



Structured Document Review Report (Task 3.1 – Partner)

(For completion by each partner institution as part of WP3 Policy and Regulatory Framework Analysis)

Section 1: Partner & Submission Info

Purpose: To capture basic information about your institution and submission.

Instructions: Please fill in all fields below. Indicate who coordinated the review within your institution.

Partner Institution	Country	Reviewer(s)	Date of Submission
POLITO	Italy	Antonelli Dario	16/12/2025

Section 2: List of Documents Reviewed

Purpose: To provide metadata for all documents selected for review.

Instructions: List the 4–6 national and institutional documents your institution analysed. Include official titles and details. Use one line per document.

For each document, provide brief metadata in a table:

Doc ID	Title	Issuing Authority	Year	Type (Law/Strategy/Policy/Guideline)	Scope (National/Institutional)	Short Description
D26	Indicazioni per l'impiego di soluzioni di Intelligenza Artificiale	POLITO	2025	Guideline	Institutional	This document outlines the characteristics, risks, and preliminary recommendations for the conscious use of Generative AI solutions by university personnel, particularly emphasizing data confidentiality and human responsibility.
D27	Recommendations on the USE OF AI IN EDUCATION	POLITO	2025	Guideline	Institutional	These recommendations provide guidance on the appropriate use of Generative AI tools in educational activities, focusing on master's theses and academic assessments.
D28	CODICE DI COMPORTAMENTO DEL POLITECNICO DI TORINO	POLITO	2014	Policy	Institutional	This Code establishes the minimum duties of diligence, loyalty, impartiality, and good conduct required of all employees, collaborators, and staff of the Politecnico di Torino.
D29	Linee guida per il corretto comportamento degli studenti	POLITO	2021	Guideline	Institutional	These guidelines define academic and non-academic misconduct by students, outlining behaviors contrary to university principles and the disciplinary actions that may follow.
D30	ISTRUZIONI OPERATIVE IN MATERIA DI	POLITO	2021	Guideline	Institutional	These instructions provide mandatory operational guidelines for authorized personnel on the lawful, secure, and



	TRATTAMENTO DATI					correct handling of personal data in both electronic and paper formats.
D31	piano Strategico di Ateneo 2024-2030	POLITO	2024	Strategy	Institutional	This Strategic Plan outlines the Politecnico di Torino's trajectory for 2024-2030, focusing on becoming an international, competitive, and recognized institution undergoing digital and green transitions.
D32	Piano per la Trasformazione Digitale 2024-2026	POLITO	2024	Strategy	Institutional	This plan supports the planning, execution, and monitoring of ICT actions enabling the University's digital transformation, aligning with national AGID guidelines for the Public Administration.
D33	REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679	POLITO	2022	Regulation	Institutional	This Regulation establishes rules for the protection of personal data at the Politecnico di Torino in implementation of EU Regulation 2016/679 (GDPR).
D49	Linee guida per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche	Ministero dell'istruzione e del merito (Ministry of Education and Merit)	2025	Guideline	National	The guidelines provide the reference principles, ethical and technical requirements, and operational instructions for integrating Artificial Intelligence into Italian school institutions.
D50	STRATEGIA ITALIANA PER L'INTELLIGENZA ARTIFICIALE 2024-2026	Dipartimento per la Trasformazione Digitale (DTD) and AGID (Agenzia per l'Italia Digitale)	2024	Strategy	National	This document lays out the Italian national plan for the research, development, application, and governance of Artificial Intelligence across public and private sectors for the 2024-2026 period.
E5	REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (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	The European Parliament and the Council of the European Union	2024	Law	Supranational	This regulation, known as the Artificial Intelligence Act (AI Act), establishes harmonized, risk-based rules for the development, placing on the market, and use of AI systems across the European Union.

Section 3: Cross-Document Analysis by Category

Purpose: To summarise what the reviewed documents say under each key WP3 category.





Instructions: Use this table to capture relevant extracts or themes found across your reviewed documents.

