e-ISSN 2733-2039 print-ISSN 2733-2144

CHAPTER 1
GENERAL PEDAGOGY AND HISTORY OF PEDAGOGY

Core EU Principles for Digital Transformation in Higher Education Institutions: Governance, Trust, and Interoperability

Ellana Molchanova[1]

[1]*PhD (Economics), Associate Professor, Researcher, Scientific Center of Innovative Research, Pussi, Estonia, LA-Print GmbH, Germany, ORCID: https://orcid.org/0000-0001-8043-1916*

Citation:
Molchanova, E. (2025). Core EU Principles for Digital Transformation in Higher Education Institutions: Governance, Trust, and Interoperability. *Pedagogy and Education Management Review*, (4(22), 4–16. https://doi.org/10.36690/2733-2039-2025-4-4-16

Received: November 23, 2025
Approved: December 29, 2025
Published: December 31, 2025

Abstract. *Digital transformation has become a structural condition of higher education because HEIs increasingly depend on platforms and data infrastructures for teaching, assessment, mobility workflows, and institutional decision-making, while simultaneously facing heightened legal, ethical, and operational exposure. The article systematizes core EU principles relevant to digital transformation in HEIs and translates them into actionable governance requirements that connect governance, trust, and interoperability. A structured documentary analysis is applied to EU strategies, binding legal acts, and implementation-oriented frameworks. Qualitative coding is used to derive principle categories and map each category to institutional controls across the lifecycle of selection, deployment, use, monitoring, and retirement. The analysis shows that EU principles become operational in HEIs only when expressed as auditable controls with ownership and indicators. Core requirements include evidence-based adoption for educational value, accessibility as a release gate, GDPR-aligned minimization and DPIA routines, NIS2-aligned cybersecurity risk management, standards-based interoperability, mobility and credential portability governance, and risk-based AI governance under the AI Act. Digital transformation should be governed as socio-technical change where compliance and quality are properties of systems in use, not merely systems purchased. Future work should validate governance indicators across diverse HEI types, test maturity models against outcomes, and examine how interoperability, privacy, and AI oversight can be co-optimized without increasing administrative burden.*

Keywords: *digital transformation; higher education institutions; EU governance; trustworthy digital services; interoperability; GDPR compliance; cybersecurity resilience; NIS2; AI Act; accessibility by design; student mobility; micro-credentials*

JEL Classification: I23; I28; O33; O38; L86; K24

Formulas: 0; fig. 0; tabl. 3; bibl. 15

e-ISSN 2733-2039 print-ISSN 2733-2144

Introduction. Digital transformation has become a structural condition of how higher education institutions operate, teach, and cooperate across borders. Universities and other HEIs increasingly rely on digital infrastructures for learning management, assessment, research data management, student services, mobility workflows, and institutional decision making. This expansion of digital systems creates opportunities for quality improvement, flexibility, and innovation, but it also increases institutional exposure to legal, ethical, and operational risks. In practice, the same platform choices that enable personalization and efficiency can generate new vulnerabilities, including privacy intrusions, cybersecurity incidents, opaque automated decisions, and vendor lock-in that constrains academic autonomy and long-term sustainability. As a result, digital transformation in HEIs is no longer primarily a technical modernization effort. It is a governance challenge that requires institutions to align technology choices with public values, rights-based safeguards, and interoperable cooperation across the European education space.

Within the European Union, the direction of digital transformation is shaped by a combination of policy objectives and regulatory baselines. EU policy frames digitalization as a means to strengthen educational quality, resilience, and inclusion, while also supporting cross-border mobility and recognition of learning outcomes. At the same time, EU legal instruments and standards-oriented initiatives set expectations for data protection, cybersecurity risk management, accessibility, and accountable use of advanced digital systems, including artificial intelligence. For HEIs, this environment implies that "going digital" must be translated into institutional duties: defining purpose and public value, protecting fundamental rights, ensuring accessibility, maintaining operational resilience, and designing interoperability that enables secure exchange of data and credentials across institutions and countries. These duties require coordinated action across academic leadership, IT and security units, data protection roles, procurement, quality assurance, and teaching and learning support services.

