed of several critical instruments that govern the development, deployment, and data usage of AI systems⁸. The legislative architecture for AI in Poland is built upon several pillars that address different aspects of the technology's lifecycle. The *Draft Act on Artificial Intelligence Systems* (2026) is the cornerstone of this framework, serving as the primary national instrument for implementing the EU AI Act. This act defines the specific powers of the national market

⁸ M. Granat, *Digital Revolution as a Constitutional Challenge. A Polish Perspective*, in L. Mezzetti (cur.), *Science, technology and law*, cit., 121-135.

surveillance authority, the Commission for AI Development and Safety (KRiBSI), and sets out the procedural rules for conformity assessments and system registration. It also establishes the legal basis for the national AI registry, where all high-risk systems must be documented before they can be placed on the market. Another critical piece of legislation is the "Act on Open Data and Re-use of Public Sector Information." This law will be essential for AI development as it mandates that public sector data be made available in machine-readable formats, providing the "fuel" necessary for training accurate and unbiased AI models.

The Act on Data Management (2026) further complements this by transposing the EU Data Governance Act into Polish law. This act creates a framework for "data altruism," allowing individuals and companies to voluntarily share their data for the public good, such as for medical research or environmental monitoring, under strict privacy protections.

Furthermore, the Strategy for the Digitization of Poland to 2035 provides the long-term legislative and policy goals, setting specific targets for AI adoption across various sectors of the economy. These laws do not exist in isolation; they are integrated with existing statutes, such as the "Personal Data Protection Act" and the "Act on the National Cybersecurity System," creating a comprehensive legal web that covers everything from data acquisition to system deployment and security. This legislative density ensures that there are no "legal vacuums" where AI could operate without oversight. The framework also includes the original "Policy for the Development of AI in Poland from 2020," which established the initial six priority areas for AI capacity building in science, education, and the economy.

e) In Spain, the draft bill *Anteproyecto de Ley* for the Good Use and Governance of Artificial Intelligence intends to adapt Spain's legal framework to the EU AI Act, focusing on ethical AI, risk management, and innovation through sandboxes. It defines prohibited practices, obligations for high-risk systems, and transparency duties for generative AI.

The *Royal Decree 729/2023* approving the Statute of the Spanish Agency for AI Supervision establishes AESIA as an autonomous public agency with the mandate to supervise, inspect, advise, and promote the ethical and safe implementation of AI rules in Spain, acting as the national supervisory authority for AI.

Spanish Digital Rights Charter is a policy framework adopted in 2021 that clarifies and promotes the application of fundamental rights in digital environments, serving as a reference document to guide future AI legislation and public administration practices.

National Artificial Intelligence Strategy (ENIA) is a strategic document published in 2020, that sets out priorities, funding, and institutional arrangements to promote responsible AI research, deployment, and governance across Spain, linking to EU policy and the Recovery Plan.

f) In Sweden, to operationalize the EU Act at the national level, the Swedish government commissioned the report "*Anpassningar till AI-förordningen*" (SOU 2025:101). This proposed national legislative package creates a new Swedish law and ordinance to supplement the EU Act,

designating national authorities and defining their specific enforcement powers within the Swedish legal tradition.

Another critical document is the "*AI-kommissionens Färdplan för Sverige*" (SOU 2025:12), a strategic roadmap that, while not a binding law, provides the policy basis for national investments, infrastructure development, and public sector AI adoption through 2027.

Furthermore, the Data Protection Act (2018:218) remains essential, as it supplements the GDPR and governs the processing of personal data within AI systems in Sweden.

Finally, the original "National Approach to Artificial Intelligence" (2018) continues to serve as the high-level policy document setting the strategic direction for AI development, education, and ethical use, though it is increasingly being superseded by the more prescriptive EU-derived rules.

6. Jurisdictions not equipped (so far) with proposals or bills implementing the EU AI Act (Austria, Bulgaria, Croatia, Estonia, France, Latvia)

a) The Digital Austria Act 2.0 (2025) serves as the strategic framework for digital sovereignty, focusing on the use of open-source standards in public administration and the establishment of shared Large Language Model (LLM) services. This is supported by the *KommAustria-Gesetz (KOG)* §20c and TKG 2021 §194a (*Bundesgesetz über die Einrichtung einer Kommunikationsbehörde Austria („KommAustria“)* (*KommAustria-Gesetz – KOG*, 2026), which provided the legal basis for the KI-Servicestelle and the KI-Beirat, mandating the RTR to act as a national competence center for AI. These laws ensure that the regulatory bodies have the necessary resources and legal authority to monitor the market and provide guidance to stakeholders.

Furthermore, the *Informationsfreiheitsgesetz (IFG - 2024)* implements a proactive transparency regime, requiring the publication of metadata and information of general interest, which facilitates the development of transparent and accountable AI systems. The *Datenstrategie für Österreich* (2024) defines the governance of public and private sector data, emphasizing interoperability and the use of the Austrian Micro Data Center (AMDC) for research. Finally, the foundational Artificial Intelligence Mission Austria 2030 (AIM AT 2030) remains the guiding strategy for human-centered AI and economic competitiveness. Together, these pieces of legislation create a comprehensive legal environment that addresses the technical, ethical, and social dimensions of artificial intelligence, ensuring that the technology serves the public good while minimizing potential harms.

The *KI-Umsetzungsplan 2024* is Austria's 2024 implementation plan that supplements the national AI strategy AIM AT 2030. It lists 47 measures across all federal ministries to operationalize objectives such as trustworthy AI, resilience and security, sustainability and technological sovereignty while aligning national activity with the EU AI Act.

b) Supporting the EU AI Act in Bulgaria is the Concept for the Development of Artificial Intelligence in Bulgaria until 2030, a foundational

national policy document adopted by the Council of Ministers in 2020. This concept defines the strategic pillars for AI research, infrastructure, and ethics, providing a long-term vision for the country's technological advancement. Another critical component is the Digital Transformation of Bulgaria for the period 2020–2030, a cross-sectoral strategy that integrates AI into the broader national digital transition and infrastructure development. This is complemented by the National Program 'Digital Bulgaria 2025', which acts as a roadmap for modernizing public services and digital skills, including specific measures for cybersecurity and AI innovation. More recently, the Draft National Strategy for Artificial Intelligence (2025 Proposal) has been introduced as an updated operational roadmap designed to translate the 2020 Concept into concrete actions aligned with the EU AI Act. Finally, the Draft Strategy for AI in Bulgarian Education (2025) represents a specialized policy framework targeting the safe and ethical integration of AI in schools and universities, highlighting Bulgaria's commitment to preparing its workforce for an AI-driven future.