For all the reviewed documents together, partners summarise findings under each coding category:

Category	Key Extracts (Doc IDs)	Observations (coverage, strengths, weaknesses)
Ethics & Integrity	Human Responsibility: The responsibility for the production of a document "remains solely with the person" (D26). Plagiarism/Misconduct: Guidelines define academic and non-academic misconduct (D29). Code of Conduct: Establishes minimum duties of diligence, loyalty, impartiality, and good conduct for all personnel (D28). Academic Originality: The contribution of academic work "should originate from human intelligence" (D27).	The framework firmly anchors responsibility and integrity in human judgment, despite the use of AI tools. D26 directly addresses the ethical dilemma of GenAI by mandating human oversight. D29 provides the disciplinary framework, but D27 notes the current technical difficulty (probabilistic nature of AI detectors) in enforcing the plagiarism rules against AI-generated content.
Data Privacy & Security	Control and Transfer: "Any data and information provided [to external AI services] may be de facto handed over to the service provider" (D26). Prohibition: Explicitly recommends not sharing "personal, sensitive, copyrighted, or reserved information" with external AI systems (D26). Legal Basis: Full Regulation on Personal Data Protection (D33) implements the GDPR. Operational Security: Defines secure data handling, use of encryption for removable media, and incident reporting (D30).	Data security is robustly addressed for internal systems (D33, D30). However, D26 reveals a significant gap and inconsistency: the current operational reality of GenAI (external cloud services) fundamentally conflicts with the institutional data control mandate, leading to a de facto ban on sensitive data use with these tools.
Equity & Inclusion	Strategic Goal: The Strategic Plan (D31) includes a focus on "An International University" and promotes a supportive environment. Code of Conduct: Aims to protect the "dignity of workers and students" (D28). AI Bias: Recommends checking GenAI results for	D28 and D31 establish a general institutional commitment to dignity and inclusion. D26 is the only document that explicitly addresses algorithmic bias (a key element of AI ethics), advising users to be aware of





	"prejudices related to the choice of training documents" (D26).	and verify potential prejudices in AI-generated content.
Transparency & Explainability	Declaration of Use: Users should "explicitly declare the use of Artificial Intelligence systems" (D26). Probabilistic Results: AI detection tools "provide a probabilistic result" and have "no legal value" (D27).	The primary mechanism for transparency is self-declaration by the user (student/staff) when using GenAI (D26). D27 highlights the current lack of explainability and certainty in AI detection tools, which forces the university to rely on non-technical verification methods (e.g., oral discussion) for originality.
Governance Structures	Strategic Alignment: Digital Transformation Plan (D32) is aligned with the national Agency for Digital Italy (AGID) and involves the Responsible for Digital Transition (RTD). Disciplinary Body: The Disciplinary Commission is responsible for analyzing misconduct and imposing sanctions (D29). Data Roles: Defines roles like the Data Protection Officer (RPD/DPO) and Data Processors (D33, D30).	Governance is clear and vertically aligned with national digital and privacy bodies. Institutional processes and responsibilities are formally defined across general conduct (D28, D29), data protection (D33), and digital transformation (D32).
Technical Standards & Interoperability	IT Infrastructure: The Digital Transformation Plan (D32) aims to enhance and consolidate the role of the IT structure and improve existing IT Service Management (ITSM) tools. Data Storage: Recommends saving data "preferably on network resources or in the cloud made available by the University" (D30).	The focus is on consolidating and improving <i>internal</i> IT infrastructure and services (D32, D30). The documents do not detail specific technical standards for AI models but rather focus on the secure integration of existing/new systems into the institutional IT ecosystem.
Accountability & Liability	Human Responsibility: "Responsibility in the production of a document remains solely with the person who produces it" (D26). Sanctions: Violations of the conduct guidelines (D29) and the code of conduct (D28) are subject to disciplinary action and sanctions.	The institutional framework clearly assigns legal and academic accountability back to the individual (staff or student) for their final output, regardless of the AI tools used in the process (D26). This approach mitigates the





		institution's liability regarding potential AI errors or misconduct.
Sustainability	Strategic Pillar: The Strategic Plan (D31) defines a "PoliTO in Transition" which includes environmental sustainability and the goal of becoming a "zero-emission university". Digital Plan: A goal is to "Enrich Action Plan data with budget and sustainability impact of the solutions" (D32).	Sustainability is a high-level strategic commitment (D31) and is mandated as a consideration for new digital solutions within the operational plan (D32). However, there are no specific AI-related guidelines (e.g., managing the carbon footprint of AI training models) within the technical documents (D26, D27, D30).

Replicate table for each document

Section 4: Gaps, Overlaps, and Inconsistencies

Purpose: To identify where your national/institutional frameworks are strong, missing, or contradictory.

Instructions: Use bullet points or short paragraphs to describe gaps, overlaps, and inconsistencies. Refer to specific document IDs when possible.

- **Gaps:** Elements not covered in any of the reviewed documents (e.g., no reference to AI in teaching).
- **Overlaps:** Common elements repeated across multiple documents.
- **Inconsistencies:** Conflicts between national vs. institutional policies or contradictions within documents.

Doc ID:	D49 / D50 National policies
Gaps:	• Specific Legal Liability Framework: D50 highlights a current gap regarding the "emergent issues of attributing responsibility for cyberattacks using AI tools". While D50 mandates collaboration between the new AI Agency and the National Cybersecurity Agency (ACN), the document itself does not provide the concrete legal mechanism or framework to resolve this complex attribution problem. • Sector-Specific Operational Guidelines Beyond Education: While D50 provides strategic pillars for the Public Administration and Enterprises, the documents lack the level of detailed operational guidelines (like D49 provides for schools) for other critical high-risk sectors. Detailed national compliance procedures for specific high-risk uses in areas like healthcare or banking, as required by E5, are not yet articulated in a dedicated guideline document. • Monitoring and Evaluation Metrics for Education: D49 provides operational instructions, but a detailed, independent framework for monitoring and evaluating the success and impact of the AI introduction in schools, beyond D50's general monitoring section, is not explicitly defined in the education guideline itself.





Overlaps	The national framework (D50 and D49) is heavily influenced by and aligns with the supranational legal framework (E5). • Ethical and Foundational Principles: All three documents share a common foundation in principles of trust, transparency, fairness, and accountability in AI. D49, for instance, dedicates a section to "Requisiti etici dell'IA," directly mirroring the ethical considerations that underpin E5. • Regulatory Alignment: D50 explicitly states its role in implementing and nationalizing the European regulatory framework (E5), viewing the AI Act as the foundational structure for Italy's AI governance. • Focus on Skills and Training: Both national documents prioritize the development of AI skills and awareness. D50 includes a "Strategia per la Formazione" (Strategy for Training) at the national level, while D49 provides the specific, detailed operational instructions for integrating AI into school institutions.
Inconsistencies	• Risk of Jurisdictional Overlap ("Over Regulation"): D50 explicitly acknowledges an inconsistency risk stemming from "over regulation" and the "superimposition of disciplines and competences" ("sovrapposizioni di discipline e competenze") among existing regulatory bodies (like Banca d'Italia and Consob) and the newly created AI Agency. This reveals an internal structural conflict in the Italian implementation of E5, which the new national Agency is intended to resolve by simplifying application. • Tension Between Simplification (D50) and Stringent Compliance (E5): D50 stresses that the new Agency must allow for an "intelligible application" that favors the productive system and innovation. This goal of simplification and innovation promotion is in potential tension with the inherently complex and stringent risk-based compliance regime mandated by the legal requirements of E5, especially for high-risk AI systems.
Doc ID:	(D26, D27, D28, D29, D30, D31, D32, D33) Institutional framework at POLITO
Gaps:	• Legal/Contractual Framework for High-Risk AI (E5): There is no specific institutional document that comprehensively outlines the <i>compliance procedure</i> for the implementation and use of high-risk Artificial Intelligence systems (as defined by the European AI Act - E5) within the university. The current focus is on GenAI (D26, D27), but an internal protocol is missing for the audit and adaptation of pre-existing AI systems in sensitive areas such as administration, HR, or student services. • Dedicated Financial Strategy for Digital Transition: Although the Strategic Plan (D31) and the PTTD (D32) indicate digital transformation as a primary objective and an enabling factor, there is no document illustrating the long-term <i>financial strategy</i> or <i>resource allocation plan</i> to support all the necessary projects (ICT, infrastructural, training) needed to bridge the "competence gap" and build the new infrastructure (D31, D32). • Institutional Policy on AI and Open Science: The Strategic Plan (D31) mentions the "Open Science Study Center" and the enhancement of the data infrastructure for research. However, a formal policy is not available that defines the rules for Open Science (data sharing and accessibility) and the use of AI (particularly GenAI) in the production and dissemination of scientific knowledge, beyond the general recommendations for citation (D26, D27).
Overlaps	• Digital Transformation as a Strategic Objective: Digitalization is not just a technical project (D32), but a strategic pillar (D31). The Strategic Plan (D31) frames it as a paradigm shift involving "people, technologies, and processes", while the PTTD (D32) translates it into concrete actions aligned with AGID (the Italian Digital Agency).





	• Centrality of Security and Data Protection: The principles of Security and Privacy by design permeate the framework. The Privacy Regulation (D33) and Operating Instructions (D30) define traditional roles and procedures (RPD/DPO, CISO, data breach), while the AI Guidelines (D26) reinforce the prohibition against entering sensitive data into external AI tools, reiterating caution in data management. • Emphasis on Training and Competencies: The need to raise competency levels is recognized as fundamental for the entire community. The University promotes "Training" activities for staff (D33, D30), and the Strategic Plan (D31) and PTTD (D32) insist on the need to invest to "close the competence gap" for personnel. • Human Responsibility and Originality: The AI-specific documents (D26, D27) agree that AI is only a support tool: ○ Responsibility for the material produced "remains with the person" (D26). ○ The "spark" of the thesis contribution "should originate from human intelligence" (D27).
Inconsistencies	• Conflict between Control (D33/D30) and GenAI Functionality (D26): ○ The institutional Data Protection framework (D33, D30) is based on the principle of the University's control over the data and platforms used. ○ The AI Guidelines (D26) highlight that GenAI tools operate in a cloud-based mode, transferring the data entered ("any data and information") to third-party systems (external providers), a process that is "de facto handed over to the service provider" without guarantee of confidentiality. Result: A fundamental inconsistency exists between the operational reality of current AI technologies and the Polytechnic's data protection control model, which D26 attempts to resolve with a prohibition ("Do not insert any personal, sensitive, copyrighted, or reserved information") rather than a technical/legal compliance solution for the institutional use of these tools. • Enforcement of Student Conduct (D29) vs. AI Assessment (D27): ○ The Student Code of Conduct Guidelines (D29) establish the basis for disciplinary action against "academic misconduct" (e.g., plagiarism, unauthorized use of material). ○ The Recommendations on AI in Education (D27) explicitly admit that AI detection tools only provide a "probabilistic" result and have "no legal value". ○ Result: There is a conflict between the rule (D29, which requires certain identification of the violation for the application of a disciplinary sanction) and the current technological capacity for verification (D27), forcing the institution to base the evaluation of originality more on the oral defense and the student's self-declaration than on the objective verification of the written work.

Section 5: Identified Risks

Purpose: To identify any potential ethical, legal, pedagogical, social, or technical risks that emerge from the policies you analysed.

Instructions: List any risks revealed by the documents or by the absence of clear guidance. Indicate whether the institution has a response or mitigation measure.





