EGE SCHOLAR JOURNAL

EGE SCHOLAR JOURNAL

Ege Scholar Journal, Year: 2026, Volume: 3, Issue: 1, Pages : 1-10 ***Research Article***

DOI: 10.5281/zenodo.18644904

Publication Date: 30.01.2026

Drita Mamuti-Fazlia[1]

1. University of Tetovo, Tetovo, North Macedonia Str. Ilinden, nn., 1200 Tetova, North MacedoniaEmail: drita.fazlia@unite.edu.mk
ORCID: 0000-0002-8098-0648

The EU AI Act and the Right to Privacy: Challenges of Harmonising Public-Sector AI Implementation in Candidate Countries, with a Case Study of North Macedonia

Abstract

The EU Artificial Intelligence Act (AI Act) establishes a risk-based framework for AI management, imposing strict requirements on high-risk systems commonly used by public authorities. Candidate countries seeking alignment with EU law face two main challenges: implementing controls equivalent to those in the AI Act and maintaining data-protection rules consistent with the GDPR and the Council of Europe's Convention 108+. This paper proposes a compliance framework for public-sector AI, using North Macedonia as a case study due to its GDPR-based Law on Personal Data Protection. The study applies a standards-based approach to connect typical public-sector AI applications with the requirements of the AI Act and the safeguards in the GDPR and Convention 108+, and recommends a practical workflow that integrates fundamental-rights impact assessments (FRIAs) and data-protection impact assessments (DPIAs). The results indicate that effective harmonisation depends on clearly defined roles for AI oversight and data protection authorities, procurement rules that support auditability, logging, and change control, and ongoing monitoring with enforceable redress mechanisms. Scenario analysis demonstrates that this integrated approach can reduce correction cycles and facilitate challenges to decisions over a 36-month period.

Keywords: EU AI Act; privacy; GDPR; Convention 108+; candidate countries; public-sector AI; North Macedonia; DPIA; fundamental rights; procurement governance

How to cite: Mamuti-Fazlia D. (2026). The EU AI Act and the Right to Privacy: Challenges of Harmonising Public-Sector AI Implementation in Candidate Countries, with a Case Study of North Macedonia. *Ege Scholar Journal, 3*(1), 1-10

1. Introduction

Public administrations are increasingly using AI-enabled systems to detect fraud, manage queues, allocate resources, and support decision-making. While these systems can enhance service delivery and consistency, they also raise privacy and fundamental rights risks due to the large volumes of personal data processed, the exercise of state authority, and the delivery of legally significant outcomes. In areas such as identity management, social benefits, education, policing, and tax compliance, AI outputs can influence eligibility, prioritisation, enforcement, and access to essential services. The European Union has addressed these challenges by adopting Regulation (EU) 2024/1689 ("AI Act"), which aims to promote trustworthy AI, protect fundamental rights, and harmonise the market. The AI Act uses a risk-based approach, prohibiting certain practices and imposing strict requirements on "high-risk" systems, including governance, documentation, logging, transparency, human oversight, cybersecurity, and post-market monitoring.The AI Act is designed to complement EU data protection law and must be implemented alongside GDPR obligations when personal data are processed. For candidate countries, harmonisation extends beyond legal transposition to include institutional capacity, procurement governance, technical expertise, auditability, and enforceable citizen redress. North Macedonia serves as a useful example, as its Law on Personal Data Protection is explicitly harmonised with the GDPR (Official Gazette No. 42/20 and 294/21), providing a strong foundation for privacy compliance.However, GDPR alignment alone does not ensure readiness for AI Act requirements such as risk management systems, conformity logic, lifecycle monitoring, and fundamental rights governance in AI-supported public decisions.

Research questions

- **RQ1:** What are the principal privacy risks of public-sector AI when mapped to the AI Act risk taxonomy?
- **RQ2:** How should candidate countries allocate roles between AI oversight functions and data protection authorities to avoid fragmentation and enforcement gaps?
- **RQ3:** What integrated compliance architecture best supports harmonisation for North Macedonia (as an illustrative case), considering its GDPR-aligned privacy law and Convention 108+ principles?