c) Croatia's national transposition process for the EU Artificial Intelligence Act is organized through an inter-ministerial working group convened by the Ministry of Justice, Administration and Digital Transformation. The group's mandate is to prepare a draft implementing law and related administrative measures that will operationalize Regulation (EU) 2024/1689 within Croatia, identify the national supervisory and market surveillance authorities required by the AI Act, and coordinate technical and sectoral guidance to stakeholders. The working-group membership published by the ministry includes representatives from central ministries, the Croatian Personal Data Protection Agency (AZOP), the ombudsperson's offices, academic and research institutions and industry bodies, reflecting an approach designed to balance rights protection, market functioning and innovation. The national transposition work explicitly references the EU instrument and timelines (Regulation (EU) 2024/1689) and coordinates with national authorities already designated for fundamental-rights oversight.

This is supported by the Digital Croatia Strategy 2032, a comprehensive ten-year framework adopted by Parliament that sets the strategic goals for digital transformation, including the development of an innovative digital economy and the expansion of AI-enabled public services. Another critical component is the National AI Plan 2032 (Draft), 2025, a government-initiated policy document that outlines the long-term vision for AI in Croatia, focusing on three pillars: policy formulation, investment, and effective deployment. The Smart Specialization Strategy (S3) 2029 further identifies "Digital products and platforms" as a priority area, specifically highlighting machine learning and AI as horizontal enablers for the Croatian economy. Additionally, the National Recovery and Resilience Plan (NPOO) acts as a multi-billion euro investment plan that funds specific AI projects in the public sector, such as e-justice and digital health initiatives, while mandating reforms to support the digital transition. These laws and strategies work in tandem to create a legal environment that prioritizes both safety and growth. The Act on the Implementation of the General Data

Protection Regulation also remains a cornerstone, providing the necessary legal safeguards for the processing of personal data within AI systems, ensuring that Croatian citizens' privacy is protected in accordance with the highest European standards.

d) In Estonia, the Draft Data and Artificial Intelligence White Paper 2024–2030 (2024) is a strategic government document outlining Estonia's long-term vision, missions, and implementation program for its data economy and AI ecosystem. It defines key focus areas such as data governance, trustworthy AI, language technology, skills development, and international alignment, guiding future regulatory and operational initiatives.

AI and Data Action Plan (Kratt) 2024–2026, 2024 serves as an operational roadmap that details Estonia's strategic priorities and concrete measures for advancing data economy and AI capabilities. It focuses on strengthening public and private sector adoption, promoting Estonian language technology, improving skills and education, and ensuring human-centric AI development, building on previous national AI strategies.

AI Leap — national AI in education initiative serves as a national education program launched in 2025 by the Ministry of Education and Research. It provides free access to leading AI learning applications and comprehensive AI literacy and professional development for teachers and students across upper-secondary schools and vocational education, emphasizing ethical, privacy, and safety concerns.

e) The legislative landscape in France is anchored by several key acts that predate and complement the EU AI Act. The *Loi n° 2016-1321* (Digital Republic Law) is perhaps the most significant, as it established the legal right for citizens to receive an explanation for any individual decision made by an algorithm in the public sector. This was followed by the *Loi n° 2018-493* (Data Protection Act), which updated the 1978 '*Informatique et Libertés*' law to align with the GDPR while adding specific French protections for biometric and health data. More recently, the *Loi n° 2024-449* (SREN Law) has emerged as a critical piece of legislation for the AI era. The SREN Law addresses the infrastructure of AI by regulating cloud service providers, mandating interoperability, and limiting the anti-competitive practices of 'hyperscalers.' It also grants new powers to ARCOM to regulate online safety and content moderation, areas where AI is heavily utilized. Another important legislative development is the Decree No. 2022-676, which established the *Service de garantie de l'identité numérique (SGIN)*, a framework for secure digital identity that incorporates AI-driven authentication while maintaining high privacy standards. These laws are supported by the Code of Relations between the Public and the Administration (CRPA), which codifies the transparency requirements for public sector algorithms. Together, these pieces of legislation create a comprehensive framework that addresses the data, the infrastructure, and the specific applications of AI across both the public and private sectors. The French Parliament is also actively considering new bills related to the protection of intellectual property in the context of generative AI, ensuring that creators are fairly compensated when their works are used for model training.

f) The legislative landscape in Latvia is anchored by several key instruments that work in concert to regulate the AI lifecycle. The *Law on the Latvian Artificial Intelligence Centre (2025)* is the foundational act, establishing the Centre as a public foundation with the mandate to coordinate national AI policy, manage the regulatory sandbox, and provide expert opinions to other state agencies. This is complemented by the Law on the Development of Artificial Intelligence (2025), which sets out the broader strategic objectives for the national AI ecosystem, including the promotion of AI literacy and the ethical use of automated systems in public administration.

Older but still relevant documents, such as the Digital Transformation Guidelines 2021–2027 (2021) and the 2020 Informative Report, provide the policy context and long-term vision that continue to guide the interpretation and implementation of these newer, binding statutes. Together, these laws form a comprehensive net that captures both the developmental potential and the inherent risks of AI technology.

7. Implementing the EU AI Act: authorities and governance in the Member States

Since the AI Act entered into force on the 1st of August of 2025, Member States have to implement the AI Act also on the organizational and governance side⁹.

Member States are required to designate or establish three kinds of authorities as part of the implementation of the EU AI Act.

First, a “market surveillance authority” acting as a single point of contact shall undertake the activities and adopt the measures provided for under Regulation (EU) 2019/1020 concerning market surveillance and product compliance (Art. 3(26)). Accordingly, this authority is based on the already established framework of market surveillance authorities within EU law and is entrusted with ensuring that only products compliant with Union legislation are placed on the EU market.

Second, a “notifying authority” shall constitute the national authority responsible for establishing and carrying out the procedures relating to the assessment, designation, notification, and monitoring of conformity assessment bodies (Art. 3(19) and Art. 28(1)). “Conformity assessment bodies” are entities entrusted with conducting third-party conformity assessment activities, including testing, certification, and inspection procedures (Art. 3(21)).