This article responds to the need for a coherent institutional interpretation of the EU approach. It identifies core EU principles relevant to digital transformation in HEIs and explains how these principles can be operationalized as concrete governance requirements. The central argument is that successful digital transformation depends on the integration of three dimensions. Governance provides accountability and lifecycle oversight, trust ensures legality, safety, and legitimacy, and interoperability enables scalable cooperation and mobility without sacrificing institutional control over data and academic processes. By translating principles into institutional controls, the article supports HEIs in moving from fragmented digital adoption toward a consistent, auditable, and quality-oriented transformation agenda.

e-ISSN 2733-2039 print-ISSN 2733-2144

Literature review. EU digital transformation in HEIs is framed as a socio technical modernization agenda that links educational quality, institutional resilience, and Europe wide cooperation. The Digital Education Action Plan emphasizes two strategic priorities, namely building a high performing digital education ecosystem and strengthening digital skills and competences, which together push HEIs to professionalize platform governance and learning design rather than treating digitalization as a procurement project (European Commission, 2021). In parallel, the European Strategy for Universities positions universities as key actors in the twin green and digital transitions and highlights the need for coordinated capacity, partnerships, and long term investment (European Commission, 2022). The Digital Decade Policy Programme provides a macro governance frame that strengthens expectations for measurable progress on digital infrastructure, skills, and public service modernization, which indirectly sets performance pressure on HEIs as major public service organizations (European Union, 2022).

A second stream concerns trust and fundamental rights in digital environments. GDPR establishes a rights based baseline for lawful processing, transparency, and accountability in handling student and staff data (European Union, 2016), while NIS2 and the EU Cybersecurity Act reinforce a risk management approach to cybersecurity governance and certification oriented assurance in networked services (European Union, 2022; European Union, 2019). Trust is also extended to identity and authentication, where eIDAS and the European Digital Identity Framework support cross border recognition and secure transactions, which is increasingly relevant for enrolment, credentialing, and student mobility workflows (European Union, 2014; European Union, 2024). A third stream focuses on interoperability and portability in the European Education Area, including micro credentials and the European Student Card Initiative, which operationalize the principle that education related data must be usable across institutions and borders (Council of the European Union, 2022; European Commission, n.d.). Finally, the rise of AI in education brings a dual alignment requirement: values based expectations for trustworthy AI and compliance with the AI Act risk logic, especially where AI is used in admissions support, assessment, or student monitoring (European Commission, 2019; European Union, 2024).

Aim. This article aims to systematize the core European Union principles that should guide digital transformation in higher education institutions (HEIs) and translate them into actionable governance requirements. It focuses on how EU policy, regulatory instruments, and sector initiatives shape institutional choices about infrastructure, learning platforms, data, artificial intelligence, cybersecurity, accessibility, and cross border student mobility.

e-ISSN 2733-2039 print-ISSN 2733-2144

Methodology. The article applies a structured documentary analysis of EU level strategies, binding legal acts, and implementation oriented frameworks. Sources are selected based on relevance to higher education governance and digital transformation, including the Digital Education Action Plan, the European Strategy for Universities, and the Digital Decade Policy Programme, alongside regulatory baselines for privacy, cybersecurity, data governance, and trustworthy AI. The analysis uses qualitative coding to derive principle categories, then maps each principle to institutional controls across the lifecycle of selection, deployment, use, monitoring, and retirement of digital systems.

Results. Digital transformation in higher education institutions (HEIs) should be governed as a socio technical change that affects educational quality, rights, trust, and cross border cooperation. In the EU context, this implies a dual obligation for HEIs: to pursue modernization that demonstrably improves teaching, research, and services, and to ensure that digital systems remain lawful, secure, accessible, and interoperable over their full lifecycle (European Commission, 2021, 2022; European Union, 2016, 2022). The core EU principles below are therefore formulated as institutional requirements rather than as abstract values. Each principle is paired with governance artifacts that make implementation auditable and sustainable.

Purposeful transformation and educational value. Digital initiatives should be justified by an explicit educational or institutional purpose, expressed as measurable value for learners, staff, and institutional performance. A transformation program should require a documented "benefit case" that identifies the learning or service problem, expected outcomes, and conditions of appropriate use (European Commission, 2021). This requirement reduces technology driven adoption and supports quality assurance integration. The minimum institutional standard is a decision trail that links investment to outcomes and enables post implementation evaluation.

Inclusion and accessibility by design. Accessibility is an institutional baseline, not an optional enhancement, because digital learning and student services are core public functions. HEIs should embed accessibility requirements in procurement, design, and testing workflows, and treat accessibility as a release gate for production systems (European Union, 2016, 2019). Inclusion extends beyond technical accessibility to usability across language, socio economic constraints, and heterogeneous digital experience. A mature model institutionalizes accessibility audits and assigns clear ownership for remediation.