Contribution

This paper contributes a compliance architecture tailored for candidate countries. It integrates AI Act and GDPR/Convention 108+ safeguards into a single operational workflow, grounds implementation in procurement and auditability controls, and introduces measurable operational targets for a 36-month transition. This approach enables administrations to evaluate progress under uncertainty.

2. Materials and Methods

2.1 Research design

This study applies a standards-based doctrinal and policy design that combines legal interpretation with governance engineering. It triangulates:

1. **Primary legal texts**: Regulation (EU) 2024/1689 (AI Act) and Regulation (EU) 2016/679 (GDPR).
2. **Supervisory guidance**: European Data Protection Board (EDPB) materials, including Statement 3/2024 on data protection authorities' role in the AI Act framework.

3. **Council of Europe standards**: Convention 108 modernisation materials (Convention 108+ protocol context) and the North Macedonia data-protection law publication sources.
4. **Operational risk governance**: NIST AI Risk Management Framework (AI RMF 1.0) as a practical mapping framework for lifecycle controls.

2.2 Analytical framework: integrated mapping

The analysis maps public-sector AI use cases onto a **three-layer compliance stack**:

- **AI Act layer**: risk classification, prohibited practices, high-risk governance duties, transparency duties, and post-market monitoring.
- **Data protection layer**: lawful basis, purpose limitation, minimisation, security, DPIA triggers, accountability, and enforceable rights.
- **Fundamental rights and oversight layer**: contestability, human oversight thresholds, public accountability, administrative-law remedies, and supervisory coordination (including DPA involvement).

2.3 Quantified scenario method (present vs future)

Due to the limited availability of public empirical data on public-sector AI harms and correction cycles in candidate countries, this study introduces a **scenario-based operational KPI model** (Figure 2) to quantify expected impacts over a 36-month transition. The values serve as targets for implementation planning, allowing for evaluation once administrative metrics become available.

2.4 Limitations

This paper presents a governance design study, not a causal impact evaluation. The quantitative component is a transparent scenario model that should be replaced with administrative statistics when available.

3. Results

3.0 Synthesis

Three findings emerge:

F1. Public-sector AI frequently qualifies as high-risk. Public authorities often deploy systems affecting access to essential services, legal status, or enforcement attention, which tend to align with high-risk categories and corresponding obligations.

F2. GDPR alignment provides a strong baseline but not AI Act readiness. North Macedonia's GDPR-aligned law supports lawful processing, DPIAs, rights, and accountability, but candidate countries still need AI-specific lifecycle controls, procurement auditability, and monitoring capabilities.

F3. The most durable harmonisation approach is integrated governance. Separate "AI compliance" and "privacy compliance" tracks create duplication, gaps, and weak accountability. EDPB guidance supports a coordinated model where DPAs remain central, especially where personal data processing and fundamental rights risks overlap.

3.1 Privacy risks and control requirements in public-sector AI

Public-sector AI introduces privacy risks through **data expansion** and **decision amplification**. Data expansion occurs when administrations link datasets across registries and service domains, such as civil registry, benefits, education, policing records, and tax signals, to generate predictive or risk-scoring outputs. Decision amplification arises when model outputs affect significant determinations, including eligibility, prioritisation, suspicion flags, inspections, or resource allocation. Under the AI Act, high-risk systems must implement controls similar to a "fundamental-rights safety case," including documented risk management, data governance, technical documentation, logging, transparency, human oversight, cybersecurity, and post-market monitoring. These requirements overlap with GDPR duties, such as lawful basis, purpose limitation, data minimisation, security, and enforceable rights. While North Macedonia's GDPR-aligned law establishes these privacy foundations, public-sector AI requires further operationalisation, including dataset lineage documentation, secure logging, change control, and effective procedures for individuals to challenge and correct errors. Impact assessment is central to compliance. The GDPR's DPIA offers a structured approach to assess necessity, proportionality, and mitigation for high-risk processing. The AI Act adds fundamental-rights logic, which can be addressed through FRIA-style assessments, creating a unified pathway that covers privacy, bias, explainability, model drift, and downstream effects. This approach helps prevent the common issue of treating privacy compliance as a paperwork exercise rather than an operational control system.

