UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

Progress by innovation



Artificial Intelligence Conformity Assessment in Ukraine

CONVERGENCE WITH EUROPEAN UNION LEGISLATION

ACKNOWLEDGEMENT

This report has been prepared by the Centre for European Policy Studies (CEPS) for the United Nations Industrial Development Organization (UNIDO), within the project "*Supporting the reconstruction and development of industrial sectors in Ukraine by fostering digital transformation and the innovation ecosystem*", funded by the Governments of Austria and Bulgaria and implemented under the UNIDO Green Industrial Recovery Programme for Ukraine (2024–2028) in partnership with the Ministry of Economy, Environment and Agriculture of Ukraine and the Ministry of Digital Transformation of Ukraine. It forms part of a broader series of joint CEPS–UNIDO analytical outputs on artificial intelligence (AI), designed to support Ukraine's industrial reconstruction, digital transformation and alignment with the European Union *acquis* and accession process. For the purpose of the analysis of publicly available sources, the cutoff date of this report is August 2026.

This report contributes to UNIDO's work on digital transformation, artificial intelligence and innovation ecosystems and was prepared under the overall guidance of the UNIDO Division of Digital Transformation and Artificial Intelligence (TCS/DAI). The Division promotes digital transformation and artificial intelligence, as well as associated technologies, as part of innovation ecosystems encompassing productive capacities in manufacturing, services and digital firms, with the aim of advancing the competitiveness of industries and manufacturing firms in Member States.

This report has been prepared by **Mr. César Dro** and **Mr. Eduardo Brito** from the Centre for European Policy Studies (CEPS) under the overall guidance of **Mr. Nikolaus Martys**, Industrial Development Expert, UNIDO. The publication represents a collaborative effort and has benefited from valuable inputs from both UNIDO and CEPS colleagues. UNIDO and CEPS extend their sincere appreciation to project partners, national stakeholders and sector experts who provided insights, data and feedback throughout the preparation of this report.

www.unido.org

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION

© UNIDO 2026 - All rights reserved

This document has been produced without formal United Nations editing. The designations employed and the presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations Industrial Development Organization (UNIDO) concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries, or its economic system or degree of development.

Copyright ©2026 - United Nations Industrial Development Organization - www.unido.org
Images ©2026 - www.unido.org, http://stock.adobe.com

TABLE OF CONTENTS

Executive Summary 4

Introduction 5

1. The EU AI Conformity Assessment Regime 6
   - 1.1 A RISK-BASED ARCHITECTURE 8
   - 1.2 HIGH-RISK CONFORMITY ASSESSMENT ROUTES (AI ACT ARTICLE 43) 8
   - 1.3 STANDARDS AND THE PRESUMPTION OF CONFORMITY 10
   - 1.4 INSTITUTIONAL ARCHITECTURE 13
   - 1.5 GENERAL-PURPOSE AI OBLIGATIONS 14
   - 1.6 THE DIGITAL OMNIBUS ON AI 15
2. Current State of AI Governance in Ukraine 16
   - 2.1 STRATEGY AND POLICY LAYER 19
   - 2.2 LEGAL LAYER 21
   - 2.3 INSTITUTIONAL LAYER 23
   - 2.4 TECHNICAL STANDARDS LAYER 25
   - 2.5 ECOSYSTEM LAYER: PRIVATE SECTOR, ACADEMIA AND THE WINWIN GLOBAL INNOVATION STRATEGY TO 2030 26
   - 2.6 WARTIME CONSTRAINTS 28
   - 2.7 DUAL-USE AI AND THE CIVILIAN REGIME 30
3. Ukrainian AI Regulation in the New Legislative Framework 32
4. EU–Ukraine Gap Analysis 36
   - 4.1 GAP MATRIX 39
   - 4.2 CROSS-CUTTING GAPS 41
   - 4.3 SEQUENCING 42
   - 4.4 EU–UKRAINE IMPLEMENTATION CHANNELS: LESSONS FROM IP ALIGNMENT 42
   - 4.5 ANTICIPATING EU PRIORITIES AND UPCOMING LEGISLATION 43
5. The GPAI Code of Practice: Implications for Ukraine 44
6. Building AI Auditing Expertise in Ukraine 48
   - 6.1 BUILDING AI AUDIT ROLES 51
   - 6.2 WHAT AN AI AUDIT CURRICULUM SHOULD COVER 52
   - 6.3 INSTITUTIONAL HOME FOR CAPACITY-BUILDING 53
   - 6.4 PUBLIC-PRIVATE COORDINATION AND CAPACITY-BUILDING 53

Conclusions and Recommendations 54

References 56

Acronyms 61

Executive Summary



Ukraine has committed itself to joining the European Union, and this has implications for its approach to AI regulation. The EU AI Act, in force since August 2024, makes conformity assessment the operational core of AI regulation and, as part of the EU *acquis*, part of the conditionality attached to Ukraine's accession path and to the Ukraine Facility. The Digital Omnibus on AI, agreed by the co-legislators in May 2026 and formally adopted in June 2026, defers the application of high-risk obligations to 2 December 2027 (stand-alone systems) and 2 August 2028 (systems embedded in products). For Ukraine, this opens a 12- to 16-month implementation-readiness window in which to prepare.

This report examines what EU-compatible AI conformity assessment requires and where Ukraine currently stands. Three findings emerge. First, in the EU regime most high-risk obligations are discharged through provider-side internal control rather than third-party certification; harmonised standards, led by CEN-CENELEC JTC 21, determine how legal requirements become auditable, and Ukraine has been tracking the development of these standards with an objective of direct implementation. Second, Ukraine's staged strategy of starting with voluntary ecosystem preparation before adopting binding EU-aligned legislation is sound for an accession country, and its technical-regulation, accreditation and standardisation infrastructure offers a usable backbone. Third, the binding gaps are mainly institutional and operational: there is no independent data-protection authority, no designated AI supervisory architecture, uncertainty over the timely delivery of the planned Single Digital Regulator, and a thin pool of AI audit expertise, all under wartime constraints and a complex civilian/dual-use boundary.

The report recommends using 2026–2027 to further build enforceability before legislating: complete data-protection reform, further standards-tracking and mirroring, develop a national AI audit curriculum, define a civilian interface for dual-use AI, prepare a fallback option for AI supervision should the Single Digital Regulator be delayed, maintain the NPAA timeline for the legislative phase, map and then update sectoral AI Act conformity assessment readiness, both legislative and in infrastructure, to anticipate the EU's own sectoral legislation updates, anticipate upcoming EU digital priorities and organise AI alignment as an implementation partnership with EU bodies.

Introduction

The European Union (EU) Artificial Intelligence (AI) Act entered into force on 1 August 2024 and was the world's first comprehensive horizontal AI law (European Parliament and Council of the European Union 2024). Its rules related to high-risk AI applications rely on **conformity assessment**: a procedure derived from EU product-safety law and used to define auditable obligations on providers and deployers of high-risk AI systems, and on providers of general-purpose AI models. For general-purpose AI (GPAI) models (unless they are classified as posing a systemic risk), it focuses on **technical documentation, transparency, copyright compliance and a training-data summary**. For Ukraine, two factors make this legislation immediately relevant for its own AI framework:

1 **ACCESSION CONDITIONALITY**

Ukraine has been a candidate country for accession to the European Union since 2022. The Commission's Ukraine Report 2025 assesses digital transformation as being "between a moderate and a good level of preparation", but specifically flags institutional gaps that bear directly on AI supervision – notably the absence of an independent data-protection supervisory authority1 and limited horizontal market-surveillance capacity (European Commission 2025). The Ukraine Plan 2024–2027 (Government of Ukraine 2024) makes "digital transformation" one of three cross-cutting priorities tied to the disbursement of the €50 billion Ukraine Facility (The Ukraine Facility - European Commission 2026). Since the entry into force of the AI Act, AI conformity assessment is part of the EU *acquis* on which this conditionality is based.

2 **EVOLVING LEGISLATION**

In June 2026, the European Parliament and Council adopted the Digital Omnibus on AI as part of a wider simplification package for the EU digital *acquis* (Niestadt 2026; European Council 2026b), setting a revised implementation timeline for the application of high-risk AI rules. Under the agreed direction, stand-alone high-risk AI systems would become subject to the relevant obligations on 2 December 2027, while high-risk AI systems embedded in products covered by EU sectoral safety legislation would follow a later date, 2 August 2028 (European Council 2026a).

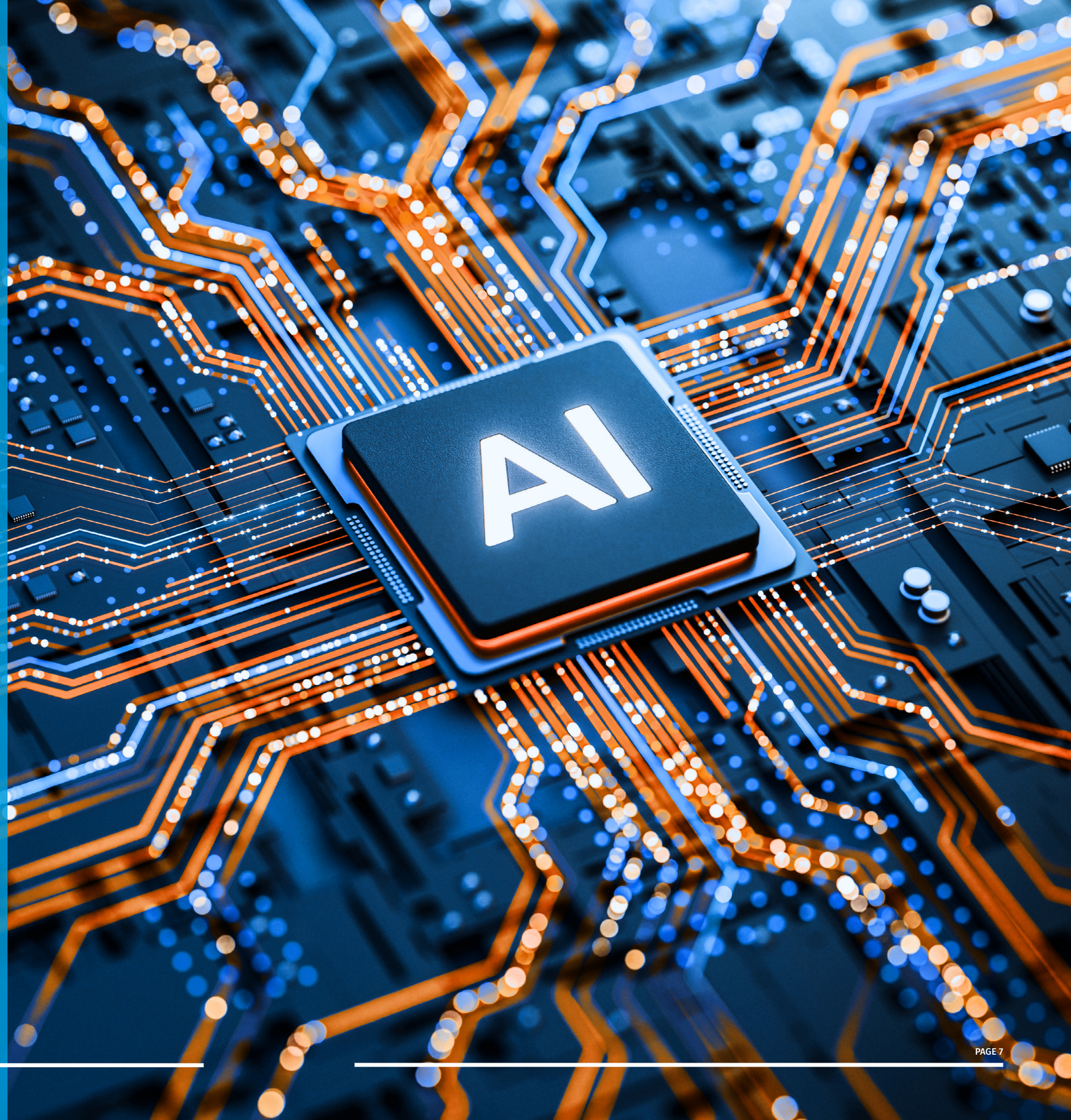
The latter point has a strategic implication for the Ukrainian legislative timeline: as the political agreement confirms a deferral of the obligations for providers of high-risk AI systems (16 months for Annex III stand-alone high-risk systems, 12 months for Annex I product-embedded high-risk AI systems and sandboxes), for Ukraine this means 12–16 additional months to set up the related institutional architecture and enforcement capabilities. In practice, this means shoring up standards-tracking capacity, audit skills, sandbox design, sectoral conformity assessment pathways and supervisory functions that will be needed once AI Act alignment becomes formally testable in EU accession and market access contexts. Other EU initiatives now in preparation that Ukraine should anticipate are discussed in Section 4.5.

1) This role is currently performed by the Ukrainian Parliament Commissioner for Human Rights (Ombudsman): https://ombudsman.gov.ua/en

1

The EU AI Conformity Assessment Regime

AI conformity assessment cannot be prepared only through a future horizontal AI law. It also requires sectoral readiness in areas such as medical devices, transport, critical infrastructure, radio equipment and other regulated product domains, where AI-related requirements may need to be integrated into existing technical regulation, accreditation, notification and market-surveillance practices.



1.1 A RISK-BASED ARCHITECTURE

Because the AI Act is risk-based, its provisions are intended to be proportionate to the level of risk posed by a given AI application. Risk here refers essentially to fundamental rights, to the safety of people and infrastructure and, in the case of general-purpose artificial intelligence (GPAI) models, to systemic risk.

