

EU Data Governance, AI Ethics, and Responsible Digitalisation in Higher Education: A Compliance–Capability Framework for Universities

Igor Britchenko¹, Inga Lysiak²

¹Doctor of Science (Economics), Professor, University of the National Education Commission, Krakow, Poland, ORCID: <https://orcid.org/0000-0002-9196-8740>

²Ph.D. (Technical Science), Eng., Institute of Management, Economics and Logistics, Pomeranian University in Starogard Gdanski, Starogard Gdanski, Poland, ORCID: <https://orcid.org/0009-0001-8450-3216>

Citation:

Britchenko, I., & Lysiak, I. (2025). EU Data Governance, AI Ethics, and Responsible Digitalisation in Higher Education: A Compliance–Capability Framework for Universities. *Public Administration and Law Review*, 4(24), 12–19. <https://doi.org/10.36690/2674-5216-2025-4-12-19>

Received: November 18, 2025

Approved: December 29, 2025

Published: December 31, 2025



This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY-NC 4.0\) license](#)



Abstract. Higher education institutions function as complex data ecosystems that simultaneously act as data holders, data users, and data intermediaries across teaching, research, and administration. This complexity makes EU data governance and responsible AI directly relevant to universities because compliance increasingly depends on organisational capability linked to fundamental rights protection, cybersecurity resilience, and market integrity. Sector scale amplifies risk because routine administrative errors, biased automated decisions, or weak access control can produce cumulative harm and erode institutional trust. The objective of this abstract is to formulate a compliance–capability framework that aligns EU data governance instruments with AI ethics and responsible digitalisation requirements and translates them into implementable institutional mechanisms. The study applies qualitative policy and legal analysis through doctrinal mapping of the EU regulatory stack relevant to universities, including the GDPR, the Data Governance Act, the Data Act, and the AI Act. It synthesises trustworthy AI ethics frameworks and integrates descriptive indicators on cross-border mobility, digital skills, and cyber risk to support risk-based governance design. Criteria-based institutional design reasoning is used to connect legal duties to governance roles, evidence artefacts, and monitoring indicators across the data and AI lifecycle. Results show that universities face overlapping duties because a single workflow may combine personal data processing, research data sharing, learning analytics, and AI-supported decision support. The GDPR remains foundational, while the Data Governance Act structures trusted reuse, the Data Act addresses fair access, and the AI Act introduces risk-based transparency, oversight, and AI literacy expectations. Further research should test interoperability models for research data sharing and measure how maturity in training and oversight reduces rights violations and incident rates.

Keywords: EU data governance; higher education; responsible digitalisation; GDPR; Data Governance Act; Data Act; AI Act; trustworthy AI; learning analytics; research data governance; interoperability; cyber resilience.

JEL Classification: I23, I28, K24, L86, M15, O33, O38

Formulas: 0; **fig.:** 0; **table:** 3; **bibl.:** 18

Introduction. Higher education institutions operate as complex data ecosystems that combine public-interest missions with platform-mediated teaching, cross-border research collaboration, and large-scale administrative processing. This reality makes universities simultaneously data holders, data users, and data intermediaries, often within the same institutional workflow. EU digital regulation increasingly treats data governance and responsible AI as inseparable from fundamental rights, cybersecurity resilience, and market integrity, which shifts compliance from a purely legal exercise to an organisational capability. The practical challenge for higher education is therefore not whether to digitalise, but how to digitalise in a way that is lawful, ethically grounded, and operationally auditable across teaching, research, and governance functions. This is especially urgent given the scale of the sector: in 2023, the EU reported 18.8 million tertiary education students, indicating that even routine administrative errors can produce high aggregate harm. At the same time, digital skills gaps remain structural because only 56% of EU citizens aged 16–74 had at least basic digital skills in 2023, while the EU target for 2030 is 80%. In such conditions, responsible digitalisation in higher education must be designed for uneven user capability, unequal access, and heightened exposure to social engineering and identity compromise.

Literature Review. Research on EU data governance has evolved from privacy-centric compliance toward ecosystem governance that emphasises lawful access, trusted sharing, interoperability, and safeguards against misuse. The Data Governance Act institutionalises a governance layer for data sharing through regulated data intermediation services and frameworks for the reuse of certain public sector data, which is particularly relevant for university research consortia and cross-sector data spaces. The Data Act adds a complementary logic focused on fair access to and use of data, addressing contractual imbalance and exceptional public-interest access, which affects data-intensive research partnerships and procurement of connected services used in campuses and laboratories.