Risk ID	Description (of Risk)	Level	Potential Impact	Source Doc ID	Mitigation or Policy Response
R01	Data Leakage and Privacy Violation via External AI (Legal/Technical): The use of external, non-controlled Generative AI (GenAI) systems transfers institutional data and user input to third-party providers, violating the principles of data control (GDPR/D33) and risking the unauthorized disclosure of reserved or sensitive information.	High	Legal penalties (GDPR fines), institutional data breach, loss of user trust.	D26, D33, D30	Prohibition: D26 explicitly mandates: "Do not share with these systems reserved or protected information, personal data, etc." D30/D33 provide the foundational internal data protection framework.
R02	Compromised Academic Integrity and Pedagogical Shift (Pedagogical/Integrity): The inability of current AI detection tools to provide legally binding evidence (they are "probabilistic" and have "no legal value" - D27) undermines the enforcement of student misconduct rules (D29) against AI-assisted plagiarism.	High	Devaluation of qualifications, lack of confidence in assessment results, increased administrative burden on disciplinary bodies.	D27, D29	Pedagogical Redesign: D27 recommends emphasizing oral discussion, assessing in-class/supervised work, and verifying that the original idea ("the spark") originates from human intelligence.
R03	Compliance Gap for High-Risk AI Systems (Legal/Governance): Absence of detailed internal procedures for the auditing, implementation, and management of High-Risk AI systems (as mandated by the EU AI Act/E5), particularly in administrative, HR, or student service areas.	High	Failure to comply with EU Regulation, regulatory sanctions from national AI Agency, institutional disruption if a system must be suspended or decommissioned.	D50/E5 (establishes the necessity), D32 (lack of specific protocol)	Strategic Alignment (Incomplete): D32 states a goal to align with national digital transformation plans, implying future compliance, but a concrete implementation protocol is currently missing.
R04	Algorithmic Bias and Discrimination (Ethical/Social): AI systems may generate results or decisions influenced by "prejudices related to the choice of training documents" (D26), potentially perpetuating systemic bias in research, administrative outputs, or educational content.	Medium	Unfair decisions, erosion of equity and inclusion goals, reputational damage.	D26	User Awareness and Verification: D26 advises users to be aware of this risk and to "check the created contents" and verify the results, acting as the final ethical gatekeeper.
R05	Failure to Close the Competence Gap (Strategic/Resource): The strategic commitment to digital transformation (D31) and the explicit goal to	Medium	Suboptimal execution of the Digital Transformation Plan (D32), decreased efficiency, and	D31, D32	Strategic Goal: D32 outlines the goal to "invest in management and IT communication skills" and "launch a





"launch a structured IT training program for all staff to bridge the competence gap" (D32) is a high-cost, long-term endeavor. The lack of an explicit, dedicated financial strategy creates a risk of underfunding and failure to execute this critical pillar.		personnel resistance to technological change.		structured IT training program," which addresses the need but not the financial certainty.
--	--	---	--	--

Section 6: Additional Checks – Policy Implementation and Adoption

Purpose: To trace how EU-level AI and digital education frameworks are implemented at the national and institutional levels.

Instructions: Provide short written answers (2–4 sentences per field) explaining how implementation occurs and to what extent.

Check Area	Guiding Question	Partner Assessment / Notes (brief)
Tracking Implementation (EU → National → Institutional)	How do EU-level policies (AI Act, GDPR, DEAP) translate into your national and institutional documents?	The translation from EU policy to institutional reality is robust in principle but fragile in practical implementation, following a pattern of "top-down strategic alignment" with a "bottom-up operational struggle." • Strength: The GDPR framework is fully matured and transposed, forming a strong baseline. The AI Act has been successfully anchored in the national strategy (D50) with a clear roadmap (new agency), and the DEAP is effectively localized through education-specific national (D49) and institutional (D27) guidelines. • Weakness: The main fragility lies at the institutional, operational level, particularly concerning new technologies like GenAI. The need to comply with GDPR (control) and the AI Act (risk-management) clashes with the default settings of popular, external GenAI tools (lack of control), forcing the institution to rely on prohibitions (R01) and non-technical mitigation measures (oral exams, self-declaration R02) rather than secure, compliant technical





		solutions. The framework is currently strategic and reactive (reacting to risks) but not yet fully proactive in implementing the deep structural changes (like high-risk AI protocols R03) required for full legal compliance.
Extent of Implementation	Was implementation partial or full? Provide brief reasoning and examples.	See Table 'Extent of Implementation'
Institutional Adoption of AI Regulations	How has your institution implemented or enforced AI-related guidelines (e.g., academic policies, staff guidance, committees)?	All of them