The AI Act tiers AI systems into "Unacceptable risk" (prohibited), "High-risk", "Limited-risk" and "Minimal-risk" categories, coupled with a parallel regime for general-purpose AI (GPAI) models, with systemic-risk GPAI as a sub-tier (described in Articles 51 to 55; European Parliament and Council of the European Union 2024).

Within this framework, the compliance burden falls mainly on two groups: providers of high-risk systems, which must follow the conformity assessment routes set out in Article 43 of the AI Act; and providers of GPAI models presenting systemic risk, which must meet the obligations set out in Articles 53 and 55 respectively.

1.2 HIGH-RISK CONFORMITY ASSESSMENT ROUTES (AI ACT ARTICLE 43)

Under Article 43 of the AI Act, two routes coexist for the compliance assessment of high-risk AI systems:

1. **INTERNAL CONTROL (ANNEX VI)**

   The provider carries out a self-assessment of the system against the relevant requirements (risk management, data governance, technical documentation, logging, transparency, human oversight, accuracy, robustness, cybersecurity and post-market monitoring). This is the default route for stand-alone high-risk AI systems listed in Annex III points 2–8 (critical infrastructure, education, employment, essential services, law enforcement, migration, justice and democratic processes).

2. **NOTIFIED-BODY INVOLVEMENT (ANNEX VII)**

   Conformity is established through an assessment of the quality management system and of the technical documentation, with the involvement of a national notified body.[2] This is especially relevant for AI systems with applications in biometrics (Annex III point 1), where the provider can choose between the Annex VI and Annex VII routes only if harmonised standards or common specifications exist and have been fully applied; otherwise Annex VII (third-party) applies.

2) A Notified Body is a conformity assessment body notified in accordance with this Regulation and other relevant European Union harmonisation legislation (AI Act, Article 3(22)) and delivers certificates for AI systems. Such bodies must be legal entities established under the national law of an EU Member State, must be independent of any AI provider and must be able to perform their tasks as AI conformity assessors in accordance with Article 31.

For high-risk AI systems embedded in products already subject to sectoral CE-marking[3] regimes (machinery, medical devices, in-vitro diagnostic medical devices, etc.), the conformity assessment follows the relevant sectoral route, with AI Act requirements integrated into that sectoral assessment.

The integration of AI safety into sectoral safety practices is therefore not a purely horizontal AI compliance problem: where sectoral product-safety legislation applies, AI Act requirements interact with existing CE-marking and conformity assessment routes. For Ukraine, this means that AI conformity assessment cannot be prepared only through a future horizontal AI law. It also requires sectoral readiness in areas such as medical devices, transport, critical infrastructure, radio equipment and other regulated product domains, where AI-related requirements may need to be integrated into existing technical regulation, accreditation, notification and market-surveillance practices. This aspect, however, is not urgent, as the EU itself has yet to make the necessary updates to most of its sectoral legislation. Machinery is a notable exception to this parallel application: following the Digital Omnibus, machinery is exempted from the direct application of the AI Act, and AI-related health and safety requirements are to be added through delegated acts under the Machinery Regulation (Regulation (EU) 2023/1230), which therefore prevails over the AI Act for AI embedded in machinery (European Parliament and Council of the European Union 2026). For Ukraine, AI requirements for machinery will therefore be introduced through the update of that technical regulation to the Machinery Regulation and its delegated acts, and the future Ukrainian horizontal AI law and its sectoral legislation on machinery should reflect this carve-out. Overall, most of the obligations for providers of high-risk AI systems in the EU are operationally discharged through self-assessment rather than third-party certification. This is the most important pivot point for Ukraine: building credible AI conformity assessment is primarily a question of equipping providers and deployers with auditable internal processes, and only secondarily about standing up notified bodies. The notified-body track matters, but

Ukraine's early capacity-building should focus on documentation, risk management, quality management, data governance, post-market monitoring and procurement-side due diligence.

for a narrower set of cases and with a much heavier institutional burden. This also means that Ukraine's early capacity-building should focus on documentation, risk management, quality management, data governance, post-market monitoring and procurement-side due diligence, rather than treating notified-body designation as the first priority (European Commission 2022).



3) *The European Economic Area legal safety standards ("Conformité Européenne" – CE).*

1.3 STANDARDS AND THE PRESUMPTION OF CONFORMITY

The European Committee for Standardisation and the European Committee for Electrotechnical Standardisation Joint Technical Committee 21 on Artificial Intelligence (CEN-CENELEC JTC 21) is developing the harmonised standards intended to support implementation of the EU AI Act. Its work covers areas such as AI trustworthiness, risk management, quality management, conformity assessment, data governance, bias, robustness, cybersecurity, logging, transparency and related implementation topics (European Commission 2026). Once relevant harmonised standards are cited in the Official Journal of the European Union, compliance with those standards can support the AI Act's presumption of conformity. The June 2025 JTC 21 overview (Krog 2025) showed a substantial delay in the delivery of the standards; the CEN/CENELEC Boards adopted in October 2025 an acceleration package to deliver the standards by Q4 2026 (CEN-CENELEC JTC21 2025). The first deliverable of that package, EN 18286:2026 – AI quality management system for EU AI Act regulatory purposes, was delivered in June 2026 (CEN - CEN/CLC/JTC 21 2026). The full package includes several other standards, to be delivered in 2026–2027 and summarised in Table 1 (CEN-CENELEC JTC 21 2026).



TABLE 1: Mapping of AI conformity dimensions to relevant standards and their importance for the alignment of Ukrainian AI legislation with the EU framework

AI Act implementation need	Relevant standards / pathway	Why it matters for Ukraine
Risk management	EN ISO/IEC 23894 - AI Risk Management Guidance (published); ISO/IEC risk-management standards.	Converts high-level risk obligations into auditable processes for providers and deployers.
Quality management	EN 18286:2026 Quality management system for EU AI Act regulatory purposes; ISO/IEC 42001:2023 - AI management systems.	Supports internal control, documentation, governance and continuous improvement.
Data governance	EN ISO/IEC 5259-1 to 5259-4 Artificial intelligence - Data quality for analytics and machine learning (published); CEN/CLC ISO/IEC/TR 24027:2023; Information technology - Artificial intelligence (AI) - Bias in AI systems and AI-aided decision-making (published).	Supports compliance for high-risk systems relying on training, validation and testing data.
Transparency and documentation	prEN ISO/IEC 24970 Artificial intelligence - AI system logging (under enquiry); EN ISO/IEC 12792:2025 Information technology - Artificial intelligence (AI) - Transparency taxonomy of AI systems (published); prEN 18229-1 and 18229-2 AI trustworthiness framework (logging and transparency; under enquiry), technical documentation and record-keeping.	Creates evidence trails for providers, auditors, regulators and public buyers.
Human oversight	prEN 18229-3 and 18229-4 AI trustworthiness framework (human oversight and accuracy; under enquiry); Standards and guidance on oversight, controllability and human-system interaction.	Helps translate legal duties into operational design, deployment and monitoring controls.
Accuracy, robustness and cybersecurity	CEN/CLC ISO/IEC/TR 24029-1:2023 Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview (ISO/IEC TR 24029-1:2021; published); adjacent cybersecurity certification pathways where applicable.	Supports resilience in the context of the war against Russia, accuracy and Article 15 cybersecurity expectations.
Conformity assessment	CEN/CLC/TR 17894:2024 Artificial Intelligence - Artificial Intelligence Conformity Assessment (published); prCEN/CLC/TR 18347 - Overview and architecture of standards in support of the EU AI Act (under drafting); New Legislative Framework (NLF)/ Blue Guide logic.	Helps define how internal control and third-party assessment should be evidenced and reviewed.

Ukraine should also track adjacent certification pathways. Under AI Act Article 42(2), high-risk AI systems certified, or covered by a statement of conformity, under a recognised EU cybersecurity scheme pursuant to the ENISA Regulation (Regulation (EU) 2019/881) may be presumed to comply with the AI Act's Article 15 cybersecurity requirements, but only insofar as the certificate or statement of conformity actually covers those requirements (European Parliament and Council of the European Union 2024). This makes schemes such as the European Common Criteria-based Cybersecurity Certification Scheme (EUCC) relevant as possible cybersecurity certification pathways. For Ukraine, the practical implication is that AI standards-tracking should be coordinated with cybersecurity certification and accreditation policy, especially for high-risk AI systems deployed in security-sensitive or regulated sectors.

Standards readiness appears to be key to articulating legal alignment and operational conformity assessment. The current delay by CEN-CENELEC in delivering the standards can be assumed to be one reason for the

Standards readiness appears to be key to articulating legal alignment and operational conformity assessment.

Omnibus deferral. Without harmonised standards, presumption of conformity is unavailable or incomplete; without presumption of conformity, both self-assessment and notified-body routes become more discretionary, costly and legally uncertain. Ukraine's alignment work should therefore track CEN-CENELEC JTC 21 outputs, corresponding ISO/IEC standards, and adjacent cybersecurity certification pathways at least as closely as the AI Act text itself, and ensure their timely transposition into its national standards (DSTU).

Ukraine's alignment work should track CEN-CENELEC JTC 21 outputs.



1.4 INSTITUTIONAL ARCHITECTURE



EU governance is by nature multi-level, and the EU AI governance regime is no exception. At the EU level, the AI Office supports implementation and supervises general-purpose AI obligations; the AI Board coordinates Member State authorities; and national market-surveillance authorities in Member States are responsible for supervising and enforcing obligations relating to standard and high-risk AI systems. In parallel, notified bodies in each Member State may be designated for specific conformity assessment tasks and national accreditation bodies assess the competence of those bodies, while market-surveillance authorities operate under the broader EU product-safety and market-surveillance framework. This institutional stack reflects the NLF logic: essential requirements, harmonised standards, presumption of conformity, conformity assessment, CE marking and post-market surveillance (European Commission 2022).

For Ukraine, the institutional lesson is that AI conformity assessment cannot be assigned to a single body in isolation. It will require coordination between the future AI supervisory authority, the data-protection authority, the national accreditation infrastructure, sectoral market-surveillance authorities, public procurement actors and technical-testing capacity, as well as standards bodies (notably by using the status of affiliate body to CEN-CENELEC acquired in 2023 by the Ukrainian Scientific, Research and Training Center on Standardization, Certification and Quality Problems (UkrNDNC)).[4]

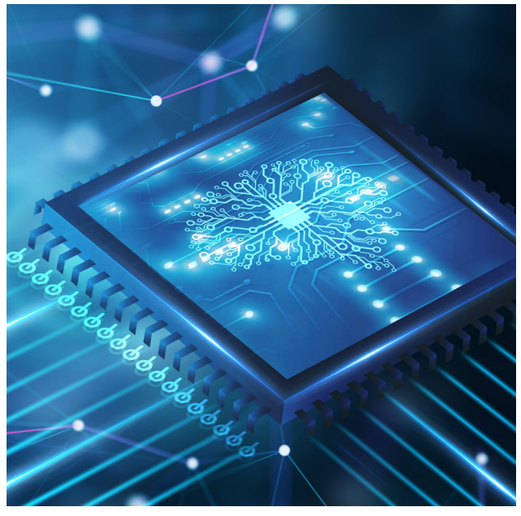
4) UkrNDNC is the Ukrainian national body for standardisation and certification; see section 2.4 on the Ukrainian technical and standards layer.

1.5 GENERAL-PURPOSE AI OBLIGATIONS

GPAI obligations apply to model providers, rather than to downstream deployers. The GPAI Code of Practice, finalised on 10 July 2025 and endorsed by the Commission and the AI Board on 1 August 2025, operationalises Articles 53–55 through three chapters: Transparency, Copyright, and Safety and Security (the last applies only to providers of systemic-risk GPAI under Article 55; European Commission 2025; European Parliament and Council of the European Union 2026). Adherence is voluntary; under Articles 53(4) and 55(2), with Article 56 establishing the framework for codes of practice, providers that adhere to an approved Code of Practice may rely on it as an adequate means of demonstrating compliance with their Article 53 (and, where relevant, Article 55) obligations, pending the publication of harmonised standards (European Commission 2025).

Ukraine's near-term GPAI exposure is mainly deployer-side, as it does not currently appear to host a general-purpose AI model provider in the systemic-risk tier, but provider-side exposure is already emerging: in 2025 the Ukrainian government launched a state infrastructure for AI development, the AI Factory, together with efforts to build a national large language model (LLM; European Commission 2025). GPAI models are currently being trained using large-scale compute on Ukrainian infrastructure, for use by the general population and for commercial purposes, while the Ukrainian government has issued no recommendation or regulation on how these models should address data protection or systemic risks(Digital State Ukraine 2026). A large part of its immediate exposure will nonetheless arise through public-sector procurement, integration and deployment of GPAI models developed by EU, US or other foreign providers. Near-term policy should focus on deployer-side risk management, transparency in public-sector use, contractual due diligence, access to provider documentation where available, and procurement clauses that require sufficient information on model capabilities, limitations, data governance and safety practices. As Ukraine's sovereign AI and national LLM initiatives build provider-side GPAI capacity, this focus should be complemented by guidance for domestic model providers on data protection, transparency and systemic-risk management, drawing on the GPAI Code of Practice. Should Ukraine join the European Union, these rules would fall under the AI Office, and early compliance capacity would make the transition easier. Until accession, a Ukrainian authority would need to perform the monitoring and supervisory functions that the AI Office exercises in the EU, and should prepare from the outset to hand these functions over to the AI Office once Ukraine joins the Union (see Section 2.3).