Together, the notifying authority and the market surveillance authority are defined as the national competent authorities (Art. 3(48)). These authorities are required to operate independently, impartially, and free from bias, while also possessing sufficient technical expertise, financial means, human resources, and infrastructure necessary to effectively perform their functions under the AI Act (Art. 70(1) and (3)). Furthermore, the

⁹ N. A. Smuha (cur.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge, 2025.

Commission is tasked with facilitating the exchange of experience and best practices among national competent authorities (Art. 70(7)).

Third, Member States are required to designate national public authorities responsible for enforcing compliance with obligations relating to the protection of fundamental rights in connection with high-risk AI systems listed in Annex III. Such authorities must be granted the power to request and access any documentation prepared or maintained pursuant to the AI Act where such documentation is necessary for the effective exercise of their mandate within the scope of their jurisdiction (Art. 77(2))¹⁰.

The synoptic analysis of the organizational solutions adopted by the Member States of the European Union when implementing the AI Act within their domestic legal systems shows a scenario in which three main models prevail: a) jurisdictions equipped with a systematic organic structure (market surveillance authority, notifying authority, fundamental rights protection bodies); b) jurisdictions that have established or identified one or more supervisory authorities on the digital market, but have not (so far) provided for the designation of a notifying authority; c) jurisdictions that still lack digital market supervisory and notification authorities.

It is also worth emphasizing that, regardless of the specific solution adopted within the various experiences regarding the adoption of monistic, dualistic, or polycentric models, all legal systems have one or more political bodies vested within the executive branch with the function of providing political direction and coordinating administrative activities regarding artificial intelligence. These bodies are supported by independent administrative authorities and/or agencies with specialized and sector-specific functions of active, consultative, and oversight administration, as well as by monitoring bodies that are typically entrusted with the delicate task of overseeing the correct use of artificial intelligence and its compatibility with fundamental human rights¹¹.

7.1 Jurisdictions equipped with a systematic organic structure (market surveillance authority, notifying authority, fundamental rights protection bodies)

α) This category includes experiences that have established or identified independent administrative authorities for digital market oversight, as well as notification authorities, as well as bodies for the protection of fundamental rights in relation to the use of artificial intelligence. The model followed is monistic in each of the areas considered. It has been adopted by the Czech Republic, Cyprus, France, Germany, Hungary, Malta, Poland, Lithuania and Italy.

a) The Czech Republic is in the process of finalizing its national AI legislation to align with the EU AI Act, with the Ministry of Industry and Trade (MIT) - *Ministerstvo průmyslu a obchodu* (MPO) acts as the central

¹⁰ H.P. Olsen et al. (cur.), *Artificial Intelligence, Humans and the Law*, London, 2025.

¹¹ R. Abbott, E. Rothman (cur.), *Elgar Concise Encyclopedia of Artificial Intelligence and the Law*, Cheltenham, 2025.

coordinator and lead authority, responsible for national AI strategy and AI governance.

The Czech Telecommunication Office (CTU) / *Český telekomunikační úřad* (ČTÚ) has been designated as the primary market surveillance authority for AI, handling general supervision and acting as the single point of contact.

The Office for Technical Standardization, Metrology and Testing (ÚNMZ) / *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* has been designated as the notifying authority, responsible for evaluating and appointing notified bodies for conformity assessments.

The Public Defender of Rights (Ombudsman) is expected to play a role in protecting fundamental rights regarding AI deployments.

The Office for Personal Data Protection (ÚOOÚ) / *Úřad pro ochranu osobních údajů* is responsible for supervision concerning high-risk AI systems in areas like law enforcement, migration, and justice.

The Czech National Bank (ČNB) / *Česká národní banka* supervises AI systems used by financial institutions under its jurisdiction.

The Czech Agency for Standardization (ČAS) / *Česká agentura pro standardizaci* is involved in establishing and managing the regulatory sandbox.

b) The primary regulatory bodies overseeing AI compliance and governance in Cyprus are split into three central roles.

The Deputy Ministry of Research, Innovation and Digital Policy (DMRID) leads the overarching coordination of the AI Act's implementation at the national level, formulates regulatory frameworks, manages compliance preparation, and represents Cyprus directly on the European Artificial Intelligence Board (AI Board). The Commissioner of Electronic Communications has been designated as the primary national Single Point of Contact for the AI Act in Cyprus, working as Notifying Authority, responsible for establishing and executing the necessary procedures for the assessment, designation, and notification of conformity assessment bodies, and as Market Surveillance Authority (MSA), acting as the primary watchdog monitoring AI product compliance, issuing withdrawals, and enforcing corrective measures across industries.

The Commissioner for Personal Data Protection as Specialized Market Surveillance Authority (MSA) directly supervises specific high-risk AI systems defined under Annex III of the AI Act (specifically categories 1, 6, 7, and 8, which involve biometric identification, law enforcement, migration/asylum, and administration of justice). It is also tasked with enforcing prohibitions on forbidden AI practices that fall within her data protection domain.

Under Article 77 of the AI Act, Cyprus has additionally notified the European Commission of three specific authorities responsible for safeguarding fundamental rights against risks posed by high-risk AI systems: the Commissioner for Personal Data Protection, the Commissioner for Administration and the Protection of Human Rights (Ombudsman), and the Attorney-General of the Republic of Cyprus.

c) France has opted for a decentralized approach that coordinates sector-specific regulators. The *Direction générale de la concurrence, de la consommation et de la répression des fraudes* (DGCCRF) is set as the single point of contact and coordinates market surveillance, supported by sector-specific agencies, while the *Direction générale des entreprises* (DGE) leads on regulatory implementation, acting as the notifying authority to oversee standardization and implementation.

The CNIL (*Commission Nationale de l'Informatique et des Libertés*) remains the key authority for AI systems impacting personal data, fundamental rights, and AI model oversight.

To the purposes of technical support and expertise, the ANSSI (*Agence nationale de la sécurité des systèmes d'information*) is responsible for cybersecurity requirements in AI systems; the PEReN (*Pôle d'expertise et de régulation numérique*) provides technical audits and assessment support.

Various sectoral regulators are involved, overseeing AI within their specific domains: medical devices (ANSM), media (ARCOM), finance (ACPR (Banque de France); transport (various bodies overseen by the Ministry of Transportation).

d) Germany is currently implementing the EU AI Act through the proposed AI Market Surveillance and Innovation Promotion Act (KI-MIG). The draft bill, approved by German Federal Cabinet on February 11, 2026, designates the primary national competent authorities.