Fundamental rights, privacy, and lawful data protection. Data protection must be implemented as a design and governance discipline rather than as a post hoc compliance activity. GDPR implies purpose limitation, minimization, transparency, and accountability, which in HEIs translates

e-ISSN 2733-2039 print-ISSN 2733-2144

into strict control over learning analytics, identity data, and third party processing (European Union, 2016). High impact uses should trigger Data Protection Impact Assessments and clear role definitions for controllers and processors. A practical requirement is an institution wide register of processing activities tied to each digital system and its data flows.

Cybersecurity governance and operational resilience. EU cyber governance emphasizes risk management, incident preparedness, and supply chain controls. For HEIs, this means treating learning platforms, student information systems, mobility services, and research infrastructures as operationally critical services with security baselines, monitoring, and tested incident response procedures (European Union, 2019, 2022). Resilience also includes continuity planning for outages, identity compromise, and vendor failures. The institutional requirement is a governance model with defined responsibilities, minimum controls, and a recurring assurance cycle.

Interoperability and standards based architecture. Interoperability should be pursued as a governance principle that supports cross unit coordination, cross border cooperation, and reduced vendor lock in. The European Interoperability Framework implies legal, organizational, semantic, and technical interoperability, which in HEIs becomes an architectural discipline with shared data models, API governance, and portability planning (European Commission, 2017). Interoperability must be implemented with proportional security and privacy controls, so that data exchange remains necessary, limited, and protected. The institutional requirement is an agreed standards profile for core processes and records.

Cross border mobility enablement. Mobility digitization should be governed as an end to end service that integrates registrar workflows, identity management, documentation exchange, and student support. EU mobility initiatives imply that HEIs must be capable of secure and efficient cross institutional data exchange for mobility processes (European Commission, n.d.). This requires organizational coordination, not only technical connectivity. The institutional requirement is a mobility service owner and a documented process architecture that is interoperable with partner infrastructures.

Trusted credentials and portability of learning outcomes. Micro credentials and other digital attestations require comparability and quality safeguards to remain legitimate across institutions and labor markets. The EU approach emphasizes transparency of learning outcomes, workload, assessment, and quality assurance as prerequisites for recognition (Council of the European Union, 2022). HEIs should define a credential data model, verification logic, and issuance governance, including revocation and fraud prevention. The institutional requirement is a credential governance policy aligned with quality assurance procedures.

Data governance for responsible sharing and reuse. EU data policy highlights trustworthy data sharing while preserving rights based constraints.

In HEIs, data governance requires clear stewardship roles, classification, metadata, access controls, retention, and rules for internal and external sharing (European Union, 2022, 2023). Data reuse should be purpose bound and auditable, especially where analytics may influence student support or institutional decisions. The institutional requirement is a data governance framework that covers both education and research data, with escalation and review routines.

Trustworthy and lawful AI. The EU AI Act introduces a risk based approach with stronger obligations for higher risk uses. For HEIs, this implies an AI use inventory, classification of use cases by impact, and governance that ensures documentation, human oversight, and monitoring, especially in admissions support, assessment related tools, and student risk scoring (European Union, 2024). AI governance must integrate with privacy, security, and quality assurance, because AI systems depend on data and can reshape decision processes. The institutional requirement is a controlled AI lifecycle with registration, review, and periodic re assessment.

Transparent platform governance and accountability. HEIs should formalize how platforms are selected, governed, and exited, because platform dependence can constrain academic autonomy and increase risk. EU digital governance trends strengthen expectations for transparency and accountability in digital services, which supports institutional requirements for vendor documentation, audit cooperation, and portability (European Union, 2022). Platform governance must define decision rights, acceptable risk thresholds, and evidence obligations. The institutional requirement is an accountable governance structure that manages platform risks across procurement, use, monitoring, and retirement.

The table 1 below operationalizes EU principles as controls that can be embedded in policies, procurement, and quality assurance.

The practical implication is that “principles” become measurable only when translated into specific controls with ownership, evidence, and indicators.