> **Near-term policy should focus on deployer-side risk management, transparency in public-sector use, contractual due diligence, access to provider documentation where available, and procurement clauses that require sufficient information on model capabilities, limitations, data governance and safety practices.**



1.6 THE DIGITAL OMNIBUS ON AI



Beyond the deferral discussed in the introduction, the Digital Omnibus on AI is relevant for Ukraine because it changes the implementation environment around the AI Act. The adopted text broadly maintains the Commission's proposal to delay high-risk AI obligations until the necessary standards and tools are available, while also introducing fixed application dates: 2 December 2027 for stand-alone high-risk AI systems and 2 August 2028 for high-risk AI systems embedded in Annex I regulated products (European Council 2026). It also postpones the deadline for national regulatory sandboxes to 2 August 2027, clarifies the AI Office's role in supervising certain AI systems based on general-purpose AI models, and adds a new prohibition on AI practices involving the generation of non-consensual intimate content or child sexual abuse material (European Council 2026).

The Omnibus is also important for sectoral product regulation. The provisional agreement addresses overlaps between the AI Act and sectoral legislation in areas such as medical devices, toys, lifts, machinery and watercraft. In particular, the Council states that the compromise allows the EU to limit overlapping AI Act requirements where sectoral law already contains similar AI-specific requirements, and that machinery is exempted from direct applicability of the AI Act, with AI-related health and safety requirements to be instead added through delegated acts under the Machinery Regulation (European Council 2026).

For the purposes of this report, the adoption signals that the entry into force of the rules containing obligations for high-risk AI system providers is being delayed because standards, tools, guidance and assessment infrastructure are not yet mature enough. This reinforces the case for Ukraine to treat 2026–2027 as a short preparation period for institutional and technical readiness.

> **The entry into force of the rules containing obligations for high-risk AI system providers is being delayed because standards, tools, guidance and assessment infrastructure are not yet mature enough.**

2

Current State of AI Governance in Ukraine

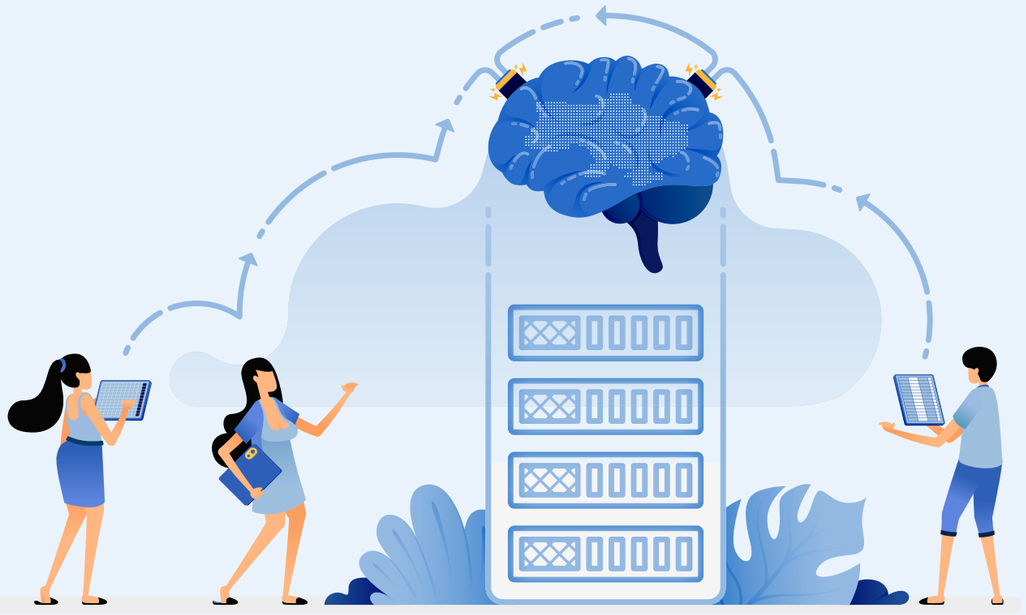
Ukraine’s AI governance landscape is developing through a combination of policy strategy, voluntary regulatory tools, innovation programmes and EU-alignment commitments. Its approach is based on staged preparation, broadly consistent with Ukraine’s accession context and with the current delay in EU high-risk AI implementation.



Ukraine's AI governance landscape is developing through a combination of **policy strategy**, **voluntary regulatory tools**, **innovation programmes** and **EU-alignment commitments**.

Its approach is based on **staged preparation**: first, voluntary guidance, business-readiness tools and sandboxing; and, in a second step, EU-aligned legislation (Ukraine Ministry of Digital Transformation 2024b).

This sequencing is broadly **consistent with Ukraine's accession context** and with the **current delay in EU high-risk AI implementation**, but it also creates a practical test: beyond policy statements, the preparatory stage must produce operational capacities for the framework to function.



2.1 STRATEGY AND POLICY LAYER



Ukraine's first national AI policy framing was the Concept on AI Development in Ukraine, approved by Cabinet of Ministers Directive No. 1556-r in December 2020 (Cabinet of Ministers of Ukraine 2020). The Concept set an early strategic direction for the development of AI in Ukraine, before the EU AI Act and before the current accession-driven phase of regulatory alignment.

The more relevant regulatory baseline is the Roadmap for the Regulation of AI in Ukraine, presented by the Ministry of Digital Transformation (MoDT) and the Expert Committee on AI Development in October 2023 (Ukrainian Ministry of Digital Transformation 2023). The Roadmap adopts a bottom-up approach: it seeks to prepare the AI ecosystem through voluntary tools, self-regulation, business-readiness measures and guidance before introducing binding legislation aligned with the EU AI Act. Its stated objective is to create a safe environment for AI, help Ukrainian businesses remain competitive and support Ukraine's integration into the EU (OECD 2025).

The White Paper on AI Regulation, published by the MoDT in June 2024, operationalises this staged model (Ukraine Ministry of Digital Transformation 2024b). It elaborates the first stage of the Roadmap and discusses voluntary instruments such as regulatory sandboxes, labelling, codes of conduct, recommendations and sectoral guidance. Its rationale is that Ukrainian businesses and public institutions should begin preparing for future AI regulation before a binding AI law is adopted.

In parallel, the WINWIN Global Innovation Strategy to 2030 (WINWIN) frames AI as one of Ukraine's strategic innovation priorities (Ukraine Ministry of Digital Transformation 2026b). Developed by the Ministry of Digital Transformation together with other institutions and international partners, it is described as a national innovation strategy. In this context, Ukraine has launched the WINWIN AI Centre of Excellence, presented as a national platform for AI development and integration across government, business and society, including

public administration, defence, healthcare, education and business (Ukraine Ministry of Digital Transformation, 2025). A Sectoral Analysis and Initial Vision for AI Development under WINWIN was presented in 2025, with Ukraine as a regional hub for AI testing, through the Centre of Excellence. The Vision identifies the lack of a clear regulatory framework for AI as a source of potential conflicts with EU standards as a threat that needs to be addressed (Ukraine Ministry of Digital Transformation 2025a).

Ukraine's AI governance strategy is sequenced around voluntary preparation ahead of the enactment of binding law. Ukraine's Roadmap, White Paper and Responsible AI materials point to a staged regulatory model: first prepare the ecosystem through voluntary tools, guidance, recommendations and sandboxing; then move toward EU-aligned binding legislation. This remains a sound posture for an accession country, especially given the deferral of EU high-risk AI obligations. The key risk is not the sequencing itself, but whether the preparatory stage produces concrete implementation deliverables: standards mapping, procurement guidance, audit training, sandbox methodology, institutional design options and sectoral readiness. With the Cabinet of Ministers Resolution No. 438 of 1 April 2026, a National Programme for the Adaptation of Ukrainian Legislation to the law of the European Union (or *Adoption of the acquis*, NPAA) was approved. It contains a comprehensive list of EU legal acts to be implemented in Ukrainian legislation and establishes an institutional and legal framework for the systematic implementation of reforms and the full alignment of Ukrainian legislation with EU law (Ukrainian Government 2026).

Ukraine's AI governance strategy is sequenced around voluntary preparation ahead of the enactment of binding law.

According to official sources, Ukraine is currently starting to prepare Stage 2 AI legislation with a draft law similar to the AI Act (OECD 2026) as defined by the NPAA. The work is led by the Ministry of Digital Transformation, together with other stakeholders (Parliament, experts and academia), within an established working group. The draft law is scheduled for submission to the Verkhovna Rada (Ukrainian Parliament) in the fourth quarter of 2026, and according to the NPAA Chapter 10, to be adopted by January 2028 (Ukrainian Government 2026). Ukraine's adoption date therefore falls between the two EU application dates confirmed by the Digital Omnibus (after 2 December 2027 for stand-alone high-risk systems and before 2 August 2028 for product-embedded systems). According to the official sources cited above, the law is projected to incorporate transitional provisions (typically two to three years) to give Ukrainian tech companies time to achieve full compliance prior to Ukraine's planned integration into the EU Single Market.

According to official sources, Ukraine is currently starting to prepare Stage 2 AI legislation with a draft law similar to the AI Act (OECD 2026) as defined by the NPAA.



2.2 LEGAL LAYER



Ukraine's legal baseline for AI conformity assessment is fragmented. There is no binding horizontal AI law yet, but several adjacent legal frameworks already shape the conditions for future AI governance, especially data protection, human-rights-based AI governance, and technical regulation.

On data protection, the Draft Law No. 6177 aimed to establish an independent supervisory authority for personal data protection and access to public information, but has not yet reached a first reading (Ukrainian Verkhovna Rada 2026). A companion law, Draft Law No. 8153 "On Personal Data Protection"[5] was adopted in first reading on 20 November 2024 and is intended to align Ukraine's data-protection framework more closely with the GDPR (Ukrainian Verkhovna Rada 2026).[6] These reforms are directly relevant to AI conformity assessment because high-risk AI systems depend on lawful data governance, accountability, impact assessment and effective oversight. They have, however, undergone significant changes since their first drafts and, while delayed owing to the Russian invasion, are, according to official sources, currently being reactivated for consideration in the Verkhovna Rada based on feedback from human rights defenders, business associations, and the European Commission's Enlargement Reports.

5) An earlier Draft Law No. 5618 "On Personal Data Protection" was rejected in 2022 (Ukrainian Verkhovna Rada 2026).

6) *"First reading"* (sometimes translated as "adopted as a basis") in the Ukrainian legal system means that the broad objective and structure of the law have been approved by the Verkhovna Rada, and that the law will then be redrafted and amended until the second (and possibly third and final) reading.

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) was opened for signature on 5 September 2024 and is the first international legally binding treaty in the AI field (Council of Europe 2024a; Council of Europe 2024b). Ukraine signed the Convention on 15 May 2025, but had not ratified it at the time of writing (Council of Europe 2026b). The signature is already relevant as a signal of Ukraine's commitment to human-rights-based AI governance, but, as the European Union has ratified the treaty, ratification will also be required as part of the EU *acquis*.

The Council of Europe frameworks are also useful for Ukraine because of the resources they have generated, notably the Methodology for assessing the risks and impacts of artificial intelligence systems from the perspective of human rights, democracy and the rule of law (HUDERIA; Council of Europe 2026a). For Ukraine, this rights-based assessment tool complements AI Act-style conformity assessment, especially in public-sector and high-risk deployments.

Ukraine's Law "On Technical Regulations and Conformity Assessment" provides the general legal backbone for technical regulation and conformity assessment, including provision for convergence with European Union legislation (Ukrainian Verkhovna Rada 2015). This means that AI conformity assessment can potentially be layered onto existing EU NLF structures, including accreditation, designated conformity assessment bodies (CABs) and sectoral market surveillance. While the law develops a comprehensive conformity assessment framework, it will require AI-specific operationalisation.

It must be noted that the scope of the planned AI law as stated in the NPAA appears to be narrower than the AI Act itself.[7] Objective 36 of the NPAA describes the law as implementing the provisions of Regulation (EU) 2024/1689 "in particular as regards the definition and classification of AI systems, taking account of risk categories" and "the prohibition of unacceptable practices and a clear list of prohibited AI applications". Conformity assessment procedures, notified bodies, the presumption of conformity through harmonised standards, market surveillance, post-market monitoring, serious-incident

It must be noted that the scope of the planned AI law as stated in the NPAA appears to be narrower than the AI Act itself.

reporting, regulatory sandboxes and general-purpose AI obligations do not appear to be mentioned in the objective, nor addressed elsewhere in the Programme in an AI context. On the face of the Programme, Ukraine has therefore committed to transposing the classificatory and prohibitive core of the AI Act. However, its conformity assessment machinery is equally important to ensure the compliance of AI and GPAI providers. If the drafting focuses on the provisions mentioned in the Programme without implementing the conformity assessment, the operational core of the AI Act might fall outside the Stage 2 law and would need to be carried either by a second legislative instrument or by secondary technical regulation under the Law "On Technical Regulations and Conformity Assessment". Clarifying this scope question is crucial to ensure a direct implementation of the EU *acquis* in the context of Ukraine's AI legislative convergence with the EU.

A future AI supervisory authority will lack credibility if the data protection authority remains structurally weak or non-equivalent to EU expectations.

Data-protection reform is a precondition for credible AI conformity assessment. Ukraine cannot operationalise EU-aligned AI conformity assessment without completing data-protection reform. Draft Law No. 8153 and the institutional reform envisaged under Draft Law No. 6177 are relevant not only for general GDPR approximation, but also for AI Act-style obligations on data governance, biometric processing, sensitive data safeguards, bias detection and mitigation, impact assessment and supervision. This is all the more relevant given that the initially planned date for adoption of the laws was June 2026, which has now lapsed (Ukrainian Government 2026). A future AI supervisory authority will lack credibility if the data-protection authority remains structurally weak or non-equivalent to EU expectations.