As central market surveillance and notifying authority is designated as primary authority the Federal Network Agency (*Bundesnetzagentur* or *BNetzA*). It will house an independent "AI Market Surveillance Chamber". Established at the Federal Network Agency, a Coordination and Competence Centre (KoKIVO) is going to act as the central coordination structure for AI regulation and support other authorities. Already operational, the BNetzA AI Service Desk supports companies and authorities in implementing the AI Regulation.

Existing authorities remain responsible as sectoral regulators for specialized sectors. For example, BaFin (Federal Financial Supervisory Authority) will oversee AI used in financial services.

Data Protection Authorities (DPAs) are responsible for overseeing AI systems related to processing personal data.

e) Following the adoption of Act LXXV of 2025, the Hungarian government has created a structured approach to regulate AI system deployment, market surveillance, and conformity assessments.

Designated and Key Regulatory Bodies include the National Economy Minister as Market Surveillance Authority & Single Point of Contact (SPoC), who oversees compliance for AI systems placed on the market or used in Hungary, and the National Accreditation Authority as notifying Authority, tasked with supervising conformity assessment bodies.

The Hungarian Artificial Intelligence Council (Hungarian AI Coalition) acts as an advisory body, which includes stakeholders from government, business, and research sectors.

For high-risk AI systems used by financial institutions, the Hungarian National Bank (*Magyar Nemzeti Bank*) will act as the market surveillance authority.

The National Authority for Data Protection and Freedom of Information (NAIH) is expected to be a key participant in overseeing AI's impact on fundamental rights.

f) Malta has designated the Malta Digital Innovation Authority (MDIA) as the primary national competent authority, Market Surveillance Authority (MSA), Notifying Authority, and Lead Coordinator for Artificial Intelligence (AI). This designation aligns with the implementation of the EU AI Act (via Legal Notice 226 of 2025), positioning the MDIA as the main supervisor for high-risk AI systems and the national AI regulatory sandbox. [1, 2, 3]

The Information and Data Protection Commissioner (IDPC) is designated as a specialized MSA focusing on the protection of personal data and fundamental rights. Its roles include overseeing high-risk AI systems specifically related to law enforcement, border management, and the administration of justice; maintaining a national registry for high-risk AI systems, and enforcing rules against prohibited AI practices that threaten privacy and data protection.

g) As of early 2026, Poland is implementing a centralized model for AI supervision under the EU AI Act, establishing a specialized, dedicated body rather than relying solely on existing distributed regulators.

Market Surveillance Authority & Single Point of Contact is the Commission for the Development and Safety of Artificial Intelligence (*Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji* – KRiBSI), a collegial body comprising members from the Office of Competition and Consumer Protection (UOKiK), Financial Supervision Authority (KNF), National Broadcasting Council (KRRiT), and Office of Electronic Communications (UKE), who is responsible for overall market surveillance, compliance checks, and coordinating high-risk AI assessment. The Ministry of Digital Affairs serves as the operational hub (Bureau) supporting the KRiBSI, holding the staff and budget for day-to-day enforcement. The Personal Data Protection Office (UODO) acts as the authority for AI matters involving data protection (GDPR) and AI regulatory sandboxes, working closely with the KRiBSI.

Notifying Authority is the Minister for Digital Affairs (*Ministerstwo Cyfryzacji*), responsible for notifying conformity assessment bodies.

The Ministry of Digital Affairs designated the Children's Rights Ombudsman, Patients' Rights Ombudsman, and the National Labor Inspectorate to oversee fundamental rights protections related to high-risk AI systems (Article 77 of the EU AI Act).

h) In Lithuania, the national competent authorities responsible for the implementation and enforcement of the EU Artificial Intelligence (AI) Act are being established and designated, with key roles assigned to the Innovation Agency Lithuania, designated as the notifying authority and responsible for creating and supervising the AI regulatory sandbox

(pursuant to Articles 28(1), 57(1), and 70(1) of the AI Act); the Communications Regulatory Authority, designated as a market surveillance authority and acting as the single point of contact for AI regulation; the Ministry of Economy and Innovation of the Republic of Lithuania, responsible for the overall regulatory framework and overseeing the adoption of the AI Act.

i) Italy has established a comprehensive national framework for Artificial Intelligence through Law No. 132/2025, which entered into force on October 10, 2025, acting as the first EU country to pass such dedicated legislation to complement the EU AI Act.

The law designates a dual-authority structure for AI governance: the Agency for Digital Italy (AgID) acts as the Notifying Authority and is responsible for promoting innovation and development of AI, defines procedures, evaluates, accredits, and monitors entities responsible for verifying the compliance of AI systems; the National Cybersecurity Agency (ACN) acts as the Market Surveillance Authority and as the single point of contact for AI compliance, aligning with the EU AI Act: as the Lead Authority for the use of AI in cybersecurity, handles surveillance, inspection, and sanctioning activities related to AI systems, ensuring their security and resilience. A special coordination committee within the Presidency of the Council of Ministers ensures cooperation between AgID, ACN, and other public/independent authorities.

Established authorities retain their powers, including the Italian Data Protection Authority for privacy, as well as the Bank of Italy, CONSOB, IVASS, and AGCOM for financial, insurance and communication sectors.

AgID and ACN jointly establish experimental spaces (sandboxes) for AI development.

β) In some jurisdictions, the assignment of market surveillance functions has followed a polycentric model, characterized by the distribution of these functions among multiple competent bodies, identified according to their material scope of operation and taking into account specialization criteria. This is the case in Denmark, Latvia, Luxembourg, and Sweden.

1) Denmark has designated three key entities as its national competent authorities.

The Agency for Digital Government (*Digitaliseringsstyrelsen*) acts as the national coordinating supervisory authority. It serves as Denmark's central point of contact for the European Commission and other EU member states. It also holds the role of notifying authority under Article 70(1) of the AI Act, making it responsible for assessing and monitoring the bodies that perform AI conformity tests. Additionally, market surveillance responsibilities are distributed among three distinct authorities depending on the domain and application: the Agency for Digital Government (*Digitaliseringsstyrelsen*), that exercises cross-sectoral market surveillance powers over standard commercial and public-sector AI systems; the Danish Data Protection Agency (*Datatilsynet*), who supervises specific high-risk or prohibited AI systems, including AI used for profiling, personality trait tracking, and predicting criminal offenses; the Danish Court Administration (*Domstolsstyrelsen*), who acts as the market surveillance authority for AI

deployment within court environments, explicitly restricted to administrative and non-judicial operations.