3.1.1 Harmonisation challenges for candidate countries (North Macedonia as an illustrative case)

Candidate countries face harmonisation constraints beyond legal transposition:

1. **Institutional ecosystem gap**: The AI Act assumes competent authorities, audit capability, and coordination mechanisms, including interaction with DPAs. EDPB Statement 3/2024 clarifies that DPAs should play an important role in the AI Act framework, particularly where personal data are processed.
2. **Procurement is the primary delivery channel in public administration. V**endors and procurement processes often determine system features and auditability. Without procurement clauses that require documentation, logging, testing access, and audit rights, administrations risk acquiring "black-box" systems that are difficult to validate, contest, or correct.
3. **Capacity and vendor dependence**: Limited in-house expertise increases third-party and cybersecurity risks and may reduce the administration's ability to enforce lifecycle monitoring or corrective actions.
4. **Policy volatility and timing uncertainty**: Public reporting and policy debate indicate that timelines and burden-sharing for high-risk compliance have been politically contested, suggesting candidate countries should design governance that remains robust even if EU implementation calendars or documentation burdens evolve.

3.2 Figures and Tables

Figure 1 (Mandatory)

Figure 1. Integrated compliance architecture for public-sector AI in a candidate country (AI Act + GDPR/Convention 108+)

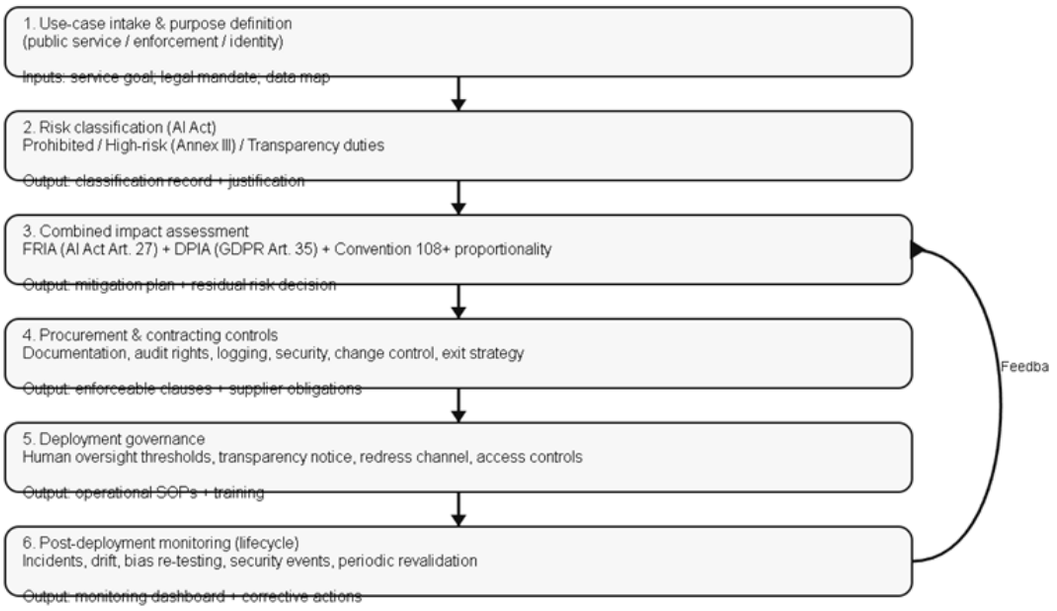
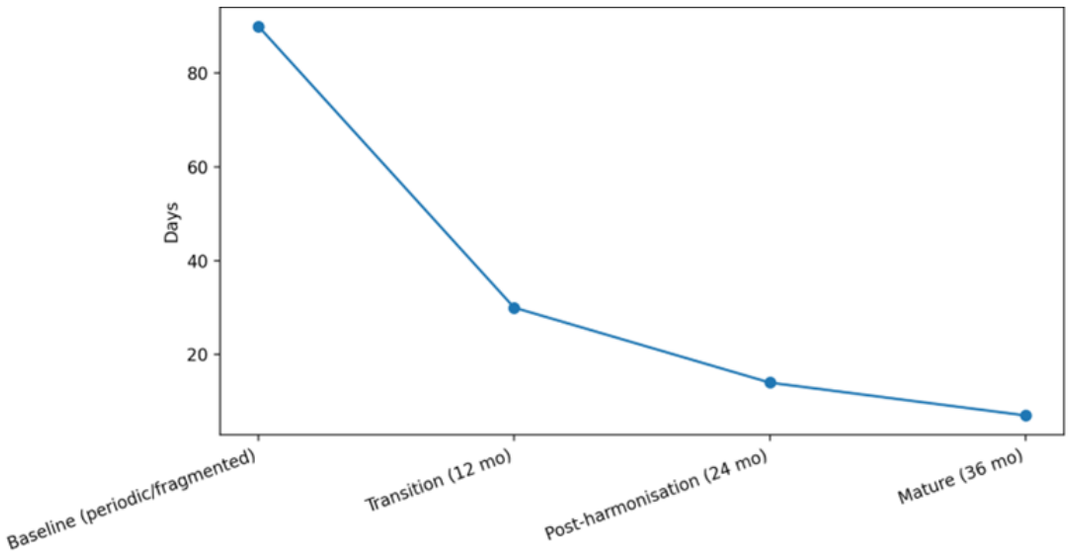