7) This assessment is based on an automated translation of the original Ukrainian text, which is available at: www.kmu.gov.ua/npas/pro-zatverdzhennia-natsionalnoi-prohramy-adaptatsii-zakonodavstva-ukrainy-do-prava-t10426

2.3 INSTITUTIONAL LAYER



The Ukrainian government has shown policy initiative on AI but does not yet have a formal AI supervisory architecture. The Ministry of Digital Transformation leads the AI regulatory roadmap, Responsible AI work, and WINWIN-related initiatives, while the Expert Committee on AI Development provides advisory capacity rather than enforcement powers (Ukraine Ministry of Digital Transformation, 2026). The Office of the Ukrainian Parliament's Commissioner for Human Rights currently supervises personal data protection, but Ukraine does not yet have a fully independent data-protection authority equivalent to those of EU Member States. Existing accreditation, conformity assessment and market-surveillance bodies may provide part of the future implementation backbone, but they do not yet have an AI-specific mandate. Draft Law No. 6177 would establish an independent statutory authority – the National Commission for Personal Data Protection and Access to Public Information – transferring oversight away from the current Ombudsman's Office to meet EU requirements for independent enforcement (Ukrainian Verkhovna Rada 2021).

Ukraine's main institutional gap is the absence of an enforceable AI conformity assessment architecture. Ukraine has AI policy coordination, advisory structures, general accreditation infrastructure and interim data-protection supervision, but is missing a legally designated and operationally capable architecture for AI supervision, standards coordination, sandbox oversight, post-market monitoring and enforcement. According to the NPAA Chapter 10, Objective 15, a Law establishing a Single Digital Regulator of Ukraine should be in force by January 2028, with the regulator to be launched and functioning within nine months of that law's entry into

Ukraine's main institutional gap is the absence of an enforceable AI conformity assessment architecture.

force to implement acts such as the one establishing the European AI Office. The intended remit of the new regulator covers electronic communications and digital services "and, subsequently, artificial intelligence" (Ukrainian Government 2026).

The regulator's remit, as proposed by the Programme, could pose problems of design. Firstly, the AI mandate is sequenced after the digital-services mandate rather than alongside it, so AI supervision may arrive later than the AI law itself. Secondly, a digital regulator built around platform and communications regulation is not, on its own, an AI Act Article 70 market-surveillance authority: the AI Act's supervisory model relies on sectoral market-surveillance authorities and a notifying authority (European Parliament and Council of the European Union 2024), which would be under the remit of the Ministry of Economy in Chapter 1 of the Programme, not under the digital regulator. While the actual scope of the envisioned digital regulator and its coordination mechanisms with the market-surveillance authorities remains to be seen in the actual draft of the law, this issue should be addressed from its inception.

Stakeholders consulted for this report stressed that the creation of regulatory authorities is a major issue extending well beyond AI. Alignment with the EU digital *acquis* requires regulatory capacity in around ten fields, from data to education and copyright law, and Ukraine will need to set up or designate an authority with adequate powers and expertise for each of them. AI legislation therefore cannot be assessed in isolation: it needs to be aligned with the other reforms under way, such as those on data protection, the free flow of data and the Data Act.

The delivery of the Single Digital Regulator within the NPAA timeline is uncertain. The timeframe is very short, and the regulator would have to be built from scratch, including its mandate, staff and procedures. Ukraine should therefore prepare for a scenario in which the Single Digital Regulator is not operational in time to apply the aligned legislation. Given the financial and staffing constraints on the state, one option would be to empower an existing body, such as the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services (NCEC), especially for monitoring and enforcement. The infrastructure capacity needed for AI supervision will have to be built in either scenario.

A further challenge concerns the allocation of powers. After accession, a significant share of supervisory powers, such as those of the European Commission and the AI Office over GPAI models, will be exercised at EU level. Until then, these functions will need to be performed by a Ukrainian authority, which should be designed from the outset to hand them over to the AI Office once Ukraine joins the EU. This arrangement is complex and could significantly expand the powers of national market-surveillance authorities during the pre-accession period, which calls for safeguards against potential abuses of power.

While the actual scope of the envisioned digital regulator and its coordination mechanisms with the market-surveillance authorities remains to be seen in the actual draft of the law, this issue should be addressed from its inception.

Several practices could support this institutional build-up. Chief Digital Transformation Officers (CDTOs), already present across Ukrainian public institutions, could help develop the Single Digital Regulator and deploy regulatory sandboxes (Roman 2026). Direct exchanges and twinning arrangements with authorities in EU Member States such as Austria and Bulgaria would allow Ukrainian authorities to exchange practices with their EU counterparts. A cost assessment of the creation of AI supervisory structures under the AI Act can inform the expected cost of regulation on Ukrainian entrepreneurs (European Commission 2021), and the United Kingdom's Digital Regulation Cooperation Forum offers a model of cooperation between digital regulators (Digital Regulation Cooperation Forum 2023). Ukraine's progress in agentic government also positions it to take a creative, trailblazing approach to the design of its supervisory institutions (Ionan 2026). More broadly, progress in good governance and in the quality of institutions will condition the credibility of any new authority.

2.4 TECHNICAL STANDARDS LAYER



As mentioned before, the SE UkrNDNC performs the functions of Ukraine's national standards body and is recognised at national, European and international levels (ISO 2026). Ukraine has historically adopted international and European standards into the DSTU system, which creates a channel through which ISO/IEC and CEN-CENELEC outputs can be incorporated into the national technical framework.

For AI conformity assessment, the critical question is whether this standards channel is being used systematically for AI Act alignment. CEN-CENELEC JTC 21 is developing European AI standards, including harmonised standards in support of the EU AI Act, while ISO/IEC 42001 provides a certifiable international framework for AI management systems. According to official sources, UkrNDNC tracks CEN-CENELEC JTC 21 and ISO/IEC JTC 1/SC 42 (Artificial Intelligence) outputs through national technical committees (such as TC 20 "Information Technologies"). UkrNDNC has been adopting key foundational standards – most notably ISO/IEC 42001 (Artificial Intelligence Management Systems - AIMS) and ISO/IEC 23894 (AI Risk Management) into the national system as DSTU standards.

Ukraine needs to continue its dedicated AI standards-tracking and mirroring work. Standards will determine how AI Act requirements become auditable in practice. Ukraine should therefore maintain and strengthen its structured mechanism to track CEN-CENELEC JTC 21 work, relevant ISO/IEC standards, ISO/IEC 42001 implementation, and adjacent cybersecurity certification pathways, and implement these in time to submit its application for full membership to CEN-CENELEC by December 2027 as planned by the NPAA (Ukrainian Government 2026). This function should extend to connecting the UkrNDNC, the Ministry of Digital Transformation, the National Accreditation Agency of Ukraine (NAAU), sectoral regulators, CABs, public procurement authorities and the WINWIN AI Centre of Excellence.

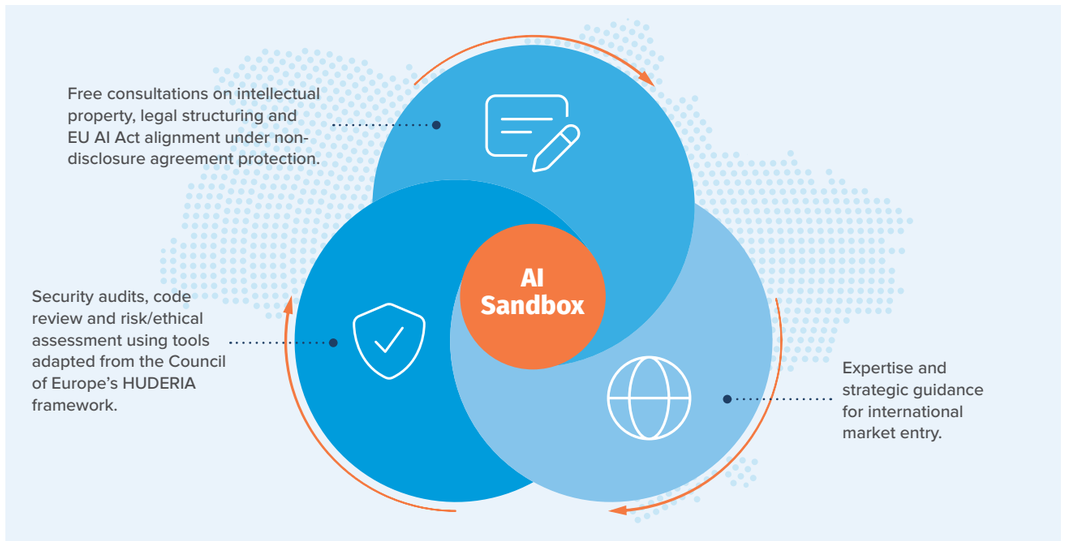
Ukraine needs to continue its dedicated AI standards-tracking and mirroring work.

2.5 ECOSYSTEM LAYER: PRIVATE SECTOR, ACADEMIA AND THE WINWIN GLOBAL INNOVATION STRATEGY TO 2030

Ukraine's AI ecosystem is based on an experienced and dynamic IT sector, resilient and scaled-up defence technology and cybersecurity capabilities, academic expertise and public-sector digitalisation experience. Its AI sector is one of the fastest growing in Europe, projected to grow from USD 573.7 million in 2026 to USD 3.22 billion by 2031. In addition, Ukraine shows high AI literacy: 42 per cent of adults and 70 per cent of teenagers use AI on a regular basis as of 2026 (Ukraine IT Association 2026). These assets matter because AI conformity assessment will require not only regulators, but also technical evaluators, internal compliance officers, auditors, testing capacity, procurement expertise and deployer-side risk management.

Established by the Ministry of Digital Transformation as part of the broader WINWIN Global Innovation Strategy to 2030, the WINWIN AI Centre of Excellence is designed as Ukraine's primary national institution for coordinating AI expertise and implementation across public governance, defence and the private sector, while the AI Sandbox focuses specifically on regulatory compliance, risk testing and legal alignment (such as EU AI Act preparedness; Ukraine Ministry of Digital Transformation 2026b).

At present, the ecosystem is primarily framed around innovation, deployment and scaling rather than assurance. The WINWIN AI Centre of Excellence is positioned as a platform for AI development and integration across government, business and society; this makes it a plausible capacity-building anchor, but not automatically an assessment body or regulator (Ukraine Ministry of Digital Transformation 2026b). Launched in collaboration with the Ukrainian Startup Fund, the AI Sandbox serves as a legal, technical and business testing environment. It is designed to help local start-ups scale responsibly while aligning with international frameworks such as the EU AI Act and the GDPR. It comprises three support tracks, as depicted below.



Overall, Ukraine is positioning itself as a burgeoning hub for AI innovation in Eastern Europe, with a rich pool of tech talent, a robust IT sector and increasing interest from global investors and companies (AI World 2026). The ecosystem continues to grow, but it is not yet organised around conformity assessment. The private sector, academia, defence-tech community and AI Sandbox could support future AI conformity readiness, especially through training, testing, sandbox participation and model-evaluation capacity. What remains is to organise these assets around assurance functions in support of regulatory supervision, while maintaining ongoing support for innovation.

Overall, Ukraine is positioning itself as a burgeoning hub for AI innovation in Eastern Europe, with a rich pool of tech talent, a robust IT sector and increasing interest from global investors and companies (AI World 2026). The ecosystem continues to grow, but it is not yet organised around conformity assessment.



2.6 WARTIME CONSTRAINTS

Ukraine is currently defending against the invasion of the Russian Federation (United Nations General Assembly 2022). Wartime conditions are operationally binding on any AI-governance capacity-building effort in Ukraine. Four constraints are especially relevant, as listed below.

Human capital and institutional bandwidth

First, human capital and institutional bandwidth, through talent migration, military service and reorientation towards defence technology and defence policy are compressing the civilian regulatory and technical talent pool. At the same time, Ukraine's digital sector remains a major economic asset: in the first half of 2025, telecommunications, computer and information services accounted for 43 per cent of Ukraine's service exports (Ukraine Ministry of Digital Transformation 2025b). This means Ukraine has relevant technical capacity, but that capacity is under pressure and unevenly distributed between civilian, defence and export-oriented activities.

Need for infrastructure resilience

A second constraint is the need for infrastructure resilience: energy, connectivity and physical security risks affect testing, evaluation and deployment infrastructure and timelines. Sovereign AI infrastructure initiatives, such as cooperation with NVIDIA and domestic AI compute capacity with Kyivstar, can be understood partly as resilience and strategic-autonomy measures (Ukraine Ministry of Digital Transformation 2025c; Lo Nostro and Marchandon 2025). For AI conformity assessment, testing environments, secure compute, data access and model-evaluation infrastructure must be reliable enough to support auditability and post-market monitoring. However, as they might not be present in sufficient capacity, Ukraine might find itself obliged to outsource these to providers under different conformity regimes (NVIDIA in this case being under the US conformity and assessment framework).

Regulatory bandwidth

A third constraint is the "regulatory bandwidth", that is, the capacity of policymakers to prioritise these matters over more pressing topics. The Verkhovna Rada's legislative agenda is dominated by war-related legislation, pushing pre-war legislation to the back of the queue and slowing EU accession priorities (Bulba, Burul, and Melnychuk 2026). Non-urgent reforms, including AI legislation, compete for limited administrative and political attention, and must contend with a Verkhovna Rada with a diminished quorum.[8] A partial solution to this issue would be to prioritise a sequence based on preparatory tools that are useful even before a full AI law is adopted: voluntary guidance, sandbox design, standards mapping, AI audit training, procurement clauses and data-protection reform, which may contribute to other political priorities.