These designated market surveillance authorities possess the mandate to protect fundamental rights and enforce compliance conducting unannounced on-site inspections, issuing binding injunctions, imposing temporary or permanent prohibitions on non-compliant AI systems, and enforcing financial penalties and administrative fines.

m) Latvia has designated its national competent authorities to implement and enforce the EU AI Act as of May 2025: the governance structure involves a central, coordinating ministry and several sectoral market surveillance authorities. Responsible Authority for AI Act Implementation is the Ministry of Smart Administration and Regional Development (VARAM); Notifying Authority is the Ministry of Economy. Market surveillance is distributed across specialized agencies, including the State Data Inspectorate (DVI) for prohibited AI, the Consumer Rights Protection Centre (PTAC) for consumer protection, and the Health Inspectorate (VI) for health. Additional sector-specific supervision is provided by transport agencies (CAA, Maritime Administration, Railway Inspectorate, Technical Supervision Agency, CSDD), the State Service for Quality of Education, security bodies (VDD, MIDD, SAB), and the Bank of Latvia for the financial sector.

Latvian National Accreditation Bureau (LATAK) works as National Accreditation Body.

Ombudsman of the Republic of Latvia operates as Fundamental Rights Authority.

n) In Luxembourg, the CNPD (*Commission Nationale pour la Protection des Données*) has been designated as the default market surveillance authority, the single point of contact, and the central coordinator for AI systems not covered by specialized sectoral authorities.

Sector-Specific Surveillance Authorities retain their competences in peculiar areas: the CSSF (*Commission de Surveillance du Secteur Financier*) acts as the surveillance authority for AI systems used in the financial sector; the Commissariat aux Assurances (CAA) oversees AI systems related to the insurance sector; the ALIA (*Autorité luxembourgeoise indépendante de l'audiovisuel*) manages AI systems related to media and transparency; the JSA (Judicial Supervisory Authority) monitors AI systems used by judicial courts and prosecution services.

Notifying Authority is the OLAS (*Office Luxembourgeois d'Accréditation et de Surveillance*), responsible for the accreditation and supervision of conformity assessment bodies.

o) Sweden has established a roadmap for implementing the EU AI Act, with most designated authorities set to be fully active by August 2, 2026.

As Main Market Surveillance Authority and Single Point of Contact has been designated the Swedish Post and Telecom Authority (*Sv. Post- och telestyrelsen, PTS*) as the primary authority to coordinate market surveillance and act as the national single contact point.

The Swedish Post and Telecom Authority (PTS) and the Swedish Medical Products Agency (*Läkemedelsverket*) are the two main notifying authorities, responsible for approving notified bodies.

In addition to PTS, a total of 11 market surveillance authorities are proposed to handle sector-specific AI regulations. This includes the Swedish Medical Products Agency for high-risk AI in medical devices.

The Swedish Agency for Digital Government (DIGG) is tasked with supporting AI uptake and regulation within public administration.

7.2. Jurisdictions that have established or identified one or more supervisory authorities on the digital market, but have not (so far) provided for the designation of a notifying authority

A monist model of conferring supervisory functions on the digital market to a single authority has been adopted by Austria, Belgium, Estonia, Romania, Slovenia, and Spain.

a) Austria is in the process of finalizing the designation of its national competent authorities for the EU AI Act: it is widely expected that RTR GmbH (Austrian Regulatory Authority for Broadcasting and Telecommunications) will be formally designated as the main market surveillance authority and national supervisor, although this is still pending final confirmation. The RTR GmbH has established an AI Service Desk (point of contact) to support the implementation of the EU AI Act and serve as the information hub. Furthermore, the Austrian government has published a list of 19 potential bodies across 8 areas, covering existing regulators, to oversee specific sectors under the AI Act.

As the existing AI governance structure, a *KI-Beirat* (AI Advisory Board) works as a national board composed of experts from research and business to advise on AI policy; the AI Policy Forum, composed of members from various ministries, coordinates AI regulation across the government; the AI Stakeholders Forum, that includes various stakeholders, gives input on AI implementation; the *Kommunikationsbehörde Austria* (*KommAustria*) has been designated as a competent authority regarding specific articles related to digital content and communications oversight; the Financial Market Authority (FMA) is expected to serve as the market surveillance authority for the insurance and banking sectors when AI systems are used in those high-risk financial functions.

b) Belgium is in the process of finalizing its national governance structure for the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). While a single, overarching AI regulator is still being established, some bodies have been identified as key competent authorities and supervisory bodies.

According to the 2025–2029 Federal Government Agreement, the Belgian Institute for Postal Services and Telecommunications (BIPT/IBPT) has been identified as the Market Surveillance Authority for AI. Under Article 77 of the EU AI Act, Belgium has designated a granular list of 21 specific bodies empowered to supervise high-risk AI systems, particularly where fundamental rights are at stake. In particular, the Federal

Agency for Medicines and Health Products (FAMHP) is responsible for AI systems in medical devices; the Belgian Data Protection Authority (DPA) handles issues related to profiling, automated decision-making, and GDPR compliance, and has published specific AI Guidelines; the Federal Public Service (FPS) Economy plays a key role in AI regulation implementation, acting as a point of contact for the EU AI Board; FPS Strategy and Support (BOSA) has worked out the national plan for AI development; the Ethics Advisory Council on Data and AI has been appointed by the Minister of Civil Service and the State Secretary for Digitization to provide guidance.

Depending on the nature of the AI application, pre-existing authorities may intervene: the FAMHP (AFMPS), competent Authority for Health Products and Medicinal Products, supervises AI used in the medical field; the National Bank of Belgium (NBB) acts as market surveillance authority for AI systems used in the banking and financial sectors.

c) In Estonia, the national competent authorities responsible for the implementation and enforcement of the EU AI Act (Regulation (EU) 2024/1689) and tasked with overseeing AI compliance, market surveillance, and conformity assessments, are the Estonian Technical Surveillance Authority (*Tarbijakaitse ja Tehnilise Järelevalve Amet - TTJA*), designated as the market surveillance authority, responsible for supervising AI products and services in the market; the Data Protection Inspectorate (AKI), that - while primarily a data protection authority - is designated as an authority protecting fundamental rights under Article 77 of the AI Act, overseeing the impact of AI systems on privacy and civil liberties; the Ministry of Economic Affairs and Communications, who leads the development of AI policy and strategies and oversees the overall implementation of AI technology into the public sector; the Estonian Internal Security Service (*Kaitsepolitsei - Kapo*), acting as a competent authority, particularly regarding security aspects and potentially overseeing high-risk AI applications in specific sectors.

d) Romania has structured its national competent authorities for the EU AI Act (Regulation (EU) 2024/1689) through a hybrid model, designating specific bodies for market surveillance, conformity assessment, and fundamental rights protection.

The main, central authority designated is the National Authority for Administration and Regulation in Communications (ANCOM), which serves as the single national contact point and market surveillance authority, who is responsible for the overall implementation of the AI Act and monitoring AI systems.

Sector-specific Surveillance Authorities are the ANPC (National Authority for Consumer Protection), jointly responsible with ANCOM for AI in radio equipment and toys; the ANMDM (National Agency for Medicines and Medical Devices), responsible for AI in medical devices, ASF (Financial Supervisory Authority) & BNR (National Bank of Romania), responsible for AI in financial services, and ANSPDCP (National Supervisory Authority for Personal Data Processing), designated for the oversight of biometric systems and AI, acting as an authority for fundamental rights.

Pursuant to Article 77 of the AI Act, Romania has empowered several bodies to protect fundamental rights, including the ANSPDCP (personal

data), the National Council for Combating Discrimination, and the Labor Inspectorate.

The Ministry of Research, Innovation, and Digitalization (MCID) and the Romanian Committee for Artificial Intelligence (AIR) provide strategic policy coordination and support implementation.

e) In Slovenia, the designation of national competent authorities for the implementation of the EU AI Act involves multiple specialized bodies to ensure comprehensive oversight.

Under the draft Act on the implementation of the EU AI Act (published in 2025), Slovenia has designated several key institutions to act as market surveillance and notifying authorities: the Agency for Communication Networks and Services (AKOS), identified as the primary market surveillance authority for AI, responsible for enforcing rules on high-risk systems and prohibited practices; the Ministry of Digital Transformation, who acts as the central coordinating body and leads the establishment of the National AI Competence Center, which serves as a "one-stop-shop" for SMEs and research; the Information Commissioner of the Republic of Slovenia, who serves as the authority for data protection issues related to AI systems; the Insurance Supervision Agency (AZN), who oversees AI systems specifically within the insurance sector, and the Bank of Slovenia, who acts as the market surveillance authority for AI used within the banking and financial services sector.

f) Spain has established a comprehensive framework for artificial intelligence (AI) supervision, positioning itself as the first European Union member state to set up a dedicated national supervisory agency.

AESIA (*Agencia Española de Supervisión de la Inteligencia Artificial* / Spanish Agency for the Supervision of Artificial Intelligence) is the central body responsible for overseeing the ethical and safe use of AI, ensuring compliance with both European Union regulations and the Spanish AI law. It functions as the national market surveillance authority and acts as the single point of contact.

Enforcement in Spain is distributed among existing sectoral authorities to manage risks in specific areas: the AEPD (*Agencia Española de Protección de Datos* / Spanish Data Protection Agency) is responsible for AI risks related to personal data and digital rights; the Bank of Spain and the CNMV (*Comisión Nacional del Mercado de Valores*) act as supervisory authorities for high-risk AI systems in creditworthiness, credit rating, and financial markets; the Directorate General of Insurance and Pension Funds (DGSFP) oversees high-risk AI in life and health insurance; the General Council of the Judiciary (CGPJ) monitors AI systems used in the administration of justice; the Central Electoral Board (*Junta Electoral Central*) supervises AI systems associated with democratic processes.

The Artificial Intelligence Advisory Council (*Consejo Asesor de Inteligencia Artificial*) advises the government on the design and implementation of AI policies, including the National Artificial Intelligence Strategy; the Spanish AI Regulatory Sandbox has been identified as a controlled testing environment designed to prepare companies for the requirements of the EU AI Act.

In some jurisdictions, digital market oversight functions have been distributed among multiple administrative authorities, some newly established, others leveraging existing responsibilities and powers under current legislation. This model has been adopted in Croatia, Finland, Ireland, the Netherlands, Portugal, and Slovakia.

a) The Republic of Croatia has designated several key bodies to act as national competent authorities for the supervision and enforcement of the EU Artificial Intelligence Act. The Ministry of Justice, Public Administration and Digital Transformation is responsible for notifying the European Commission of these designations.

Several bodies have been identified as competent authorities, particularly focused on the protection of fundamental rights under Article 77 of the AI Act: the Ombudswoman of the Republic of Croatia (*Pučka pravobraniteljica*), the Ombudsperson for Children (*Pravobraniteljica za djecu*), the Ombudsperson for Gender Equality (*Pravobraniteljica za ravnopravnost spolova*), the Ombudsperson of Persons with Disabilities (*Pravobraniteljica za osobe s invaliditetom*), the Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka - AZOP*), the State Electoral Commission (*Državno izborno povjerenstvo*) and the Agency for Electronic Media (*Agencija za elektroničke medije*).

In particular, tasked with supervising the compliance of AI systems with the AI Act, particularly regarding the protection of fundamental rights when using high-risk AI systems, is AZOP (Personal Data Protection Agency), that plays a central role in supervising AI systems that process personal data.

The designated authorities are responsible for ensuring that only compliant AI products are available on the market.

b) Finland has adopted a decentralized model to implement the EU AI Act, designating several existing authorities to supervise AI systems based on their sector, with the Ministry of Economic Affairs and Employment (*Työ- ja elinkeinoministeriö*) leading the overall implementation.

Authorities identified as national competent authorities/market surveillance authorities for the AI Act in Finland are the Finnish Transport and Communications Agency (*Traficom*), point of contact for the EU AI Act, who supervises AI applications in communications, transport, and, in early drafts, functioned as the single point of contact; the Finnish Safety and Chemicals Agency (*Tukes*), who handles market surveillance for technical products; the Finnish Financial Supervisory Authority (*Finanssivalvonta*), who monitors AI in the financial sector; the Finnish Medicines Agency (*Fimea*), who monitors AI applications in healthcare and pharmaceuticals; the Finnish National Supervisory Authority for Welfare and Health (*Valvira*), who monitors AI in health and welfare services; the Finnish Energy Authority (*Energiavirasto*), who monitors AI related to energy systems; the Finnish Customs Agency (*Tulli*), who controls AI devices entering the market from abroad; the Occupational Safety and Health Administration (*Työsuojelu*), who oversees AI systems in the workplace.