Table 'Extent of Implementation'

EU Policy	State of Implementation	Brief Reasoning and Example
GDPR (Data Protection)	Partial/Mature but Challenged	The foundational legal structure is fully implemented (D33, D30), but the influx of GenAI creates an operational conflict. The institution's response (D26) is a prohibition on entering sensitive data into external AI systems, which is a compliance measure but limits the intended full, modern use of the technology.
AI Act (E5) (AI Regulation)	Partial/In Progress (High Risk Gap)	National strategy (D50) is perfectly aligned, explicitly stating its role in implementing E5 and creating a new regulatory body to manage compliance. However, at the institutional level, a concrete protocol for managing High-Risk AI systems (R03) in non-academic functions (e.g., administration, HR, assessment tools) is missing .
DEAP (Digital Education)	Partial/High Strategic Alignment	The strategic pillars (D31, D32) and educational guidelines (D49, D27) directly address DEAP's call for digital skills and AI ethics in education. However, the plan's success is dependent on bridging a major Competence Gap (R05) and securing long-term funding, meaning the full realization of the educational objectives is still contingent on future resource allocation and execution.





Section 7: Partner Reflections

Purpose: To gather qualitative reflections and recommendations from each partner.

Instructions: In 1–2 short paragraphs, reflect on the overall strengths and weaknesses of your policy environment regarding AI in higher education and any recommendations for UM to include in the consolidated Policy Analysis Report.

The PoliTO policy environment regarding AI in higher education is commendable for its **rapidity and deliberate alignment** with new, stringent European regulations. The major strength lies in the swift and targeted **Guidelines for the Use of AI in Education (D27)** and the **Indications for AI Solutions (D26)**, which tackle the immediate, critical risks of Generative AI (GenAI) use, focusing on academic integrity, human accountability, and data privacy. This preemptive approach prevents policy drift and anchors AI use firmly in the existing ethical codes (D28) and legal compliance (D33). The alignment is also visible in the strategic documents (D31, D32) that frame digital transition and skill development as top-tier goals, consistent with the EU's Digital Education Action Plan.

However, the policy framework's primary weakness is its **reactive nature and fragmentation** when faced with the operational realities of GenAI. The internal policy is forced to rely on **prohibition** (banning sensitive data use in external AI tools - R01) because the institution has not yet developed or procured a secure, compliant **internal AI ecosystem**. Furthermore, the governance structure is strategically incomplete, as evidenced by the missing detailed protocols for **High-Risk AI compliance (R03)** required by the EU AI Act. This gap in proactive operational planning risks exposing the university to regulatory non-compliance and slowing the adoption of AI where it could provide the most benefit (e.g., in administration and research data management).

Recommendations for the Consolidated Policy Analysis Report:

1. **Prioritize Secure, Internal AI Infrastructure:** Recommend an immediate project mandate within the Digital Transformation Plan (D32) to acquire or develop a **GDPR-compliant, private cloud GenAI service** for staff and students. This would resolve the fundamental conflict between privacy policy (D33) and the use of modern AI tools (D26), enabling full implementation rather than partial prohibition.
2. **Formalize High-Risk AI Compliance Protocol:** Mandate the development of an internal "AI Act Compliance Protocol" to formalize the auditing, procurement, and risk-management procedures for all **High-Risk AI systems** used by the University (as required by E5), integrating this protocol directly into the responsibilities of the Responsible for Digital Transition (RTD) and the Data Protection Officer (DPO).
3. **Establish Dedicated AI Skills Budget:** Recommend assigning a **dedicated, protected budget line** for the "structured IT training program" (D32) to close the competence gap (R05). This is essential to ensure that the policy ambitions for digital transformation are backed by necessary resources to educate both staff (on compliance) and students (on responsible use).