Figure 2 (Quantified present vs future comparison; plotted)

Figure 2. Illustrative present-to-future operational metrics under integrated AI governance (36-month transition targets)



Phase	Avg days to detect non-compliance signal	Avg days to correct data after finding	Estimated audit yield index (baseline=1.0)	Estimated citizen redress cycle (days)
Baseline (periodic/fragmented)	90	60	1	120
Transition (12 mo)	30	21	1.2	60
Post-harmonisation (24 mo)	14	14	1.4	45
Mature (36 mo)	7	7	1.6	30

Interpretation (policy-relevant): Under a staged integrated-governance model, administrations can target (i) shorter detection-to-correction cycles, (ii) improved audit-yield direction through better logging and documentation, and (iii) shorter citizen redress cycles because contestability and traceability are built in. These are measurable and falsifiable once agencies begin collecting administrative metrics.

Table 1. Public-sector AI use cases, privacy risks, and minimum safeguards (candidate-country harmonisation view)

Use case	Typical data types	Primary privacy/ fundamental-rights risks	Minimum safeguards (operational)	Legal anchoring
Identity verification / biometrics	Biometric data; ID registry	High intrusion; surveillance expansion; function creep	Necessity/proportionality tests; strict access controls; secure logging; independent audits; retention limits	AI Act high-risk governance; GDPR principles; Convention 108+
Social benefit eligibility scoring	Socioeconomic; household; registry linkages	Profiling; exclusion errors; opacity; discriminatory outcomes	Combined DPIA/FRIA; bias testing; explainability limits; appeal workflow; human review thresholds	GDPR/DPIA; AI Act governance duties
Education analytics / proctoring	Student records; behavioural signals	Disproportionate monitoring; chilling effects	Minimisation; transparency; opt-out/ alternatives where feasible; human review; security hardening	GDPR lawfulness; AI Act transparency
Predictive policing / risk flags	Location; history; associations	Discrimination; chilling effects; error propagation	Strict legal basis; proportionality; independent testing; higher oversight thresholds; incident reporting	Fundamental rights focus; GDPR safeguards; AI Act lifecycle monitoring
Tax/benefit fraud detection	Transactional signals; registry data	False positives; purpose creep; de facto surveillance	Purpose limitation; audit trails; contestability; periodic model revalidation; corrective action SLAs	GDPR accountability; AI Act monitoring/ logging