The Office of the Data Protection Ombudsman (*Tietosuojavaltuutetun toimisto*) oversees AI systems regarding data privacy, fundamental rights, and high-risk systems under Article 77.

c) Ireland has adopted a distributed enforcement model for the EU AI Act, designating 15 National Competent Authorities (NCAs) that align with existing sectoral regulatory lines. These authorities are tasked with supervising AI systems within their specific domains to leverage existing deep sectoral expertise.

Central Coordinating Body is the National AI Office (NAIO) / AI Office of Ireland, established as a new statutory independent body under the Department of Enterprise, Tourism and Employment (DETE).

It serves as Ireland's Single Point of Contact for the EU, coordinates the activities of all 15 NCAs, facilitates access to technical expertise, and hosts a regulatory sandbox to drive safe innovation.

The 15 NCAs responsible for oversight and enforcement include financial services (Central Bank of Ireland), data protection (Data Protection Commission - DPC), specifically for AI processing personal data, media and online safety (*Coimisiún na Meán*), health safety (Health and Safety Authority (HSA) and the Health Products Regulatory Authority (HPRA), communications (Commission for Communications Regulation - ComReg), competition and consumer protection (Competition and Consumer Protection Commission - CCPC), transport (Commission for Railway Regulation, National Transport Authority (NTA), and the Marine Survey Office, employment and utilities (Workplace Relations Commission- WRC) and the Commission for Regulation of Utilities (CRU), government and health services (Minister for Enterprise, Tourism and Employment, Minister for Transport, and the Health Service Executive (HSE).

d) The Netherlands has adopted a decentralized, hybrid supervisory model for AI regulation, aligning with the EU AI Act's enforcement requirements by August 2025. Rather than creating one single AI authority, the Dutch government has designated existing sectoral regulators to oversee AI within their respective domains.

Coordinating roles are attributed to the Dutch Authority for Digital Infrastructure (RDI) (*Rijksdienst Digitale Infrastructuur*) and to the Dutch Data Protection Authority (AP) (*Autoriteit Persoonsgegevens*) lead the coordination. Work as sectoral supervisors (market surveillance authorities) the Dutch Authority for the Financial Markets (AFM) and Dutch Central Bank (DNB) (finance); the Health and Youth Care Inspectorate (IGJ) (healthcare); the Netherlands Food and Consumer Product Safety Authority (NVWA) (consumer protection/product safety; the Netherlands Labour Authority (NLA) (labor); Human Environment and Transport Inspectorate (ILT) (transport, infrastructure).

The Netherlands Institute for Human Rights (CRM) is designated for monitoring fundamental rights.

e) Portugal has designated ANACOM - *Autoridade Nacional de Comunicações* (National Communications Authority) as the main national regulator, market surveillance authority and Single Point of Contact for AI supervision under the EU AI Act. Additionally, 14 distinct authorities have been identified to participate in the broader market surveillance landscape for AI, ensuring that sector-specific expertise is utilized.

The CNPD (*Comissão Nacional de Proteção de Dados* - National Data Protection Commission) is expected to play a critical role, particularly in handling issues related to data usage, privacy, and fundamental rights.

Portugal has adopted a structured approach to digital rights, focusing on creating an inclusive, ethical, and safe environment. The national strategy, known as the National Digital Strategy (EDN), aims to promote the digital transition by ensuring the protection of fundamental rights and universal access to technologies. Article 268 of the Portuguese Constitution guarantees the right of access to administrative courts for the defense of digital rights and controls digital administrative behavior. Portugal is actively implementing digital identity solutions, including digital travel credentials based on identity cards for free movement within the EU. The country is a leader in the EU, having launched digital wallets for businesses to simplify interactions with public administrations. Portugal offers specific visas (such as the D8 visa) for digital nomads, regulating remote work for those operating from outside the country. The Portuguese Charter of Human Rights in the Digital Era (*Carta Portuguesa de Direitos Humanos na Era Digital*), approved by Law No. 27/2021 on May 17, 2021, is a landmark legal framework in Portugal that establishes a set of fundamental rights, freedoms, and guarantees specifically for the digital environment. It ensures that rights protected in physical life are also guaranteed in cyberspace. The Charter covers a broad spectrum of digital rights, including free access to the internet, promoting digital inclusion and bridging the digital divide, protection of the right to express, create, and share information online without censorship, protection of privacy, including the right to protection against abusive geolocation and the "right to be forgotten" (erasure of personal data), the right to acquire skills necessary for safe and active participation in the digital society, the right to a secure, resilient digital environment, the right to meeting, manifestation, association, and participation in the digital environment. The Law mandates the State to combat disinformation ("fake news") in accordance with European Action Plans. The Charter calls for transparency in automated decision-making and artificial intelligence to prevent discrimination and it aligns with European efforts to improve conditions for workers on digital platforms.

The CNCS (*Centro Nacional de Cibersegurança* - National Cybersecurity Centre) is involved in strengthening the supervision of AI systems, as seen in hosting European Working Group meetings on AI.

The ERC (*Entidade Reguladora para a Comunicação Social*) is identified as a potential stakeholder in supervising AI in media.

f) Slovakia is currently in the process of designating and establishing its National Competent Authorities (NCAs) to fulfill its obligations under the EU AI Act.

The primary responsibility for AI governance in Slovakia is centralized within the Ministry of Investments, Regional Development and Informatization (MIRRI), who acts as a key competent authority for the Slovak AI landscape and it is tasked with exercising rights and obligations related to AI experimental environments (sandboxes) and overseeing national AI strategies, and the National Security Authority (NBU), who collaborates with MIRRI to evaluate the use of AI in security procedures and serves as a critical partner in the national coordination center for cybersecurity.

As the identification of Market Surveillance and Notifying Authorities are concerned, under the AI Act framework, Slovakia is adapting

existing statutes (notably Act No. 318/2025 Z. z.) to designate specific market surveillance authorities to ensure AI product compliance and notifying authorities to monitor conformity assessment bodies.

7.3. Jurisdictions that still lack digital market supervisory and notification authorities.

In two jurisdictions—Bulgaria and Greece—one or more digital market supervisory and notification authorities have not yet been designated. However, these jurisdictions are equipped with a variety of bodies with specialized and sector-specific expertise that ensure—albeit in its core—the implementation of a minimal organizational structure designed for the sector-specific management of the various areas encompassing the artificial intelligence constellation.

a) In Bulgaria, the designation of national competent authorities for the EU AI Act is currently in a preparatory stage, with a national framework still being finalized. While specific single authorities for market surveillance and notification have not yet been fully established by law, some entities and structures play key roles in Bulgaria's AI regulatory and policy landscape. The Ministry of e-Government, successor to previous IT and communications policies, oversees the development of AI concepts and is expected to house a Public Council for Information Technologies and Information Society with a dedicated thematic working group for AI. The Ministry of Interior - General Directorate Combating Organised Crime, currently designated as a competent authority for specific digital security and cybercrime matters (specifically relating to terrorist content online), serves as a primary contact point for these areas. The Communications Regulation Commission (CRC) has been recently designated as the Digital Services Coordinator and competent authority under the Digital Services Act (DSA), which overlaps with broader AI and digital platform oversight. The Commission for Personal Data Protection (CPDP) acts as a competent authority for specific areas of supervision, particularly regarding data protection and fundamental rights in digital contexts. The Council for Electronic Media works as a competent authority for specific areas under digital governance frameworks. [1, 2, 3, 4, 5]

b) For specialized areas like telecommunications and security, three bodies have been identified as competent authorities for specific regulatory tasks: the Telecommunications and Postal Committee (EETT), the Prosecutor of the Anti-terrorist Unit and the National Intelligence Service (EYP).

While the formal, single national authority pursuant to Article 70 is still being finalized, the Greek government has identified key bodies responsible for supervising high-risk AI systems and enforcing fundamental rights.

The Ministry of Digital Governance, who leads the implementation of the AI Act and acts as the central coordinator, represents Greece in the AI Board and has submitted a list of key authorities to the European Commission, which includes the Hellenic Data Protection Authority (ΑΠΔΠΧ / HDPA), responsible for data protection issues in AI systems; the Greek Ombudsman (Συνήγορος του Πολίτη), who oversees the impact of

AI on citizens' rights and non-discrimination; the Hellenic Authority for Communication Security and Privacy (ΑΔΑΕ), who handles privacy in communications related to AI; the National Commission for Human Rights (ΕΕΔΑ), who monitors high-risk AI compliance with fundamental rights.

The Special Secretariat for AI and Data Governance, a new entity established in 2025 under the renamed Ministry of Digital Governance, oversees AI strategy. The High-Level Advisory Committee on Artificial Intelligence has been established in November 2023 under the Prime Minister's office to develop the national AI strategy ("A Blueprint for Greece's AI Transformation"); the Coordinating Committee for AI, established under Law 4961/2022, oversees the implementation of AI rules in both public and private sectors.

8. Final remarks

The reconstruction of the regulatory and organizational models followed by European Union member states in implementing the EU regulation on artificial intelligence (improperly referred to as the AI Act) at national level has already been outlined in the previous paragraphs, and re-presenting the categories into which they are divided here would risk becoming a tiresome repetition of previously delineated taxonomies. Rather, it is important to highlight some essential aspects that emerge from the analysis conducted above. These considerations may seem obvious, banal, and predictable, but they are nevertheless purposefully conceived to identify some interpretations of an extremely complex and diverse subject matter. The regulatory framework for this matter, first and foremost, is being drawn toward the Euro-unitary hub, shifting its essential center of gravity from the periphery (the States) to the center (the European legislator). This choice, while abstractly capable of denoting the Union's tendency to favor an anomalous expansion of its scope of regulatory powers (a phenomenon highlighted on a variety of sensitive fronts), appears justified by the need to define a comprehensive set of rules dedicated to artificial intelligence, aimed at regulating its development and use according to a risk-based approach, while also ensuring innovation, protection of fundamental rights, and the functioning of the internal market¹².

The impact on Member States is particularly significant, since the regulation—as a directly applicable act—imposes concrete obligations not only on businesses but also on national administrations, redefining institutional structures, public policies, and supervisory models¹³. In other words, this choice is designed to avoid regulatory divergences and obstacles to the internal market, and—since it was conceived based on the risks deriving from the use of artificial intelligence—to define a uniform framework of rules and principles aimed at protecting the fundamental rights of individuals affected by the operation of AI systems. This results in a significant reduction in Member States' regulatory autonomy in AI

¹² M. Kovač, *Generative Artificial Intelligence. A Law and Economics Approach to Optimal Regulation and Governance*, Berlin, 2025.

¹³ P. Ahrweiler, N. Gilbert (cur.), *Participatory Modelling and Simulation to Improve AI-based Public Social Services*, Berlin, 2026; L. Torchia, *Potere digitale*, Bologna, 2026.

matters, in the need to adapt existing legislation to avoid conflicts, and in a greater integration of digital policies at the European level¹⁴. These are developments that will merit positive appreciation if their purpose is demonstrated to foster greater legal certainty and a more uniform flow of judicial decisions. It cannot be denied that the proliferation of guidelines and, more generally, soft law, developed by national legal systems in implementing European legislation, may represent, in the long run, a critical factor in guaranteeing the fundamental corollaries of the rule of law, particularly in terms of the knowledge and publicity of rules, as well as the democratic nature of their development.

The implementation of the EU AI Act has led, as we have seen, to the creation of new institutional and multilevel governance structures, in which national sovereignty is balanced by strong European coordination mechanisms. While the institutional frameworks designed by EU Member States typically tend to identify a body within the executive branch (minister, ministerial committee) vested with the function of providing political direction and coordinating administrative activities in the field of artificial intelligence, there is systematic recourse to the establishment of independent administrative authorities or sector-specific agencies, which support the government with advisory functions, or perform fully autonomous supervisory, control, monitoring, and inspection functions, responsible for establishing and performing the procedure for assessment, designation, and notification of conformity assessment bodies and for their monitoring, as well as for enforcing the respect for fundamental rights obligations in Member States in relation to high-risk AI systems.

If national politics (broadly understood as legislators, parliaments or governments) is being given ample space, both in favor of the European Union legislature and in favor of soft law sources, the phenomenon of the repositioning of the center of governance from governments to independent administrative authorities and/or agencies, technical bodies with specific and high-level sectoral expertise, which are frequently given the additional role of monitoring and protecting fundamental human rights, appears no less significant. It is the shaping figure, not necessarily the sinister shadow as too many catastrophic visions seem to predict, that the science and technology project onto the law, on the substantive and organizational side¹⁵.

Luca Mezzetti
Università degli Studi di Bologna
luca.mezzetti@unibo.it

¹⁴ A. Gattini, *La tecno-sovranià nella prospettiva del diritto internazionale*, Turin, 2026.

¹⁵ L. Mezzetti, *Science, Law and Democracy*, in Idem (cur.), *Science, Technology and Law*, cit., 9-29.