In parallel, AI ethics literature increasingly converges with “governance by design,” where ethical principles are operationalised via documentation, transparency, risk assessment, and accountability structures. The EU Ethics Guidelines for Trustworthy AI propose a lawful, ethical, and robust approach and articulate requirements such as transparency, human oversight, and accountability that have become de facto design expectations in academic AI deployments. Global normative instruments reinforce this direction, notably UNESCO’s Recommendation on the Ethics of AI and the OECD AI Principles, which underline human rights alignment, fairness, and responsible stewardship across the AI lifecycle.

Higher education digitalisation policy literature emphasises institutional capacity and pedagogical inclusion. The European Commission’s Digital Education Action Plan frames digital education as a

systemic transformation agenda, not a technology procurement agenda, and supports the view that governance arrangements must integrate skills, infrastructure, and trust. Research data governance further highlights the centrality of FAIR data practices and federated infrastructures. The European Open Science Cloud (EOSC) is explicitly positioned as a pan-European environment enabling reuse of research data and services, which strengthens the argument that data governance in universities must support cross-border sharing while preserving compliance with privacy, security, and IP constraints.

Aims. This article aims to develop a compliance–capability framework for universities that aligns EU data governance instruments with AI ethics and responsible digitalisation practices. It focuses on translating regulatory requirements into implementable institutional mechanisms across teaching and learning analytics, research data management, and administrative decision systems.

Methodology. The study applies a qualitative policy and legal analysis methodology. First, it conducts a structured doctrinal mapping of the EU regulatory stack relevant to higher education data and AI governance, including the GDPR, the Data Governance Act, the Data Act, and the AI Act. Second, it synthesises ethics frameworks from the EU Ethics Guidelines for Trustworthy AI, UNESCO, and the OECD to derive operational governance requirements suitable for university contexts. Third, it integrates descriptive statistics from Eurostat and selected cybersecurity reporting to contextualise scale, cross-border mobility, and threat exposure in higher education systems. Finally, it uses criteria-based institutional design reasoning to propose summary governance tables that connect legal duties to roles, evidence artefacts, and monitoring indicators.

Results. Higher education institutions face overlapping legal duties because a single digital workflow can simultaneously involve personal data processing, research data sharing, learning analytics, and AI-supported decision support. GDPR remains the core rights framework for personal data protection and impact assessment duties where high risk to individuals is likely. The Data Governance Act supplies mechanisms for trusted sharing and reuse, particularly relevant to public sector data reuse and regulated intermediation. The Data Act adds rules on fair access and use, affecting contractual governance and situations where data are needed for tasks in the public interest. The AI Act contributes a risk-based compliance structure that reshapes institutional responsibilities through transparency obligations, governance duties for high-risk uses, and expectations of AI literacy and oversight capacity in organisations deploying AI systems.

Table 1 summarises how key EU instruments translate into concrete university governance duties. The intent is to support compliance scoping and internal control design by linking each instrument to typical higher education use cases and evidence artefacts.

Table 1. EU data governance and AI governance instruments relevant to higher education

Instrument	Primary governance focus	Typical HE use cases	Core university deliverables
GDPR (Reg. (EU) 2016/679)	Fundamental rights in personal data processing	Student records; HR; admissions; learning analytics; research with personal data	Lawful basis register; DPIA where applicable; access controls; retention and deletion rules; breach response
Data Governance Act (Reg. (EU) 2022/868)	Trusted data sharing and data intermediation; public sector data reuse frameworks	Research consortia; data spaces participation; inter-university data exchange	Data sharing governance; intermediation compliance checks; cataloguing and access conditions
Data Act (Reg. (EU) 2023/2854)	Fair access to and use of data; contractual imbalance; exceptional public-interest access	Procurement of connected services and campus IoT; research partnerships with data holders	Contract clauses; portability and access governance; documentation for exceptional access scenarios
AI Act (Reg. (EU) 2024/1689)	Risk-based AI compliance; transparency; governance for high-risk systems	Proctoring; automated admissions triage; student support profiling; research AI deployments	Risk classification; transparency notices; human oversight model; technical documentation alignment

Source: systematized by the authors

Table 1 indicates that the most effective compliance strategy in universities is integrative rather than siloed. Institutions reduce risk when they treat data governance, AI ethics, and cybersecurity controls as one auditable system that produces reproducible evidence of lawful and responsible practice.

Responsible digitalisation requires that universities govern data and AI across the full lifecycle, from collection and generation through sharing, model training, decision outputs, and retention. Digital education policy reinforces that inclusion and quality depend on organisational readiness, not only on tools, which supports embedding governance into teaching design and staff development. The open science agenda introduces additional complexity: EOSC promotes cross-border reuse of research data and services, which makes interoperability and controlled access central to compliant sharing.

Table 2 converts the ethics and governance literature into a practical lifecycle matrix. It connects AI ethics requirements, data governance duties, and operational evidence artefacts that universities can implement and audit.

Table 2 shows that ethics becomes actionable when it is converted into controls, documentation, and remedy pathways. For universities, the decisive indicator of responsibility is not an abstract principle statement, but the existence of a governance chain that can explain, justify, and correct digital decisions.

Table 2. Responsible digitalisation lifecycle controls in higher education (governance matrix)

Lifecycle stage	Main risk in HE	Governance control	Evidence artefact for audit
Data collection and consent	Over-collection; unclear lawful basis; unequal power relations	Purpose limitation; minimisation; lawful basis clarity; accessibility of notices	Data inventory; privacy notices; consent logs where used; DPIA triggers (GDPR)
Data access and sharing	Uncontrolled dissemination; re-identification; contractual imbalance	Access governance; de-identification controls; data sharing agreements	Access logs; DSAs; risk assessment notes; sharing registers (DGA, Data Act)
Model development and procurement	Hidden training data; vendor opacity; biased outputs	Documentation requirements; procurement due diligence; bias testing	Model cards or equivalent; supplier documentation; evaluation reports (AI Act; Trustworthy AI)
Deployment in decision processes	Automation bias; unfair impact; lack of contestability	Human oversight; transparency to affected persons; appeal and remedy pathways	Oversight SOPs; transparency notices; complaint and appeal logs (AI Act; OECD)
Retention and preservation	Excessive retention; inability to reproduce results; loss of research value	Retention schedules; research data management plans; controlled archiving	Retention policy; RDM plans; repository logs (EOSC context)

Source: systematized by the authors

Several indicators demonstrate why responsible digitalisation in higher education must be designed for scale and adversarial conditions. The EU had 18.8 million tertiary students in 2023, and cross-border mobility is substantial, with 1.76 million tertiary students from abroad in the EU in 2023, equal to 8.4% of all tertiary students. This creates complex governance needs for cross-border data transfers, multilingual transparency, and consistent procedural rights protection. Meanwhile, societal capability constraints remain significant because only 56% of EU citizens aged 16–74 had at least basic digital skills in 2023, while the EU’s Digital Decade ambition sets a target of 80% by 2030.

Cyber risk evidence reinforces the urgency. A Verizon education-focused brief published in December 2025 reported that 66% of higher education organisations were hit by ransomware, which indicates that continuity and recovery planning are governance imperatives for universities, not only IT priorities.

Table 3 consolidates scale indicators and interprets them as governance requirements. The logic is that compliance must be resourced and institutionalised in proportion to exposure.

Table 3. Selected statistics relevant to responsible digitalisation in higher education (EU context)

Indicator	Reported value	Governance implication for HE
Tertiary students in the EU (2023)	18.8 million	High-volume processing requires standardised controls, role clarity, and automated compliance evidence
Students from abroad in EU tertiary education (2023)	1.76 million (8.4%)	Cross-border transparency, consistent rights handling, and interoperable governance for mobility data
Adults with at least basic digital skills in the EU (2023)	56%	Digital inclusion measures and usable transparency become risk controls, not only pedagogy choices
EU 2030 target for basic digital skills	80%	Universities become central actors in meeting the target, implying measurable digital skills strategies
Higher education organisations hit by ransomware	66%	Mandatory resilience: backups, recovery tests, least privilege, incident governance, and continuity planning

Source: systematized by the authors

Table 3 supports a practical conclusion: responsible digitalisation in higher education must be designed as a resilience-oriented governance programme. The combination of scale, mobility, skills gaps, and ransomware exposure implies that ethics and compliance must be operationalised through training, documentation, and tested response capacity.

Discussion. The results suggest that EU data governance and AI ethics converge on one institutional requirement for higher education: demonstrable accountability. GDPR establishes rights and procedural expectations for high-risk processing, while the Data Governance Act and Data Act promote lawful access and fair reuse mechanisms that are increasingly relevant for university partnerships and participation in sectoral data spaces. The AI Act extends this convergence by imposing a risk-based compliance logic that compels universities to define oversight roles, adopt transparency practices, and institutionalise documentation for certain AI uses.

From an ethics perspective, the EU Trustworthy AI framework, UNESCO, and OECD instruments provide a stable normative baseline, but their practical value depends on translation into operational controls like those summarised in Table 2. This translation is particularly important in higher education because universities deploy AI in ethically sensitive contexts, such as assessment integrity, student support, admissions, and research evaluation, where fairness, transparency, and contestability are decisive for legitimacy. Digital education policy further implies that responsibility is not only a compliance outcome but also an educational outcome, because universities shape the skills and civic expectations of future professionals.

The discussion also indicates that open science infrastructures intensify governance requirements because they normalise cross-border reuse of

research data and services. EOSC illustrates how the European model seeks to scale data-driven science through federated access, which increases the importance of interoperable metadata, lawful sharing conditions, and consistent security controls.

Finally, ransomware prevalence in higher education demonstrates that responsible digitalisation must be resilience-centred. Without tested recovery processes and governance of access privileges, universities risk losing not only service continuity but also the integrity of research records and the credibility of academic decision processes.

Conclusions. EU data governance and AI governance are increasingly designed as ecosystem regulation, and higher education institutions must respond with integrated governance systems rather than fragmented compliance. GDPR provides the fundamental rights baseline for personal data, while the Data Governance Act and Data Act operationalise trusted sharing and fair use rules that directly affect research collaboration and university procurement relationships. The AI Act strengthens the accountability layer by requiring risk-based controls, transparency, and documentation that can be audited in practice, which is essential for legitimacy in education-related AI uses.

Empirical indicators show why universities must institutionalise responsibility as capability: the sector's scale, the mobility intensity of the student population, persistent digital skills gaps, and high ransomware exposure together justify governance investment. Responsible digitalisation in higher education is therefore best implemented through lifecycle governance: clear lawful bases, controlled sharing, documented model procurement and evaluation, human oversight and remedy pathways, and resilient preservation of records and research data.

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

Conflict of interest. The authors 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 authors 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's 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). Path to the Digital Decade: The EU's plan to achieve a digital Europe by 2030. <https://www.consilium.europa.eu/en/policies/path-to-the-digital-decade-the-eu-s-plan-to-achieve-a-digital-europe-by-2030/>
2. European Commission. (2019). Ethics guidelines for trustworthy AI. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

3. European Commission. (2020). A European strategy for data (COM/2020/66 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0066>
4. European Commission. (2021). Digital Education Action Plan 2021–2027. <https://education.ec.europa.eu/focus-topics/digital-education/actions>
5. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
6. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/868 (Data Governance Act). <https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng>
7. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/2854 (Data Act). <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>
8. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
9. Eurostat. (2024). Digitalisation in Europe: 2024 edition (interactive publication). <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024>
10. Eurostat. (2024). Skills for the digital age (Statistics Explained). <https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=628712>
11. Eurostat. (2024). Tertiary education statistics (Statistics Explained). https://ec.europa.eu/eurostat/statistics-explained/index.php/Tertiary_education_statistics
12. Eurostat. (2025). 8.4% of tertiary students in the EU came from abroad. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250822-1>
13. Lysiak, I. (2025). EU Best Practices on Digital Transformation, AI and Inclusion in Universities. In Iu. Kostynets (Ed.). *Contemporary issues of digitalization in Economics, Management, Education*. (2025). Monograph. 350 p. (pp. 293-320). Scientific Center of Innovative Research. <https://doi.org/10.36690/CIDI-EME-293-320>
14. OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD Legal Instrument 0449). <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
15. OECD. (2024). AI principles. <https://www.oecd.org/en/topics/ai-principles.html>
16. Research and Innovation, European Commission. (2025). European Open Science Cloud (EOSC). https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science/european-open-science-cloud-eosc_en
17. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. <https://unesdoc.unesco.org/ark%3A/48223/pf0000380455>
18. Verizon. (2025). Reading, writing and ransomware: Education. <https://www.verizon.com/business/resources/whitepapers/Reading-writing-ransomware-education.pdf>