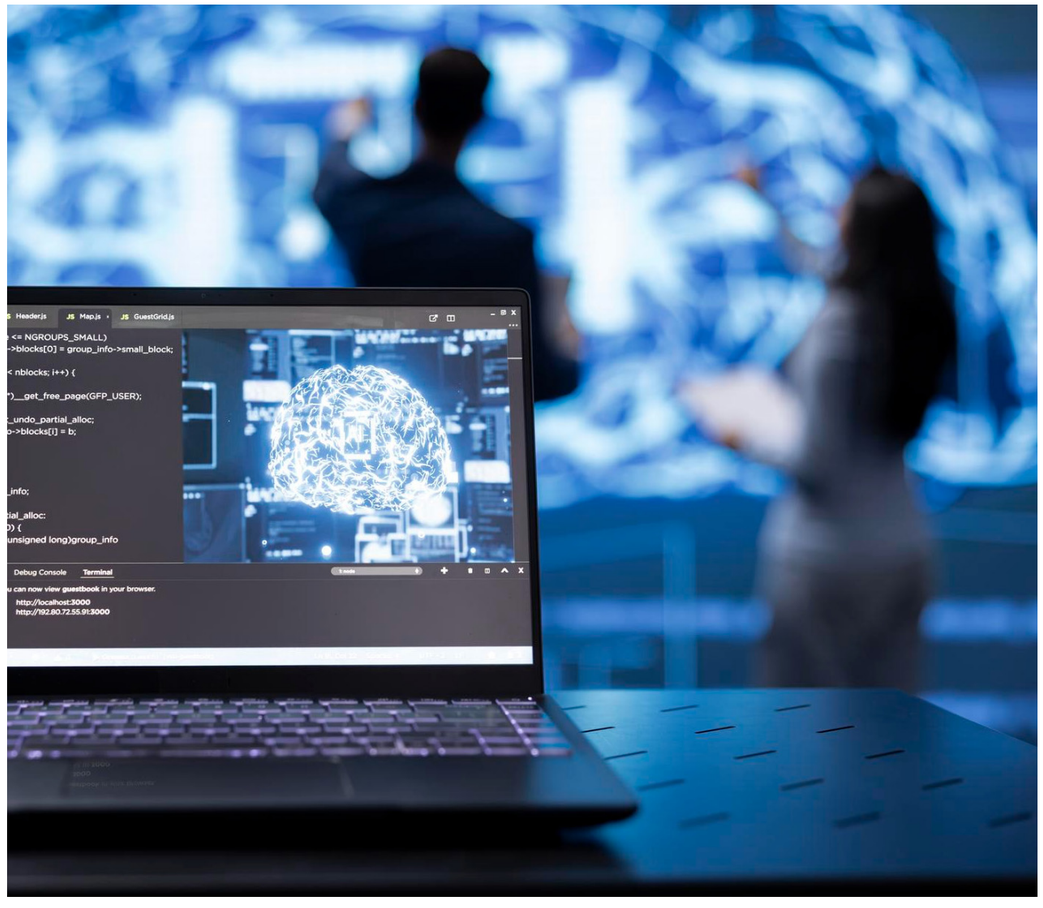
Ownership, transfer and protection of AI-related know-how

Lastly, wartime innovation also raises the issue of ownership, transfer and protection of AI-related know-how. AI systems developed in defence-adjacent, cybersecurity or public-sector contexts may later need to be commercialised, licensed, transferred to EU partners or assessed under EU-facing procurement and conformity frameworks. Ukraine's IP cooperation agenda already touches future technologies, AI, defence technologies and the Ukrainian AI language model, which makes IP protection and technology-transfer channels relevant to the broader AI governance ecosystem (European Union Intellectual Property Office 2025).

8) Currently, there are 393 sitting MPs against a constitutional 450, while 226 votes are still required to pass a law. The shortfall reflects the fact that no elections could be held in occupied constituencies in 2019, together with resignations, deaths and the seats of the banned OPFL party (44 seats). As Ukraine is under martial law, no election will be held in the foreseeable future.

Overall, wartime constraints argue for a gradual, low-fixed-cost implementation sequence for an AI conformity framework. Ukraine should prioritise measures that build AI conformity readiness without requiring the immediate creation of heavy new institutions, with the exception of the data-protection supervisor: voluntary guidance, standards-tracking, sandbox methodology, AI audit curricula, public-sector procurement requirements, data-protection reform, and targeted support for testing and evaluation capacity. This aligns with the staged approach already adopted by MoDT and preserves flexibility until the future AI law and supervisory architecture are clearer.

Ukraine should prioritise measures that build AI conformity readiness without requiring the immediate creation of heavy new institutions, with the exception of the data-protection supervisor.



2.7 DUAL-USE AI AND THE CIVILIAN REGIME

The EU AI Act does not apply to AI systems placed on the market, put into service or used exclusively for military, defence or national-security purposes (European Parliament and Council of the European Union 2024). The Council of Europe Framework Convention on AI similarly excludes activities related to national defence from its scope (Council of Europe 2024a). The civilian AI governance regime therefore does not regulate military AI directly. However, as noted above, this exclusion does not remove the dual-use problem for Ukraine: the same AI models, datasets, engineers, testing infrastructure and compute resources may be relevant in both civilian and defence-adjacent contexts.

Ukraine's wartime AI ecosystem makes this boundary especially difficult to manage. Independent analysis documents the accelerated use of AI-enabled systems in the war, including AI-enabled unmanned systems, intelligence, surveillance and reconnaissance (ISR) fusion and decision-support tools (Bondar 2025; Onderco 2025; Mysyshyn 2025). Public reporting on Ukraine's AI-enabled military capabilities also highlights the growing role of autonomy in unmanned systems while noting that human oversight remains a critical element in engagement decisions (Bondar 2025). This creates a practical challenge for civilian AI conformity assessment: whether a system falls inside or outside the civilian regime may depend less on the technical model itself than on its deployment context.

Ukrainian stakeholders consulted for this report do not consider the dual-use situation a constraint on the civilian regime, and mentioned that the ethical use of AI in the military domain is being considered in Ukrainian policy reflections. The issues below therefore concern the design of clear interfaces between the civilian and defence regimes.

Three operational issues follow. First, definitional ambiguity: a computer-vision model may be used in civilian agriculture, infrastructure monitoring or defence ISR, and its legal treatment may depend on purpose and deployment context rather than technical design alone. Second, talent and infrastructure crossover: testing laboratories, engineers, compute infrastructure, datasets and hardware production may be shared between civilian and defence-adjacent innovation ecosystems (especially at the chip level). Third, export-control and supplier-due-diligence pressure: Ukrainian providers serving EU markets may need to anticipate dual-use scrutiny under EU export-control and procurement frameworks independently of AI Act compliance (European Parliament and Council of the European Union 2021).



Overall, and especially given the current wartime context, dual-use AI requires clear civilian interfaces for Ukrainian industry and AI legislation. The dual-use grey zone is a design for Ukraine's civilian AI conformity assessment regime, which should acknowledge the AI

Overall, and especially given the current wartime context, dual-use AI requires clear civilian interfaces for Ukrainian industry and AI legislation.

Act's defence and national-security exclusion, define procedures for borderline systems, and establish clear handover protocols between civilian regulators and defence/security authorities where relevant. Sandbox rules should also clarify what can be tested in a civilian setting without triggering classified-material handling or defence-specific oversight

3

Ukrainian AI Regulation in the New Legislative Framework

For Ukraine, EU-compatible AI conformity assessment should not be treated as an entirely new institutional framework, but should make use of its existing general technical-regulation and conformity assessment framework.

The **New Legislative Framework** is the EU's general regulatory framework for the marketing of products. Its logic is to define essential legal requirements in legislation, rely on **harmonised standards** to operationalise those requirements, use conformity assessment to demonstrate compliance, attach CE marking where applicable and enforce obligations through market surveillance.

The **Blue Guide** describes this architecture as the **operating logic of EU product rules** and explains how harmonised standards support presumption of conformity once they are properly linked to legal requirements (European Commission 2022).

The **AI Act** imports this logic for **high-risk AI systems**, especially where AI systems are embedded in products already covered by sectoral EU harmonisation legislation (European Parliament and Council of the European Union 2024).



For Ukraine, EU-compatible AI conformity assessment should not be treated as an entirely new institutional framework, but should make use of its existing general technical-regulation and conformity assessment framework, including the Law of Ukraine "On Technical Regulations and Conformity Assessment" (Ukrainian Verkhovna Rada 2015). Ukraine's quality infrastructure also covers standardisation, technical regulation, conformity assessment, accreditation, metrology and market surveillance, with designated accredited bodies responsible for product conformity assessment (Ukraine Ministry of Economy and Environment 2026b). NAAU is the national accreditation body responsible for confirming the competence of conformity assessment bodies, including bodies performing testing, calibration, certification and inspection (Ukraine Ministry of Economy and Environment 2026a), and has been working with its domestic CABs to offer certifications nationally (see section 6.4, Public-private coordination and capacity-building).

Overall, Ukraine's existing conformity assessment infrastructure is an important starting point, but its AI readiness is untested. Ukraine does not need to build the entire conformity assessment ecosystem from scratch; it can instead develop its existing technical-regulation, accreditation and conformity assessment infrastructure as a foundation for future AI-specific functions. However, the question remains whether this infrastructure can absorb AI-specific assessment tasks: machine-learning expertise, model-evaluation methods, data-governance assessment, cybersecurity testing, human-oversight evaluation, post-market monitoring and coordination with sectoral regulators, especially as the two main resources identified (NAAU and WINWIN) fall under two different ministries (the Ministry of Economy and Environment and the MoDT, respectively).

Building AI-specific notified-body capacity may also prove challenging. Even in the EU, model evaluation, data-quality auditing, human oversight assessment, cybersecurity testing and post-market monitoring of adaptive or stochastic systems do not map neatly onto traditional product testing routines, and may require new technical capabilities (O'Brien et al. 2024; Raji et al. 2020). Article 43 of the AI Act also confirms that notified-body involvement is not the default route for all high-risk AI systems: many stand-alone high-risk AI systems rely on internal control, although this poses its own set of challenges (Rauh 2026).

This indicates that Ukraine should prioritise building provider-side self-assessment capacity, standards-tracking capability, sectoral market-surveillance readiness and public-sector procurement expertise first, while assessing whether and when domestic AI notified-body capacity is realistic. In the medium term, recognition of EU conformity assessment outputs or cooperation with EU-designated bodies may be more practical than attempting to create a full AI notified-body ecosystem immediately.

Ukraine should prioritise building provider-side self-assessment capacity, standards-tracking capability, sectoral market-surveillance readiness and public-sector procurement expertise first.

A practical next step is therefore to conduct an AI-readiness review of Ukraine's existing conformity assessment infrastructure. This review should cover NAAU, existing conformity assessment bodies, sectoral market-surveillance authorities, standards bodies, testing laboratories, cybersecurity certification capacity, procurement authorities and possible links to EU conformity assessment outputs. The purpose would not be to designate AI notified bodies immediately, but to identify which parts of the existing NLF-style infrastructure can be reused, which parts require capacity-building, and which functions should initially be handled through cooperation with EU bodies or external technical assistance. The most recent evaluation, carried out by UNESCO in its AI readiness assessment report, notes a lack of AI conformity assessment capacity in public procurement, as well as a general lack of dedicated approval, certification or conformity assessment mechanisms for AI in Ukraine (UNESCO 2026).

The NPAA proposes a schedule for such a review and for the related legal updates in 2026 and 2027 (Chapter 1, objectives 3 to 11), while noting that Ukraine has yet to legislate the notification of conformity assessment bodies, including the designation of a notifying authority and the procedures for notifying and monitoring such bodies.

4

EU–Ukraine Gap Analysis

AI conformity assessment depends on a broad implementation stack, covering standards, supervisory authorities, data-protection oversight, accreditation, sectoral market surveillance, sandboxing, audit capacity, post-market monitoring and private-sector readiness.



The gap between the EU AI Act regime and Ukraine's current AI governance framework is not only legal. Ukraine can approximate legal text relatively quickly, but AI conformity assessment depends on a **broader implementation stack**: standards, supervisory authorities, data-protection oversight, accreditation, sectoral market surveillance, sandboxing, audit capacity, post-market monitoring and private-sector readiness.

The main gaps are therefore **institutional**, **technical** and **operational**.