A lifecycle governance model treats digital transformation as a continuous institutional capability rather than a sequence of disconnected IT projects. This approach is consistent with the EU emphasis on building a high performing digital education ecosystem and strengthening digital capacity in education and training systems (European Commission, 2021). It also aligns with the EU regulatory logic that obligations and risks emerge throughout the use of a system, not only at the point of purchase. GDPR illustrates this logic through accountability, purpose limitation, and data minimization requirements that must be sustained over time (European Union, 2016). Similarly, NIS2 reinforces that cybersecurity is an organizational risk management responsibility that requires ongoing measures, incident readiness, and supply chain controls (European Union, 2022).

e-ISSN 2733-2039 print-ISSN 2733-2144

Table 1. EU principle to HEI control mapping

EU principle	Key EU anchor	HEI control requirement	Example indicators
Quality and educational value	Digital Education Action Plan	Evidence based adoption and evaluation	Learning outcome gains; completion gaps
Inclusion and accessibility	Web Accessibility Directive; Accessibility Act	WCAG aligned design; accessibility testing	Accessibility audit pass rate
Privacy and data protection	GDPR	Data minimization; DPIAs; vendor DPAs	DPIA coverage; retention compliance
Cybersecurity and resilience	NIS2; Cybersecurity Act	Risk governance; incident processes; assurance	Mean time to detect; supplier compliance
Interoperability	European Interoperability Framework	Open standards; API governance; data models	Shareable records rate
Mobility enablement	European Student Card; EWP	Mobility workflow digitization; secure exchange	Mobility processing time
Credential portability	Micro credentials Recommendation	Standard metadata; QA; recognition rules	Recognition rate across partners
Trustworthy AI	Trustworthy AI guidelines; AI Act	Risk classification; human oversight; documentation	Model register coverage; audit findings

Source: systematized by the author

The AI Act extends lifecycle thinking to AI systems through risk-based obligations, documentation, and oversight expectations that remain relevant as systems are updated or repurposed (European Union, 2024). For HEIs, the core governance question is therefore not whether a platform is "good," but whether it can be governed with evidence, accountability, and continuous improvement across adoption, operation, and change. Lifecycle governance also supports EU goals for interoperability and cross border cooperation, since mobility and credential portability require stable processes, shared standards, and reliable data exchange.

The table 2 links EU aligned governance to the stages where failures typically occur.

EU principles imply continuous governance, because compliance and educational quality are properties of systems in use, not only of systems purchased.

Governance maturity levels provide a practical instrument for institutional self-assessment and benchmarking because they translate principles into observable capabilities and repeatable routines. In the EU context, maturity is not equivalent to the number of platforms adopted or the sophistication of infrastructure. Instead, maturity reflects the degree to which an HEI can demonstrate educational value, rights-based safeguards, operational resilience, accessibility, and interoperability through auditable evidence across the lifecycle of digital systems.

e-ISSN 2733-2039 print-ISSN 2733-2144

Table 2. Lifecycle governance for digital transformation in HEIs

Lifecycle stage	Minimum governance artifacts	Typical high risk failure	EU aligned mitigation logic
Selection and procurement	Risk classification; accessibility and security requirements; DPIA triggers	Vendor lock in; weak safeguards	Interoperability; GDPR; NIS2
Deployment	Configuration baselines; training; transparency notices	Misuse, low adoption	Digital education ecosystem priority
Use in teaching and assessment	Acceptable use policy; academic integrity rules; human oversight	Over automation; unfair outcomes	Trustworthy AI; rights based safeguards
Monitoring	Incident logs; bias and performance checks; audits	Drift; silent harm	Accountability and continuous improvement
Retirement	Data deletion plan; portability plan; lesson learned review	Data remnants; loss of records	GDPR retention limits; interoperability

Source: systematized by the author

This orientation is consistent with EU policy emphasis on building a high performing digital education ecosystem and with regulatory approaches that require ongoing accountability in data protection, cybersecurity, and AI governance (European Commission, 2021; European Union, 2016, 2022, 2024). A maturity model is therefore a governance tool that enables leadership to identify gaps, prioritize investments, and reduce fragmentation across faculties and services by setting consistent institutional standards.

Maturity Level 1: Foundational compliance and fragmented governance. At Level 1, digital transformation is present, but governance remains largely reactive and project-based. Policies exist, yet they are often generic and inconsistently applied across faculties, programs, and services. The institution typically relies on individual departments to select tools and manage digital practices, which creates uneven privacy, security, and accessibility outcomes and increases vendor lock-in risk. Data protection activity is primarily focused on formal documentation after adoption, rather than on proactive risk assessment before deployment, despite the accountability and minimization logic central to GDPR (European Union, 2016). Cybersecurity governance is typically IT-centric and oriented toward infrastructure, with limited coverage of teaching platforms and third-party learning services, which is inconsistent with the EU shift toward organizational risk management emphasized by NIS2 (European Union, 2022). AI use, if present, is mostly unmanaged, with no systematic inventory and minimal oversight for high impact contexts, which becomes problematic under risk-based AI governance expectations (European Union, 2024). Interoperability is handled through ad hoc integrations, and mobility or credential portability processes depend heavily on manual steps. Evidence for quality assurance exists, but it is scattered, non-standardized, and difficult to reuse in audits or reviews.