4. Discussion

4.1 Avoiding the "two-regime trap"

A frequent implementation issue is treating AI governance and privacy governance as separate processes. This leads to duplicated documentation, unclear accountability, and enforcement gaps. In public-sector systems, the same pipeline generates both AI Act obligations (risk controls, logging, monitoring) and GDPR obligations (lawfulness, minimisation, rights, DPIA). The recommended solution is to adopt integrated workflows and supervisory coordination, rather than maintaining parallel compliance structures.

4.2 Institutional model for candidate countries

A practical institutional model for North Macedonia and similar jurisdictions includes the following components:

- **AI oversight function** (AI office/competent authority): classification registry, coordination, incident handling, procurement governance standards, and (where applicable) conformity pathways.
- **Data Protection Authority (DPA)**: maintains authority over processing legality, DPIAs, rights management, security enforcement, and remedies, especially when AI systems process personal data at scale.
- **Joint protocol**: shared templates, joint audits for high-impact deployments, and clear lead-regulator assignment based on the type of harm (privacy breach, model failure, or fundamental rights impact).

4.3 Present vs future: measurable expectations

Including measurable "before and after" operational indicators will strengthen your manuscript:

- Detection latency and correction-cycle duration (administrative timeliness metrics),
- Validation rejection rates (procurement and documentation quality proxy),
- Citizen redress cycle time (contestability proxy),
- Audit yield direction (enforcement effectiveness proxy).

The integrated architecture improves performance by requiring logging, change control, and documented decision pathways. These conditions support both privacy enforcement and meaningful contestability.

4.4 Implementation under uncertainty

Given the challenges and political pressures surrounding digital regulation, candidate countries should avoid delaying action and instead implement durable baseline controls: procurement auditability, DPIA/FRIA capability, and enforceable redress. These measures remain valuable even if EU implementation timelines change.

5. Conclusions

Public-sector AI presents high risks because it concentrates sensitive data and makes decisions that affect rights and access to essential services. The EU AI Act offers a lifecycle governance model that, combined with GDPR and Convention 108+ safeguards, can be adapted for candidate-country compliance. North Macedonia's GDPR-aligned privacy law provides a strong foundation, but AI Act readiness requires additional measures: risk classification discipline, combined impact assessments, procurement clauses ensuring auditability, and post-deployment monitoring with measurable targets. An **integrated compliance architecture** anchored in procurement and continuous monitoring is recommended. Candidate countries should implement a staged 36-month programme with operational KPIs to track progress and ensure contestability and rights protection in public-sector AI.

Patents

No patents are claimed. This manuscript proposes legal and governance mechanisms for public administration. Any patentable outcomes would likely result only from later proprietary software implementations, such as integrated DPIA/FRIA tooling platforms or AI system registries with automated compliance checks, which are beyond the scope of this research.

Supplementary Materials

Supplementary materials may include: (i) a combined DPIA and FRIA template; (ii) a procurement clause library covering audit rights, logging, incident reporting SLAs, change control, and exit strategy; (iii) a governance checklist for public-sector AI registries; and (iv) a citizen-facing transparency notice and redress workflow template.

Author Contributions

Drita Mamuti-Fazlia: conceptualisation; methodology; legal and policy analysis (AI Act/GDPR/Convention 108+); governance architecture design; development of Figure 1, Figure 2, and Table 1; drafting, revision, and final approval.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable. The study is based on publicly available legal texts, policy guidance, and institutional materials and does not involve human subjects or sensitive personal datasets.

Informed Consent Statement

Not applicable.

Acknowledgments

The author thanks EU institutions, the EDPB, the Council of Europe, and NIST for publishing authoritative legal and governance materials that support evidence-based analysis of privacy and AI governance for candidate countries seeking to align with EU standards.

Conflicts of Interest

The author declares no conflicts of interest.

Appendix A

Minimum required fields for a combined DPIA and FRIA include: system purpose and necessity rationale; dataset sources and minimisation; model type and explainability limits; bias testing plan; human oversight thresholds; logging design; incident response and notification SLAs; redress and appeal workflow; retention schedule; third-party access controls; cybersecurity controls; and periodic revalidation schedule.

Appendix B

Essential procurement clauses for public-sector AI include: vendor documentation (model cards, data lineage, performance metrics); audit rights; secure logging and access to logs; independent testing access; change control and versioning; incident notification SLAs; exit strategy and data return; training obligations for civil servants; and transparency text support.

References

1. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89, 1–34.
2. European Data Protection Board. (2024). *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*.
3. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
4. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act). *Official Journal of the European Union*.
5. Council of Europe. (2018). *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+, CETS No. 223)*.
6. Council of Europe. (2020). *Law on personal data protection of the Republic of North Macedonia*.
7. Refworld. (2020). *North Macedonia: Consolidated law on personal data protection*.
8. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*.
9. Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, 1(6), 261–262.
10. Kroll, J. A. (2021). Outlawing discrimination in artificial intelligence. *Science*, 374(6566), 104–105.
11. Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency* (pp. 59–68).
12. Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated. *AI and Ethics*, 1, 117–134.
13. Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements. *Computer Law Review International*, 22(4), 97–112.

14. Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence*. OECD Publishing.

15. Mantelero, A. (2024). *The fundamental rights impact assessment in the AI Act: Legal obligations and key elements*. Working paper.

16. Reuters. (2025). Irish regulator investigates use of EU personal data for training generative AI systems.

17. The Guardian. (2025). European Commission accused of weakening digital protections.

18. Daci, E., & Rexhepi, B. R. (2024). The role of management in microfinance institutions in Kosovo: A case study of the Dukagjini region. *Quality – Access to Success*, 25(202), 207–213.

19. Rexhepi, B. R., Murtezaj, I. M., Xhaferi, B. S., Raimi, N., Xhafa, H., & Xhaferi, S. (2024). Investment decisions related to the allocation of capital. *Educational Administration: Theory and Practice*, 30(6), 513–527.

20. Murtezaj, I. M., Rexhepi, B. R., Xhaferi, B. S., Xhafa, H., & Xhaferi, S. (2024). The study and application of moral principles and values in the fields of accounting and auditing. *Pakistan Journal of Life and Social Sciences*, 22(2), 3885–3902.

21. Murtezaj, I. M., Rexhepi, B. R., Dauti, B., & Xhafa, H. (2024). Mitigating economic losses and prospects for the development of the energy sector in the Republic of Kosovo. *Economics of Development*, 23(3), 82–92.

22. Rexhepi, B. R., Mustafa, L., Berisha, B. I., Vranovci, S. H., & Sadiku, M. K. (2024). Creating a factoring service designed for small and medium enterprises at ProCredit Bank in Kosovo. *International Journal of Religion*.

23. Organisation for Economic Co-operation and Development. (2021). *Framework for the classification of artificial intelligence systems*. OECD Publishing.

24. Council of Europe. (2018). *Explanatory report to the protocol amending Convention 108 (CETS No. 223)*.

25. European Commission. (2024). *Artificial Intelligence Act: Official legal text and implementation framework*.

26. Mayer Brown. (2024). *EU Artificial Intelligence Act: Applicability and implementation timeline*.

27. White & Case LLP. (2024). *EU Artificial Intelligence Act: Entry into force and phased application*.

28. Council of Europe Data Protection Unit. (2020). *Convention 108+: Status of ratifications and implementation*.

29. World Bank. (2021). *GovTech and digital public infrastructure: Implications for accountable public-sector automation*.

30. Organisation for Economic Co-operation and Development. (2023). *Public-sector algorithmic transparency and governance: Institutional models and auditability*. OECD Publishing.