4.1 GAP MATRIX

TABLE 2: Gap matrix: the EU AI Act regime and Ukraine's current AI governance framework

Dimension	EU regime	Ukraine status	Gap severity
Legal basis for AI	▪ AI Act 2024/1689 in force. ▪ Omnibus deferral adjusted implementation timelines.	▪ No binding horizontal AI law. ▪ Draft laws currently under consideration in Parliament. ▪ Adoption of a law planned for 2028 under the NPAA.	**High**
Risk taxonomy	Statutory taxonomy: prohibited, high-risk, limited-risk, minimal-risk, GPAI and systemic-risk GPAI.	Voluntary Code of Conduct (Ukraine Ministry of Digital Transformation 2024a) and policy guidance only.	**High**
Conformity assessment routes	▪ Internal control as the default for many high-risk systems. ▪ Notified-body route for narrower categories and sectoral product regimes.	▪ No AI-specific conformity assessment route. ▪ General NLF-style backbone exists through technical-regulation and accreditation infrastructure. ▪ Potential gap in the planned AI law regarding the implementation of conformity assessment provisions.	**High, with partial institutional convergence**
Sectoral conformity assessment	AI requirements interact with existing EU sectoral product-safety regimes where applicable.	▪ Sectoral readiness for AI-specific requirements not yet mapped; for machinery, AI requirements will follow the EU Machinery Regulation. ▪ No explicit requirement for AI conformity assessment to use sectoral safety regimes.	**High**
Standards	CEN-CENELEC JTC 21, ISO/IEC standards and harmonised standards supporting presumption of conformity once cited.	▪ Systematic public evidence of JTC 21 mirroring and of an ISO/IEC 42001 implementation pathway. ▪ National translation of the standards under DSTU.	**Medium**
Supervisory authority	▪ National competent authorities designated under the AI Act. ▪ EU-level coordination through AI Office and AI Board.	▪ No AI supervisory authority designated. ▪ One is planned under the NPAA, with uncertain delivery timing.	**High**

TABLE 2: Gap matrix: the EU AI Act regime and Ukraine's current AI governance framework

Dimension	EU regime	Ukraine status	Gap severity
Data-protection authority	Independent national data-protection authorities under the GDPR.	▪ Ombudsman performs interim functions. ▪ Draft Law No. 6177 on independent authority pending.	**High**
Market surveillance	Regulation (EU) 2019/1020 and AI-specific post-market obligations.	▪ General market-surveillance regime exists. ▪ AI-specific mandate and capacity not yet established. ▪ Planned under the NPAA, but posing risks as regards coordination and institutional scope.	**Medium-high**
Sandbox	▪ AI Act requires regulatory sandboxes. ▪ Omnibus deferred implementation timing.	AI Sandbox fully operational.	**Low**
Auditing and professional capacity	Emerging EU ecosystem around AI standards, conformity assessment, notified bodies, internal compliance and market surveillance.	▪ Limited AI audit capacity. ▪ No national AI audit curriculum. ▪ WINWIN AI Centre of Excellence potentially positioned but not yet mandated for assurance.	**High**
GPAI Code of Practice	▪ Voluntary EU instrument for GPAI providers. ▪ Major model providers may use it to demonstrate compliance.	▪ GPAI models trained on Ukrainian infrastructure; no guidance on data protection or systemic risks. ▪ Deployer-side relevance for procurement and public-sector use.	**Medium**
Post-market monitoring	▪ Provider obligation. ▪ Serious-incident reporting and market-surveillance enforcement.	No AI-specific post-market monitoring or incident-reporting framework.	**High**
Redress and complaints	AI Act rights to explanation/complaint mechanisms plus sectoral redress.	Not yet designed in AI-specific terms.	**Medium**
EU–Ukraine implementation channels	EU AI Office, AI Board, standardisation bodies, sectoral regulators and cooperation networks.	No structured AI-specific EU–Ukraine implementation channel yet.	**Medium**

The most severe gaps are institutional and operational: Ukraine can approximate the AI Act's legal structure faster than it can build the institutions and professional capabilities needed to implement it. The binding constraints are an independent data-protection authority, a designated AI supervisory model, sectoral conformity assessment readiness, market-surveillance capability, post-market monitoring and a pool of trained AI auditors.

The most severe gaps are institutional and operational.

4.2 CROSS-CUTTING GAPS

Four cross-cutting gaps also emerge from the gap matrix:



4.3 SEQUENCING

The central sequencing question is whether Ukraine should adopt a binding AI law before the supervisory and conformity assessment architecture is in place, or after the basic implementation assets have been prepared. The Stage 1/Stage 2 model already adopted by the MoDT and operationalised by the NPAA chooses the second path: voluntary instruments first, paving the way for binding legislation, with credible preparatory tools developed in the meantime and using the respite provided by the Digital Omnibus deferral. The major milestone is the adoption of the AI law by 2028.

Ukraine should use this period to prepare concrete assets: standards mapping, sandbox methodology, AI audit curricula, public-sector procurement clauses, data-protection authority reform, institutional-design options, sectoral conformity assessment mapping and EU cooperation channels.

Ukraine should treat 2026–2027 as an implementation-readiness window. The near-term priority should be to build the capacities that will make a future AI law enforceable: data-protection reform, conformity assessment capacity and guidance, sectoral readiness, audit training and public-sector procurement discipline. This would set the scene for binding AI legislation to land in a credible institutional and technical environment capable of enforcing it.

4.4 EU–UKRAINE IMPLEMENTATION CHANNELS: LESSONS FROM IP ALIGNMENT

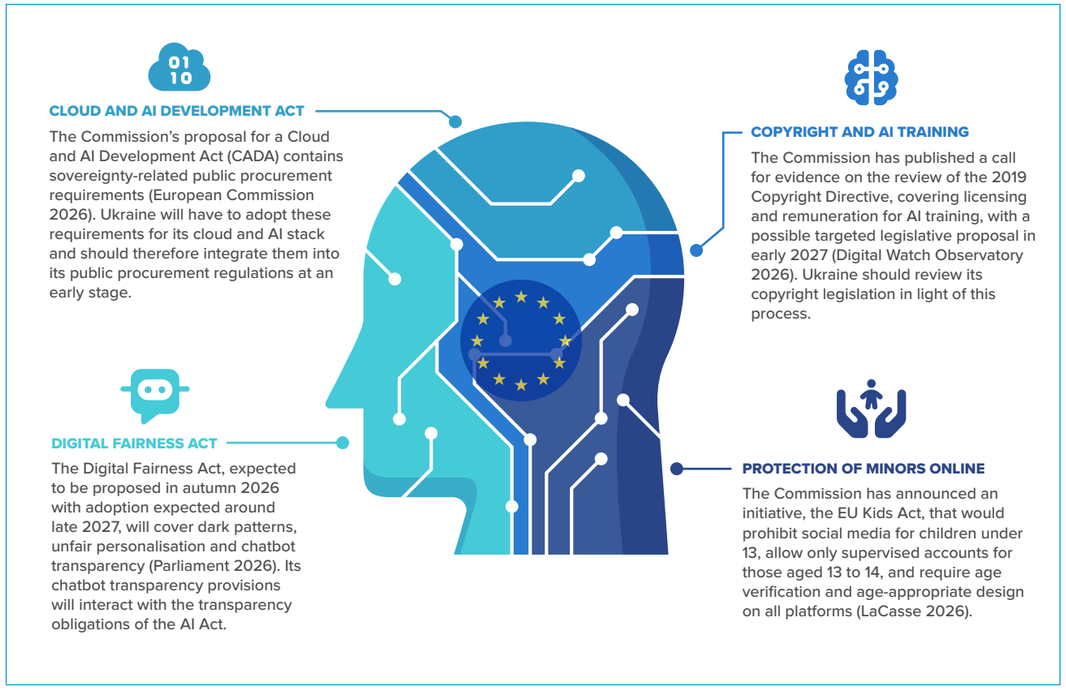
Ukraine's IP alignment offers a useful analogy for AI conformity assessment. IP approximation is not pursued only through domestic legal reform, but also through standing EU–Ukraine cooperation channels, including the EU–Ukraine IPR Dialogue, EUIPO–UANIPIO cooperation[9] and EU4IP technical assistance (European Union Intellectual Property Office 2025). AI conformity assessment will need a similar implementation model: legal transposition should be paired with durable channels for standards-tracking, conformity assessment guidance, audit training, sandbox methodology, cybersecurity certification, sectoral implementation and cooperation with specialised EU bodies.

It follows that AI alignment should be organised as an implementation partnership rather than as a purely legislative exercise. Ukraine should establish structured EU-facing channels for AI Act implementation, modelled on existing regulatory-alignment cooperation in areas such as IP. These channels should connect Ukrainian authorities and technical bodies with relevant EU actors around standards, conformity assessment, sandbox practice, audit capacity, public procurement and post-market supervision.

9) The Ukrainian National Office for Intellectual Property and Innovation.

4.5 ANTICIPATING EU PRIORITIES AND UPCOMING LEGISLATION

The EU digital *acquis* continues to evolve. Beyond the AI Act and the Digital Omnibus, several EU initiatives now in preparation will shape the digital *acquis* that Ukraine will need to adopt. Anticipating them would spare Ukraine successive rounds of legislative revision. Four initiatives are especially relevant, as depicted below.



Tracking these initiatives through the EU–Ukraine implementation channels described in section 4.4 would allow Ukraine to prepare its procurement, copyright and consumer-protection frameworks in step with the direction of EU legislation.

5

The GPAI Code of Practice: Implications for Ukraine

The General-Purpose AI Code of Practice (GPAI) is a voluntary EU instrument designed to help providers of general-purpose AI models comply with the AI Act's GPAI obligations. The Code has three chapters: Transparency, Copyright and Safety and Security.



Given Ukraine's stated aim of becoming a member of the European Union, one key resource for the voluntary private-sector commitments of Stage 1 is the **General-Purpose AI Code of Practice**. It is a voluntary EU instrument designed to help providers of general-purpose AI models comply with the AI Act's GPAI obligations (European Commission 2025).

The Code has three chapters: **Transparency**, **Copyright** and **Safety** and Security. The Transparency and Copyright chapters are relevant to all GPAI model providers, while the Safety and Security chapter applies only to providers of GPAI models with systemic risk under Article 55 of the AI Act.

The Commission describes the Code as a **tool to help providers demonstrate compliance** with obligations on transparency, copyright and safety/security pending further standardisation (European Commission 2025).



For Ukraine, the Code has three implications. First, GPAI models are already being trained on Ukrainian infrastructure for public and commercial use, while no recommendation or regulation yet addresses how these models should deal with data protection or systemic risks; provider-side exposure is therefore emerging, even though Ukraine does not currently appear to host a GPAI model provider in the systemic-risk tier (Digital State Ukraine 2026). Second, Ukrainian public-sector bodies, healthcare actors, defence-adjacent users, businesses and start-ups will increasingly deploy or integrate GPAI models developed abroad, making deployer-side procurement and due-diligence practices a priority in the short term. Third, Ukraine's development of a national large language model and its sovereign AI ambitions will increase this provider-side exposure as domestic GPAI development advances.

The GPAI Code of Practice can serve as a voluntary procurement and due-diligence reference for Ukraine. Ukraine should not treat the Code as a substitute for AI legislation or conformity assessment. However, it can be used during the preparatory stage as a practical reference for public procurement, contractual due diligence and deployer guidance. In particular, Ukrainian public buyers and AI deployers could use the provisions of the Code to request information from GPAI providers on model documentation, copyright policies, safety and security practices, model limitations and downstream risk management. This would give Ukraine an immediately usable alignment tool without prematurely imposing full provider-side GPAI obligations on domestic actors. Domestic providers training GPAI models on Ukrainian infrastructure could also be encouraged to follow the Transparency and Copyright chapters of the Code on a voluntary basis, pending national guidance on data protection and systemic risks.

The GPAI Code of Practice can serve as a voluntary procurement and due-diligence reference for Ukraine.

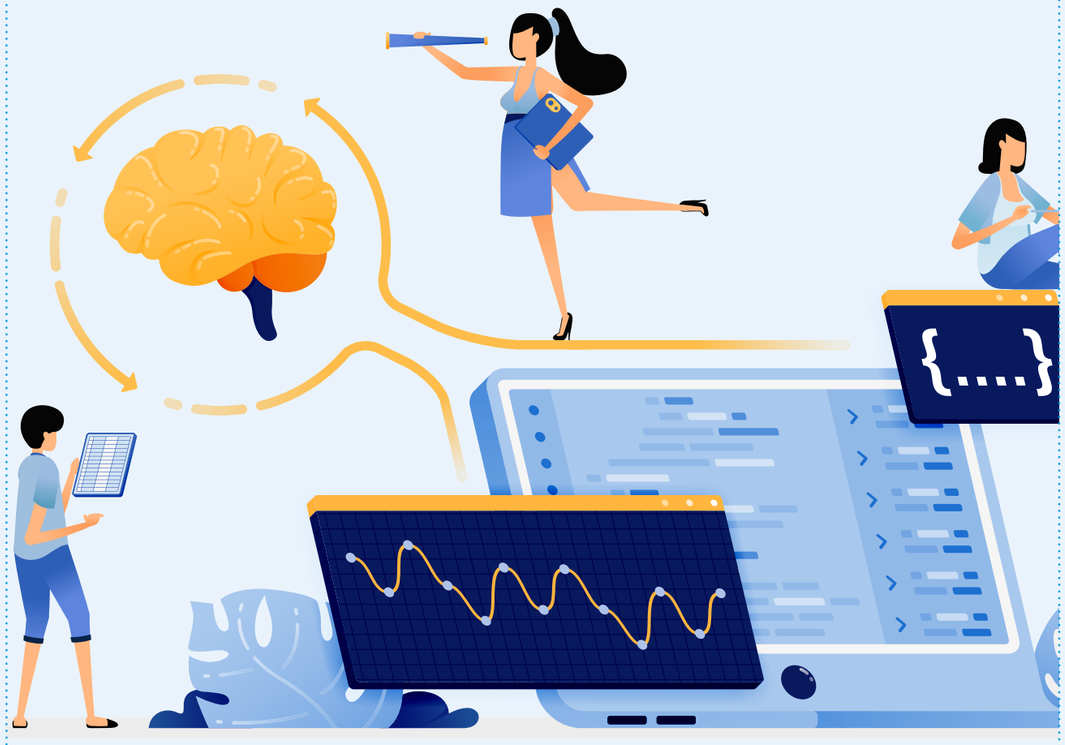
6

Building AI Auditing Expertise in Ukraine

AI conformity assessment will require a new professional skill base in Ukraine, as AI auditing should be understood as a set of overlapping roles. These would form a talent pool on which public supervision, notified bodies and private internal compliance functions could draw.



AI conformity assessment will require a **new professional skill base** in Ukraine. This is not limited to future notified-body assessors: since many high-risk AI obligations in the EU model rely on internal control and provider-side self-assessment, Ukraine will also need **trained compliance officers**, **public-sector procurement specialists**, **market-surveillance staff, technical evaluators** and **deployer-side risk managers**.



6.1 BUILDING AI AUDIT ROLES

AI auditing should be understood as a set of overlapping roles: provider-side compliance officers able to handle risk management, technical documentation, quality management and post-market monitoring; public-sector procurement officers able to include auditability and supplier-due-diligence clauses in AI contracts; market-surveillance staff able to review documentation and respond to incidents; technical evaluators and red-teamers able to test robustness, cybersecurity, bias and misuse risks; and, in narrower cases, third-party conformity assessors able to perform formal assessments where required. Together, these professionals would form a talent pool on which public supervision, notified bodies and private internal compliance functions could draw. Stakeholders identified the talent pool as a core issue. Ukraine needs specialists able to perform these roles, and the same expertise is in high demand in the EU, including in the private sector. Upskilling programmes and technical assistance projects, together with closer collaboration with Ukrainian universities on model evaluation and benchmarking capacity, would help build and retain this talent pool.



6.2 WHAT AN AI AUDIT CURRICULUM SHOULD COVER

Ukraine should build its AI audit curriculum around existing and emerging international anchors. ISO/IEC 42006:2025, published on 7 July 2025, sets requirements for AI certification bodies themselves (ISO 2025) and is layered on ISO/IEC 17021-1, which sets requirements for bodies providing audit and certification of management systems (ISO 2015). CEN-CENELEC JTC 21 standards are a natural scaffold for AI Act implementation; ISO/IEC 42001 can provide an organisational anchor for AI management systems; HUDERIA is already being used in the AI Sandbox ethical tests; and OECD tools can help map AI governance measures against broader digital regulatory frameworks (Krog 2025; CEN-CENELEC 2021; ISO 2023; Council of Europe 2026a; Sarlième et al. 2025).

A brief scan of the literature suggests that a practical curriculum should cover seven areas:

- **AI Act and Ukrainian conformity assessment frameworks** in an NLF logic, which could cover, for example, AI Act provisions and their transposition into Ukrainian law, as well as declarations of conformity, CE marking and registration. GPAI obligations and the value chain are also crucial, since most Ukrainian providers are currently downstream of foreign developers.
- **Standards and AI management systems based on ISO standards** such as ISO/IEC 42001, 42005 (impact assessment), 23894 (risk), 5259 (data quality), 24029 (robustness of neural networks). The CEN-CENELEC standards are also relevant, specifically EN 18286. However, while they are official, they do not grant presumption of conformity until they have been cited in the Official Journal and become harmonised standards.
- **Data governance and privacy**, covering both the General Data Protection Regulation and the data governance duties under Article 10 of the AI Act (representativeness, error rates, bias examination), which are critical for AI development.
- **Model evaluation and robustness**, covering technical capabilities regarding benchmark validity, construct validity, test-set contamination, fairness-metric selection and impossibility results, red-teaming protocols and the evaluation of non-transparent systems.
- **Cybersecurity**, based on Ukraine's new cybersecurity law in force since 20 April 2025, the EU Cyber Resilience Act and the January 2026 Commission proposals amending NIS2 and revising the Cybersecurity Act, and on ISO/IEC 27001 (Baker McKenzie Resource Hub 2025).
- **Dual-use identification**: because AI is to a large extent a dual-use technology, particularly at the frontier and in general-purpose models, auditors must be able to identify dual-use cases, regardless of the AI Act's exclusion of military, defence and national security matters. Subjects such as identifying dual-use potential and export control legislation would add value, and could extend to responsible AI principles in a military context, such as the NATO principles on responsible AI.
- **More general issues**, such as public-sector procurement and deployment controls, audit practices and professional ethics, and relevant EU legislation in the context of Ukraine's accession to the EU, would help auditors keep up with the rapidly evolving legal landscape in AI conformity assessment.

6.3 INSTITUTIONAL HOME FOR CAPACITY-BUILDING

The WINWIN AI Centre of Excellence could be a useful anchor for AI audit capacity-building, but it should not be treated as a regulator or conformity assessment authority. Its comparative advantage is ecosystem coordination, training, testing and convening. Supervisory and enforcement functions should remain with future competent authorities, the independent data-protection authority, sectoral regulators and market-surveillance bodies.

A realistic model would be to use WINWIN, or another existing platform, to coordinate training and professional networks, drawing on the AI Sandbox for expertise and practical experience, while keeping formal regulatory powers separate.

6.4 PUBLIC-PRIVATE COORDINATION AND CAPACITY-BUILDING

Since provider-side self-assessment will be the dominant route for many high-risk systems, much of the capacity must be built inside companies, public-sector deployers, procurement bodies and technical consultancies. Regulators need enough expertise to supervise and challenge documentation, but providers and deployers must be able to produce it in the first place.

AI conformity readiness must be built across the ecosystem, not only inside regulators. Ukraine's first priority should be to create a shared professional baseline for AI risk management, documentation, testing, procurement and post-market monitoring. This would make future AI legislation more enforceable and reduce the risk that compliance remains a formal legal exercise without operational substance.

This is important because a market for certification is already forming in Ukraine, ahead of the accreditation framework that should govern it. Domestic CABs are working with NAAU to expand their ISO/IEC 17021-1 (management system certification) accreditation scopes to formally cover ISO/IEC 42001, and some have officially begun offering AI management system and audit services, including:

- **UkrTEST:** One of Ukraine's primary conformity assessment centres has launched dedicated artificial intelligence (AI) certification services. It conducts audits against ISO/IEC 42001 (AIMS), ISO/IEC 23894 (risk management) and ISO/IEC 38507 (governance). To achieve global recognition, it provides dual certification with European partners such as GSI-CERT.
- **Local specialised auditors and consultancies:** emerging domestic providers (and localised accredited audit teams of foreign accreditation companies such as BALTUM) have introduced automated gap-analysis tools, AIMS documentation templates and Stage 1/ Stage 2 audit programmes tailored to Ukrainian start-ups preparing for both local sandbox audits and European AI Act compliance. Although a certification market is forming, it remains small. According to stakeholders, Ukraine is not yet a significant market for AI evaluation and audit, and most audits appear to be carried out by European firms, as the dual certification arrangements described above illustrate. Building domestic auditing capacity would reduce this dependence and keep audit expertise within the Ukrainian ecosystem.

Conclusions and Recommendations

Ukraine has made a strategic choice: an AI conformity assessment framework aligned with the EU, driven by accession conditionality and the Ukraine Facility. The question that remains, however, is how to make convergence enforceable. Ukraine's two-stage strategy, starting with voluntary preparation and paving the way for binding EU-aligned legislation, is sound, and the adoption of the Digital Omnibus on AI in June 2026 gives Ukraine until December 2027 (stand-alone high-risk systems) and August 2028 (embedded systems) to build the capacity that a future AI law will require.

There remain major institutional and operational gaps: an independent data-protection authority and a modern data-protection law are still pending, an AI supervisory architecture has been envisaged on paper but not yet implemented, and AI audit expertise remains scarce.

Because most high-risk obligations in the EU are discharged through provider-side internal control, readiness must be built across the ecosystem – among providers, deployers, public buyers and market-surveillance bodies – and not only within regulators.

The window is short, given the pace of AI development and deployment, the growing weight of AI in the Ukrainian economy and the emerging need for a certification market; wartime constraints and the civilian/dual-use boundary argue for a gradual, low-fixed-cost sequence with one exception: the data-protection supervisor.



RECOMMENDED STEPS

On the basis of the findings of this report, the following steps are recommended:

- **Organise AI alignment as an implementation partnership with the EU**, modelled on the IP-alignment channels and supported through the Ukraine Facility and the Instrument for Pre-Accession Assistance, and use the GPAI Code of Practice as a voluntary procurement and due-diligence reference in the meantime.
- **Continue the dedicated standards-tracking and mirroring function** connecting UkrNDNC, NAAU, sectoral regulators and the WINWIN AI Centre of Excellence, to ensure systematic adoption of CEN-CENELEC JTC 21 outputs (starting with EN 18286) and ISO/IEC 42001 into the DSTU system.
- **Complete data-protection reform as the first institutional priority:** adopt Draft Law No. 8153 or similar provisions and establish an independent supervisory authority such as the one envisaged under Draft Law No. 6177 as planned by the NPAA, a precondition for credible AI conformity assessment.
- **Map sectoral conformity assessment readiness** (ultimately focusing on domains with dual-use potential such as biotechnology, nuclear technology and cybersecurity) and prepare the integration of AI Act-style requirements into existing technical regulation, following the EU's own sectoral updates, starting with machinery, where AI-related requirements will be introduced through delegated acts under the EU Machinery Regulation.
- **Develop a national AI audit curriculum and talent pool** covering provider-side self-assessment, public procurement, market surveillance and technical evaluation, anchored in ISO/IEC 42001, ISO/IEC 42006 and JTC 21 standards, in collaboration with Ukrainian universities on model evaluation and benchmarks, and supported by upskilling programmes and technical assistance projects.
- **Remain on the timeline for binding AI legislation (AI Strategy Stage 2) proposed by the NPAA**, taking into account developments in EU legislation such as the Omnibus application dates, to preserve credibility with stakeholders and accession screening processes.
- **Given the wartime context, define a legislative or institutional interface for dual-use AI**: procedures for borderline systems, handover protocols between civilian and defence authorities, and sandbox rules that avoid triggering defence-specific oversight.
- **Conduct an AI-readiness review of the existing conformity assessment infrastructure** (NAAU, conformity assessment bodies, testing laboratories, market-surveillance authorities) to identify what can be reused, what needs capacity-building, and what should initially rely on cooperation with EU bodies. Develop in parallel a notifying-authority and conformity-assessment-body notification framework as proposed in the NPAA.
- **Prepare a fallback option for AI supervision** in case the Single Digital Regulator is not operational in time, for example by empowering an existing body such as the NCEC for monitoring and enforcement, supported by twinning arrangements with EU Member State authorities, and plan from the outset the handover of AI Office functions to the EU level upon accession.
- **Issue guidance for GPAI models trained on Ukrainian infrastructure**, covering data protection, transparency and systemic risks, drawing on the GPAI Code of Practice.
- **Anticipate upcoming EU digital priorities**, notably the Cloud and AI Development Act, the review of copyright rules for AI training, the Digital Fairness Act and the protection of minors online, and integrate them into public procurement, copyright and consumer-protection reforms.

References

REFERENCES

[1] Baker McKenzie Resource Hub. 2025. ‘Key Data and Cybersecurity Laws | Ukraine’. *Baker McKenzie Resource Hub*. https://resourcehub.bakermckenzie.com/pl-pl/resources/global-data-and-cyber-handbook-lite/emea/ukraine/topics/key-data-and-cybersecurity-laws (August 6, 2026).

[2] Bondar, Kateryna. 2025. *Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*. Center for Strategic and International Studies. (August 4, 2026). https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

[3] Bulba, Vitalii, Olena Burul, and Ivan Melnychuk. 2026. *How the Verkhovna Rada Is Slowing Ukraine’s EU Integration*. Vox Ukraine. https://voxukraine.org/en/how-the-verkhovna-rada-is-slowing-ukraine-s-eu-integration (August 4, 2026).

[4] Cabinet of Ministers of Ukraine. 2020. *Cabinet of Ministers Resolution No. 1556-r - Про Схвалення Концепції Розви... | Від 02.12.2020 № 1556-р (Текст Для Друку)*. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80 (August 3, 2026).

[5] ‘CEN - CEN/CLC/JTC 21’. 2026. https://standards.cencenelec.eu/ords/f?p=CEN:110:::::FSP_PROJECT,FSP_ORG_ID:80556,2916257&cs=12A382BDB5385F509EBAA7CD4808AFBF3 (August 7, 2026).

[6] CEN-CENELEC. 2021. ‘Artificial Intelligence’. *CEN-CENELEC*. https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/ (August 6, 2026).

[7] CEN-CENELEC JTC 21. 2026. ‘CEN - CEN/CLC/JTC 21 - Work Programme’. *CEN-CENELEC*. https://standards.cencenelec.eu/ords/f?p=205:22:::::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=114251C6C0B684FBBC069923513BF6348 (August 7, 2026).

[8] CEN-CENELEC JTC21. 2025. ‘Update on CEN and CENELEC’s Decision to Accelerate the Development of Standards for Artificial Intelligence’. *CEN-CENELEC*. https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/ (August 6, 2026).

[9] *COMMISSION STAFF WORKING DOCUMENT Ukraine 2025 Report Accompanying the Document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF REGIONS 2025 Communication on EU Enlargement Policy*. 2025. https://enlargement.ec.europa.eu/document/download/17115494-8122-4d10-8a06-2cf275eecde7_en?filename=ukraine-report-2025.pdf (July 31, 2026).

[10] Council of Europe. 2024a. *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. https://rm.coe.int/1680afae3c.

[11] Council of Europe. 2024b. *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. https://rm.coe.int/1680afae67.

[12] Council of Europe. 2026a. *HUDERIA - Methodology for Assessing the Risks and Impacts of Artificial Intelligence Systems from the Perspective of Human Rights, Democracy and the Rule of Law Resource Model for Context-Based Risk Analysis (COBRA)*. https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1.

[13] Council of Europe. 2026b. ‘List of Countries Having Ratified the Framework Convention on Artificial Intelligence, Human Rights and Democracy’. *Treaty Office*. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225 (August 4, 2026).

[14] Digital Regulation Cooperation Forum. 2023. ‘Digital Regulation Cooperation Forum (DRCF)’. https://www.drcf.org.uk (September 29, 2026).

[15] Digital State Ukraine. 2026. ‘Ukraine Moves Toward a Sovereign AI Model: National LLM to Enter Beta in 2026’. https://digitalstate.gov.ua/news/govtech/ukraine-moves-toward-a-sovereign-ai-model-national-llm-to-enter-beta-in-2026 (September 29, 2026).

[16] Digital Watch Observatory. 2026. ‘European Commission Launches Copyright Consultation Focused on AI | Digital Watch Observatory’. https://dig.watch/updates/european-commission-copyright-consultation-on-ai (September 28, 2026).

[17] Directorate-General for Communications Networks, Content and Technology (European Commission), Wavestone, CEPS, ICF, Renda, Andrea, Fanni, Rosanna, Laurer, Moritz, et al. 2021. Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe: Final Report. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/523404 (September 29, 2026).

[18] *Draft Law No. 5618 on Personal Data Protection*. 2022. (Ukrainian Verkhovna Rada) https://itd.rada.gov.ua/billinfo/Bills/Card/26873 (August 25, 2026).

[19] *Draft Law No. 6177 On an Independent Supervisory Authority for Personal Data Protection and Access to Public Information - Картка Законопроєкту, Проєкту Іншого Акта - Законотворчість*. 2021. (Ukrainian Verkhovna Rada) https://itd.rada.gov.ua/billinfo/Bills/Card/27996 (August 3, 2026).

[20] *Draft Law No. 8153 On Personal Data Protection - Картка Законопроєкту, Проєкту Іншого Акта - Законотворчість*. 2024. (Ukrainian Verkhovna Rada) https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (August 3, 2026).

[21] European Commission. 2022. *Commission Notice The ‘Blue Guide’ on the Implementation of EU Product Rules 2022 (Text with EEA Relevance) 2022/C 247/01*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022XC0629(04) (August 3, 2026).

[22] European Commission. 2025. *The General-Purpose AI Code of Practice*. https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (March 6, 2026).

[23] European Commission. 2026. ‘Proposal for the Cloud and AI Development Act (CADA) | Shaping Europe’s Digital Future’. https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada (September 28, 2026).

[24] European Commission. 2026. ‘Standardisation of the AI Act | Shaping Europe’s Digital Future’. https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation (August 6, 2026).

[25] European Council. 2026a. ‘Artificial Intelligence: Council and Parliament Agree to Simplify and Streamline Rules’. *Consilium*. https://www.consilium.europa.eu/en/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/ (August 3, 2026).

[26] European Council. 2026b. ‘Artificial Intelligence: Council Gives Final Green Light to Simplify and Streamline Rules’. *Consilium*. https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/ (August 7, 2026).

[27] European Parliament and Council of the European Union. 2021. REG/EU/2021/821 *Regulation Establishing a Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items- 2021/821 - EN - EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0821 (August 4, 2026).

[28] European Parliament and Council of the European Union. 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

[29] European Parliament and Council of the European Union. 2026. REG(EU)2026/1744 *Regulation - EU - 2026/1744 - EN - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng (August 7, 2026).

[30] European Union Intellectual Property Office. 2025. ‘The EUIPO Strengthens Cooperation at Ukraine’s Leading IP and Innovation Forum | EU Funded IP Projects’. https://internationalipcooperation.eu/en/eu4ip/news/euipo-strengthens-cooperation-ukraines-leading-ip-and-innovation-forum (August 4, 2026).

[31] Government of Ukraine. 2024. *Ukraine Facility Plan 2024-2027*. https://www.ukrainefacility.me.gov.ua/wp-content/uploads/2024/03/ukraine-facility-plan.pdf.

[32] Ionan, Valeriya. 2026. ‘Building the Agentic State: How Ukraine Is Moving Beyond Digital Government’. https://digitalstate.gov.ua/news/govtech/building-the-agentic-state-how-ukraine-is-moving-beyond-digital-government (September 29, 2026).

[33] ISO. 2015. ‘ISO/IEC 17021-1:2015’. https://www.iso.org/standard/61651.html (August 6, 2026).

[34] ISO. 2023. ‘ISO/IEC 42001:2023 - Information Technology — Artificial Intelligence — Management System’. https://www.iso.org/standard/42001 (August 6, 2026).

[35] ISO. 2025. ‘ISO/IEC 42006:2025’. https://www.iso.org/standard/42006 (August 6, 2026).

[36] ISO. 2026. ‘SE UkrNDNC Membership Page - International Standards Organisation’. *ISO*. https://www.iso.org/member/2172.html (August 4, 2026).

[37] Krog, Georg. 2025. *CEN-CENELEC-JTC21-AI-Standards-Complete-Detailed-Overview*. CEN-CENELEC JTC 21. https://jtc21.eu/wp-content/uploads/2025/06/CEN-CENELEC-JTC21-AI-Standards-Complete-Detailed-Overview.pdf (August 6, 2026).

[38] LaCasse, Alex. 2026. ‘Frontier AI Curbs, Children’s Social Media Restrictions among Priorities in EU State of the Union Address | IAPP’. IAPP.org. https://iapp.org/news/a/frontier-ai-curbs-childrens-social-media-restrictions-among-priorities-in-eu-state-of-the-union-address (September 28, 2026).

[39] Lo Nostro, Gianluca, and Leo Marchandon. 2025. ‘Ukraine Plans Domestic AI Computing Capacity with Kyivstar’. *Reuters*. https://www.reuters.com/business/media-telecom/ukraine-plans-domestic-ai-computing-capacity-with-kyivstar-2026-06-26/ (August 4, 2026).

[40] Mysyshyn, Anna. 2025. ‘Governing AI Under Fire in Ukraine’. *The Cairo Review of Global Affairs*. https://www.thecairoreview.com/essays/governing-ai-under-fire-in-ukraine/ (August 4, 2026).

[41] Niestadt, Maria. 2026. *Digital Omnibus on AI | Think Tank | European Parliament*. European Parliament Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2026)782651 (August 6, 2026).

[42] O’Brien, Joe, Shaun Ee, Jam Kraprayoon, Bill Anderson-Samways, Oscar Delaney, and Zoe Williams. 2024. ‘Coordinated Disclosure of Dual-Use Capabilities: An Early Warning System for Advanced AI’. https://arxiv.org/pdf/2407.01420.

[43] OECD. 2025. ‘Roadmap for AI Regulation in Ukraine: A Bottom-up Approach’. https://oecd.ai/en/policy-initiatives/roadmap-for-ai-regulation-in-ukraine-a-bottom-up-approach (August 3, 2026).

[44] OECD. 2026. *Governing with Artificial Intelligence: Public Governance Review of Ukraine*. https://www.oecd.org/en/publications/public-governance-review-of-ukraine_7810f059-en/full-report/governing-with-artificial-intelligence_1a82b789.html (August 6, 2026).

[45] Onderco, Michal. 2025. ‘Navigating the AI Frontier: Insights from the Ukraine Conflict for NATO’s Governance Role in Military AI’. *Journal of Strategic Studies* 48(3): 602–26. doi:10.1080/01402390.2025.2463451.

[46] Parliament, European. 2026. ‘Digital Fairness Act | Legislative Train Schedule’. European Parliament. https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act (September 28, 2026).

[47] Raji, Inioluwa Deborah, Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes. 2020. 'Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing'. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, FAT* '20, New York, NY, USA: Association for Computing Machinery, 33–44. doi:10.1145/3351095.3372873.

[48] Rauh, Maribeth. 2026. *Accountability in the Face of AI Evaluation Challenges*. Ada Lovelace Institute. https://www.adalovelaceinstitute.org/blog/accountability-in-the-face-of-ai-evaluation-challenges/ (August 4, 2026).

[49] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance)*. 2019. 151 OJ L http://data.europa.eu/eli/reg/2019/881/oj (August 3, 2026).

[50] Roman, Inna. 2026. 'Architects of the Digital State: The Institutional Role of the CDTO and the System for Training Digital Leaders in Ukraine'. Vox Ukraine. https://voxukraine.org/en/architects-of-the-digital-state-the-institutional-role-of-the-cdto-and-the-system-for-training-digital-leaders-in-ukraine (September 29, 2026).

[51] Sarlième, Pierre, James Drummond, Becky King, Natalie Cohen, and Anna Pietikäinen. 2025. *A Mapping Tool for Digital Regulatory Frameworks: Including a Pilot on Efforts to Regulate AI*. 23rd edn. OECD Regulatory Policy Working Papers. doi:10.1787/1cdad902-en.

[52] 'The Ukraine Facility - European Commission'. 2026. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/ukraine-facility_en (August 1, 2026).

[53] 'Ukraine / AI World'. https://aiworld.eu/geo/ukraine (September 9, 2026).

[54] Ukraine IT Association. 2026. *Ukraine AI Industry Map: A Comprehensive Study of the AI Sector in Ukraine*. https://itukraine.org.ua/files/UKRAINE_AI_INDUSTRY_MAP.pdf (August 4, 2026).

[55] Ukraine Ministry of Digital Transformation. 2024a. 'Voluntary Code of Conduct on the Ethical and Responsible Use of AI'. https://storage.thedigital.gov.ua/files/0/e0/e9540a11682f3bc1d0472755b09fbe04.pdf.

[56] Ukraine Ministry of Digital Transformation. 2024b. *White Paper on Regulation of AI in Ukraine - Біла Книга з Регулювання ШІ в Україні*. https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf.

[57] Ukraine Ministry of Digital Transformation. 2025a. *A Sectoral Analysis and Initial Vision for AI Development in Ukraine*. https://winwin.gov.ua/assets/files/ENG%20WINWIN_AI%201.pdf.

[58] Ukraine Ministry of Digital Transformation. 2025b. 'Ukraine IT Exports Rise to 43% of Total Trade'. https://digitalstate.gov.ua/news/it-outsourcing/it-posluhy-staly-holovnym-drayverom-eksportu-ukrayiny-u-2025-rotsi (August 4, 2026).

[59] Ukraine Ministry of Digital Transformation. 2025c. 'Ukraine's Bold AI Bet: Sovereignty with NVIDIA Tech'. https://digitalstate.gov.ua/news/govtech/suverennyy-shi-ukrayina-pochynaye-spivpratsiu-z-nvidia.

[60] Ukraine Ministry of Digital Transformation. 2026a. 'Responsible AI Portal / Regulatory Vision - Регулювання'. https://ai.thedigital.gov.ua/vision (August 4, 2026).

[61] Ukraine Ministry of Digital Transformation. 2026b. 'WINWIN - Ukraine's Global Innovation Strategy to 2030'. https://digitalstate.gov.ua/projects/tech/winwin (August 3, 2026).

[62] Ukraine Ministry of Economy and Environment. 2026a. 'Organizational Structure of the National Accreditation System of Ukraine NAAU'. https://naau.org.ua/en/2-struktura-natsionalnoi-sistemi-akreditatsii (August 4, 2026).

[63] Ukraine Ministry of Economy and Environment. 2026b. 'Quality Infrastructure in Ukraine (Standardization, Technical Regulation, Conformity Assessment, Accreditation, Metrology and Metrological Activity)'. https://me.gov.ua/Documents/Detail?id=09768736-6c01-4a40-8a32-1777586060b4&lang=en-GB (August 4, 2026).

[64] Ukrainian Government. 2026. 'National Programme for the Adaptation of Ukrainian Legislation to the Law of the European Union - Кабінет Міністрів України - Про затвердження Національної програми адаптації законодавства України до права Європейського Союзу (*acquis* ЄС)'. https://www.kmu.gov.ua/npas/pro-zatverdzhennia-natsionalnoi-prohramy-adaptatsii-zakonodavstva-ukrainy-do-prava-t10426 (September 9, 2026).

[65] Ukrainian Ministry of Digital Transformation. 2023. *Roadmap for AI Regulation in Ukraine: A Bottom-Up Approach - Дорожня Карта з Регулювання Штучного Інтелекту в Україні*. https://storage.thedigital.gov.ua/files/2/22/363bbcaec30bf9d4e598375fecac3227.pdf.

[66] Ukrainian Verkhovna Rada. 2015. *Law On Technical Regulations and Conformity Assessment - Про технічні регламенти та оцінку відповідності*. https://zakon.rada.gov.ua/go/124-19 (August 4, 2026).

[67] UNESCO, RAM. 2026. *Ukraine: Artificial Intelligence Readiness Assessment Report*. https://unesdoc.unesco.org/ark:/48223/pf0000398153.

[68] United Nations General Assembly. 2022. A/RES/ES-11/1 *Resolution of the United Nations of 2 March 2022 Condemning the Russian Aggression on Ukraine*. https://docs.un.org/en/A/RES/ES-11/1.

[69] 'WINWIN AI Center of Excellence Launched in Ukraine'. https://digitalstate.gov.ua/news/tech/winwin-ai-center-of-excellence-launched-in-ukraine (August 3, 2026).

ACRONYMS

AI	Artificial Intelligence
AIMS	Artificial Intelligence Management System (ISO/IEC 42001)
CAB	Conformity Assessment Body
CE	*Conformité Européenne* (European conformity marking)
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CEPS	Centre for European Policy Studies
DSTU	*Derzhavnyi Standart Ukrainy* (Ukrainian National Standard)
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCC	European Common Criteria-based Cybersecurity Certification Scheme
EUIPO	European Union Intellectual Property Office
GDPR	General Data Protection Regulation
GPAI	General-purpose Artificial Intelligence
HUDERIA	Methodology for assessing risks and impacts of AI systems on human rights, democracy and the rule of law
IP	Intellectual Property
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
JTC 21	CEN-CENELEC Joint Technical Committee 21 on Artificial Intelligence
LLM	Large Language Model
MoDT	Ministry of Digital Transformation of Ukraine
NAAU	National Accreditation Agency of Ukraine
NLF	New Legislative Framework
NPAA	National Programme for the Adaptation of Ukrainian Legislation to the Law of the European Union
UkrNDNC	Ukrainian Scientific, Research and Training Center on Standardization, Certification and Quality Problems
UNIDO	United Nations Industrial Development Organization
WINWIN	WINWIN Global Innovation Strategy to 2030


AI

Vienna International Centre
Wagramerstr. 5, P.O. Box 300
A-1400 Vienna, Austria

+43 1 26026-0

www.unido.org

unido@unido.org

UNITED NATIONS
INDUSTRIAL DEVELOPMENT ORGANIZATION