e-ISSN 2733-2039 print-ISSN 2733-2144

Maturity Level 2: Managed governance with defined controls and evidence routines. At Level 2, the HEI moves from project governance to institution-wide governance by defining minimum controls and implementing repeatable routines. The institution establishes a governance set, including a portfolio register of major systems, standardized procurement and review gates, and clear assignment of service owners. Digital initiatives require benefit cases that tie adoption to educational and service quality outcomes, aligning transformation with the EU policy emphasis on quality and capacity building (European Commission, 2021). Data protection governance becomes more proactive, with defined DPIA triggers, consistent vendor agreements, and documented data flows for major systems, reflecting GDPR accountability requirements (European Union, 2016). Cybersecurity governance expands to cover education platforms and third-party services, including supplier risk checks and incident readiness for learning systems, aligned with the organizational and supply-chain orientation reinforced by NIS2 (European Union, 2022). AI governance begins to formalize through an AI use register and a basic risk classification approach, especially for use cases that affect admissions support, assessment, or student progression. Accessibility governance becomes systematic through procurement requirements, acceptance testing, and remediation workflows. Interoperability is managed through a standards profile for core records and API governance rules, and mobility processes begin to align with cross-institutional exchange expectations. Evidence is increasingly standardized so that quality assurance and audits can reuse the same artifacts rather than reconstructing them.

Maturity Level 3: Integrated, auditable, and continuously improving governance. At Level 3, governance becomes integrated with institutional quality assurance and risk management in a manner that supports continuous improvement and cross-border cooperation. The institution can demonstrate that digital transformation improves educational and service outcomes while maintaining rights-based legitimacy, trust, and interoperability. Benefit cases are linked to measurable indicators and are evaluated post-implementation, with results feeding back into investment decisions. Data governance operates through stewardship roles, metadata practices, retention controls, and monitored access patterns, and it supports responsible data sharing while preserving minimization and purpose limitation (European Union, 2016). Cybersecurity is managed as an institutional capability with tested incident handling, resilience metrics, and supplier assurance practices that cover the full digital ecosystem, consistent with EU governance direction (European Union, 2019, 2022). AI governance is fully lifecycle-based. The HEI maintains a complete inventory of AI-enabled features and systems, applies risk classification, documents purpose and limitations, ensures meaningful human oversight where necessary, and monitors drift and distributional impacts. This approach is aligned with the risk-based

e-ISSN 2733-2039 print-ISSN 2733-2144

governance structure introduced by the AI Act (European Union, 2024). Interoperability is treated as an architectural and governance discipline, with stable data models, well-managed APIs, and verified portability. Mobility and credentialing processes function as end-to-end digital services with reliable cross-institutional exchange, and digital credential practices are integrated with quality assurance to support recognition and trust (Council of the European Union, 2022). At this level, governance artifacts are auditable, consistently maintained, and embedded into routine QA cycles, reducing fragmentation and enabling benchmarking.

The table 3 summarizes the minimum evidence package that an HEI should be able to produce at each maturity level to demonstrate EU-aligned governance.

Table 3. Maturity levels and minimum evidence package

Domain	Level 1 evidence	Level 2 evidence	Level 3 evidence
Strategy and value	Digital strategy statement	Benefit case template and applied cases	Evaluations linked to outcomes and investment decisions
Privacy and data protection	Partial processing records	DPIA playbook and completed DPIAs	Stewardship model, retention monitoring, audited data flows
Cybersecurity and resilience	General security policy	Platform-specific playbooks and exercises	Metrics-driven resilience, recovery testing, supplier assurance
Accessibility and inclusion	Ad hoc checks	Acceptance testing and remediation tracking	Continuous regression testing and barrier reduction program
Interoperability and portability	Point integrations	Standards profile and portability plans	Verified conformance and tested exit strategies
AI governance	No inventory	AI register and basic risk tiers	Lifecycle controls, monitoring, contestability for high impact cases
Mobility and credentials	Manual processes	Digitized workflows with defined owners	End-to-end service reliability and recognized credential governance

Source: systematized by the author

The evidence package clarifies that maturity is demonstrated through maintained artifacts and repeatable routines rather than through one-time policy publication. It also supports benchmarking because the same evidence can be compared across institutions and over time.

Discussion. The findings imply that EU principles function as an integrated governance architecture rather than a checklist of separate compliance topics. The document shows that governance, trust, and interoperability are mutually reinforcing: governance assigns ownership and lifecycle oversight, trust stabilizes legality and legitimacy through privacy, security, and accountable AI, and interoperability enables cross-border cooperation without surrendering institutional control.

This integration matters because HEIs operate as complex service organizations where learning platforms, student information systems, identity services, and mobility processes are tightly coupled. Consequently,

e-ISSN 2733-2039 print-ISSN 2733-2144

a weakness in one domain, such as ad hoc integrations, can propagate into privacy risk, security fragility, and unreliable mobility workflows, undermining educational quality and institutional autonomy.

A central governance challenge is translating principle language into decisions that are measurable and contestable. The principle-to-control mapping in the file is significant because it expresses EU anchors as operational requirements with indicators, such as DPIA coverage, accessibility audit pass rates, and incident detection performance.

This approach supports quality assurance integration by enabling post-implementation evaluation and by reducing the tendency to treat digital adoption as a procurement event. It also clarifies that interoperability must be pursued with proportional privacy and security constraints, since cross-border exchange is valuable only when it remains limited to necessary data and protected by governance routines.

Lifecycle governance further addresses the recurrent institutional failure mode where compliance deteriorates after deployment. The file's lifecycle logic emphasizes that obligations and risks emerge through configuration changes, feature updates, vendor dependencies, and evolving use practices.

This is particularly relevant for AI-enabled functions in admissions support, assessment, and student monitoring, where risk-based oversight requires inventories, documentation, human oversight, and periodic reassessment.

However, lifecycle governance introduces a practical tension: stronger oversight can increase administrative load. The maturity model addresses this by framing progress as capability building, where standardized artifacts allow evidence reuse across audits and reviews, thus reducing duplication over time.

Finally, the maturity levels provide a realistic pathway for institutions with different resources and starting points. Level differentiation clarifies that maturity is evidenced by stable routines and auditable artifacts, not by the sheer number of digital tools adopted.

This is analytically important because it shifts evaluation from technology intensity to governance capacity, which is the more plausible determinant of lawful, resilient, and equitable digital transformation in the European education space.

Conclusion. Core EU principles for digital transformation in HEIs can be operationalized as institutional duties that are measurable across the full lifecycle of digital systems. These duties include evidence-based adoption for educational value, accessibility by design, GDPR-aligned privacy governance, NIS2-aligned cybersecurity risk management, standards-based interoperability, mobility enablement, trustworthy credential portability, responsible data governance, and risk-based AI oversight. The central implication is that digital transformation is not primarily technical

modernization, but a governance problem where legitimacy, quality, and cooperation depend on clear ownership, auditable controls, and continuous improvement routines.

A lifecycle and maturity-based approach supports implementation because it aligns governance intensity with risk and institutional capability. When HEIs embed these controls into procurement, change management, monitoring, and exit planning, they reduce vendor lock-in, improve service resilience, and enable cross-border cooperation while maintaining rights-based safeguards.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Council of the European Union. (2022). *Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability (2022/C 243/02).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj%3AJOC_2022_243_R_0002
2. European Commission. (2017). *European interoperability framework (EIF).* https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework
3. European Commission. (2019). *Ethics guidelines for trustworthy AI.* https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
4. European Commission. (2021). *Digital Education Action Plan (2021–2027).* https://education.ec.europa.eu/focus-topics/digital-education/plan
5. European Commission. (2022). *European strategy for universities.* https://education.ec.europa.eu/sites/default/files/2022-01/communication-european-strategy-for-universities-graphic-version.pdf
6. European Commission. (2025). *European Student Card Initiative.* https://erasmus-plus.ec.europa.eu/european-student-card-initiative
7. European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
8. European Union. (2019). *Regulation (EU) 2019/881 (Cybersecurity Act).* https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
9. European Union. (2022). *Directive (EU) 2022/2555 (NIS2 Directive).* https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
10. European Union. (2022). *Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022D2481
11. European Union. (2022). *Regulation (EU) 2022/2065 (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
12. European Union. (2022). *Regulation (EU) 2022/868 (Data Governance Act).* https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng
13. European Union. (2023). *Regulation (EU) 2023/2854 (Data Act).* https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
14. European Union. (2024). *Regulation (EU) 2024/1689 (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

15. European Union. (2024). *Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.* https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng