

Mihaela Miruna Tudorascu

University "1 Decembrie 1918" of Alba Iulia, Romania

ORCID: 0000-0003-4641-4578

miruna.tudorascu@uab.ro

Raluca Oana Ivan

University "1 Decembrie 1918" of Alba Iulia, Romania

ORCID: 0000-0002-8019-3601

raluca.ivan@uab.ro

Personal Data Protection in Digitalized Public Administration: Challenges and Solutions in the Context of AI

Keywords: personal data protection, artificial intelligence, public administration, GDPR, EU AI Act

Summary. The rapid digitalization of public administration, accelerated by artificial intelligence (AI) technologies, promises enhanced efficiency and improved citizen services but simultaneously introduces profound risks to personal data protection. This paper examines these challenges within the context of Romania's ongoing governance reforms, proposing actionable solutions aligned with the General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act. Through a qualitative research methodology combining EU-wide regulatory analysis with Romania-focused case studies, this study addresses key tensions between AI-driven automation, such as predictive analytics, automated decision-making systems, and biometric identification, and fundamental privacy rights. With Romania advancing its Digital Governance Framework amid EU mandates, unresolved issues including algorithmic bias, surveillance concerns, and enforcement gaps threaten both public trust and regulatory compliance. This analysis offers policymakers and practitioners practical pathways to balance technological innovation with robust data protection through Privacy by Design principles, enhanced oversight mechanisms, and transparent algorithmic governance.

Ochrona danych osobowych w cyfryzowanej administracji publicznej: wyzwania i rozwiązania w kontekście AI

Słowa kluczowe: ochrona danych osobowych, sztuczna inteligencja, administracja publiczna, RODO/GDPR, unijny akt w sprawie sztucznej inteligencji

Streszczenie. Szybka cyfryzacja administracji publicznej, przyspieszona przez technologie sztucznej inteligencji (AI), obiecuje zwiększenie efektywności oraz poprawę jakości usług świadczonych obywatelom, lecz jednocześnie rodzi poważne ryzyka dla ochrony danych osobowych. Artykuł analizuje te wyzwania w kontekście trwających reform zarządzania publicznego w Rumunii, proponując praktyczne rozwiązania zgodne z ogólnym rozporządzeniem o ochronie danych osobowych (RODO/GDPR) oraz unijnym aktem w sprawie sztucznej inteligencji.

W oparciu o jakościową metodologię badawczą, łączącą analizę regulacji obowiązujących w Unii Europejskiej ze studiami przypadków dotyczącymi Rumunii, opracowanie podejmuje kluczowe napięcia między automatyzacją opartą na AI – taką jak analityka predykcyjna, zautomatyzowane systemy decyzyjne oraz identyfikacja biometryczna – a podstawowymi prawami do prywatności. W sytuacji, gdy Rumunia rozwija swoje ramy cyfrowego zarządzania zgodnie z wymogami UE, nierozwiązane problemy, w tym stronniczość algorytmiczna, obawy dotyczące nadzoru oraz luki w egzekwowaniu przepisów, zagrażają zarówno zaufaniu publicznemu, jak i zgodności regulacyjnej.

Analiza wskazuje decydentom politycznym i praktykom możliwe kierunki działania pozwalające pogodzić innowacje technologiczne z solidną ochroną danych osobowych poprzez stosowanie zasad privacy by design, wzmocnienie mechanizmów nadzoru oraz przejrzyste zarządzanie algorytmiczne.

Introduction

The rapid digitalization of public administration, accelerated by AI technologies, promises enhanced efficiency and citizen services but introduces profound risks to personal data protection. This paper examines these challenges in the context of Romania's ongoing governance reforms, proposing actionable solutions aligned with GDPR and the EU AI Act. It addresses key tensions between AI-driven automation, such as predictive analytics and biometric systems, and fundamental privacy rights, focusing on Romania's public sector where digital initiatives like ROeID¹ and government cloud platforms process vast citizen data. While literature examines GDPR implementation in Western European contexts, there is limited empirical research on how Central and Eastern European countries with less developed digital infrastructure and institutional capacity address the combined challenges of GDPR and AI Act implementation. Notably, systematic analysis is lacking on the interaction between legacy IT systems and emerging AI governance requirements, as well as on the strategies used by resource-constrained data protection authorities to enforce regulations in rapidly digitalizing environments. This study considers the gap by examining Romania's unique position as a nation pursuing ambitious digitalization amid notable capacity constraints.

With Romania advancing its Digital Governance Framework amid EU mandates, unresolved issues like algorithmic bias and enforcement gaps threaten trust and compliance, this analysis fills that void through targeted research questions and a case study. It offers policymakers practical pathways to balance innovation with protection².

The research questions of our research are:

¹ Romania's national Single Sign-On (SSO) platform for digital identity, enabling citizens to access e-government services with one set of secure credentials. Launched by the Authority for Digitalization of Romania, it supports online authentication for platforms like ghișeul.ro and is designed for EU-wide interoperability under eIDAS regulations [accessed on: 26.01.2026].

² Romania and the EU AI Act: Ready or Just Warming Up? <https://eurocloud.org/news/article/romania-and-the-eu-ai-act-ready-or-just-warming-up/> [accessed on: 26.01.2026].

RQ1: What are the primary challenges to personal data protection in AI-driven digitalized public administration, such as bias, surveillance, and unauthorized processing?

RQ2: How does Romania's implementation of GDPR and the EU AI Act address these challenges in its public sector digitalization efforts?

AI in public administration amplifies risks like massive personal data processing without adequate safeguards, algorithmic bias affecting decisions, and surveillance via tools like facial recognition. In digitalized systems, challenges include data breaches from interconnected platforms and lack of transparency in automated decisions. Globally, regulations like GDPR and EU AI Act (effective 2024) impose strict requirements, but enforcement gaps persist³.

Our research will follow a qualitative approach, combining EU-wide insights on AI privacy risks (*e.g.*, data breaches, bias) and Romania-focused analysis via legal documents, reports, and case studies. We realize a literature review on global/EU challenges, Romania case study, and synthesis of solutions with recommendations.

General Aspects

The analysis of personal data protection in AI-driven public administration requires a multi-layered theoretical framework that integrates legal, technological, and governance perspectives. This section establishes the conceptual foundation for our analysis by examining the intersection of data protection law, AI ethics, and public administration theory⁴.

The Legal Framework: GDPR and the EU AI Act. The General Data Protection Regulation (GDPR), effective since May 2018, establishes the foundational legal framework for personal data protection within the European Union. Its core principles, lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality, provide a comprehensive regime for protecting individual privacy rights. Particularly relevant to AI deployment are Articles 22 (automated decision-making), 25 (data protection by design and by default), and 35 (data protection impact assessments)⁵.

³ Hisham Hamed Al-Kasasbeh, Nasir Albalawee, Haneen A. Al-Khawaja, Ali Khaled Qtaishat, *Legal Challenges of Using AI and Big Data in Public Administration: Administrative Liability, Data Protection, and Public Services Efficiency* in International Journal of Sustainable Development and Planning, vol. 20, no. 6, June, 2025, pp. 2639-2650.

⁴ R.M. Gellert (2015), Understanding data protection as risk regulation. *Journal of Internet Law*, 18(11), pp. 3-15.

⁵ European Data Protection Board, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 2018.

The EU Artificial Intelligence Act, provisionally agreed in December 2023 and entering into force in stages from 2024–2027, complements GDPR by establishing a risk-based regulatory framework specifically for AI systems. The Act categorizes AI applications according to risk levels (unacceptable, high, limited, minimal) and imposes corresponding obligations on developers and deployers. For public administration, many AI systems fall into the high-risk category, triggering requirements for conformity assessments, risk management systems⁶, data governance, transparency, human oversight, and robustness measures.

Privacy by Design and Default. Privacy by Design (PbD), conceptualized by Ann Cavoukian⁷ and codified in GDPR Article 25, represents a proactive approach to privacy protection requiring that data protection measures be embedded into technology systems from their inception rather than added as afterthoughts. The seven foundational principles of PbD, proactive not reactive, privacy as default, privacy embedded into design, full functionality, end-to-end security, visibility and transparency, and respect for user privacy, provide a comprehensive framework for developing privacy-preserving AI systems in public administration.

This study employs a qualitative research methodology combining doctrinal legal analysis with empirical case study investigation. The methodological approach is designed to provide both theoretical depth and practical insights into the implementation challenges of data protection in AI-driven public administration. First, a comprehensive literature review examines academic publications, policy documents, and regulatory guidelines addressing AI deployment in public administration and personal data protection within the European Union. This review encompasses scholarly articles from legal, computer science, and public administration journals; EU legislative texts and preparatory materials; guidance documents from the European Data Protection Board (EDPB); reports from civil society organizations; and technical standards for AI governance.

Second, the study conducts doctrinal analysis of relevant legal instruments, including GDPR provisions, the EU AI Act, Romanian implementation legislation (Law 190/2018 on data protection measures), and decisions of the Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP). This analysis identifies gaps, ambiguities, and potential conflicts in the regulatory framework.

Third, case study methodology examines specific AI implementations in Romanian public administration, including the ROeID digital identity system, au-

⁶ European Commission, The Artificial Intelligence Act. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

⁷ Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, Canada, 2011.

tomated tax assessment systems, AI-powered social benefit allocation platforms, and biometric border control systems. Data sources include official government documentation, ANSPDCP investigation reports, media coverage, and publicly available technical specifications.

This research acknowledges several limitations. Access to detailed technical specifications of AI systems deployed in Romanian public administration is restricted due to security and commercial confidentiality concerns. The rapidly evolving nature of both AI technology and regulatory frameworks means that findings represent a snapshot of current conditions. Additionally, the study focuses primarily on legal and institutional dimensions, with limited examination of citizen perspectives and experiences.

Challenges to Personal Data Protection in AI Driven Public Administration

The deployment of AI systems in public administration creates multiple challenges to personal data protection, ranging from technical vulnerabilities to governance deficits. This section analyzes the primary challenges identified through our research.

Massive Personal Data Processing Without Adequate Safeguards. AI systems in public administration require vast quantities of personal data for training, validation, and operational deployment⁸. Unlike traditional administrative systems that process data for specific, clearly defined purposes, AI systems often aggregate data from multiple sources, creating comprehensive citizen profiles that extend far beyond the original collection purpose. In Romania, the integration of various governmental databases, like tax records, health information, social benefits data, educational records, into centralized platforms creates unprecedented concentrations of personal information.

The principle of data minimization, fundamental to GDPR, becomes particularly challenging in AI contexts. Machine learning algorithms typically perform better with larger datasets, creating institutional pressures to collect and retain maximum amounts of data rather than minimum necessary amounts. Furthermore, the lack of clear purpose limitation, AI systems may be repurposed for uses not anticipated at the time of data collection, undermines citizen control over their personal information.

⁸ Tal Zarsky, The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making, *Science, Technology, & Human Values*, vol. 41, no. 1, 2016, pp. 118-132.

Algorithmic Bias and Discriminatory Decision-Making. Algorithmic bias represents one of the most pernicious threats to fundamental rights in AI-driven administration. Bias can enter AI systems through multiple pathways⁹, like in historical data reflecting past discrimination, proxy variables that correlate with protected characteristics, skewed training datasets, or flawed model assumptions. In public administration contexts, where AI systems may determine access to benefits, assess tax liabilities, or make law enforcement decisions, algorithmic bias can perpetuate and amplify existing social inequalities.

Surveillance Capabilities and Biometric Systems. The deployment of AI-powered surveillance technologies, particularly facial recognition¹⁰ and other biometric systems, raises profound privacy concerns. While the EU AI Act prohibits certain uses of real-time remote biometric identification in public spaces, exceptions exist for law enforcement purposes, and post-deployment (retrospective) facial recognition faces fewer restrictions. In Romania, biometric systems have been deployed for border control, national ID cards, and increasingly for access to government buildings and services.

Lack of Transparency and Explainability. Many AI systems, particularly those based on deep learning neural networks, function as ‘black boxes’¹¹ where the reasoning process behind specific decisions remains opaque even to system developers. This opacity conflicts with GDPR’s transparency requirements and citizens’ rights to understand decisions affecting them. In administrative contexts, where decisions may have significant consequences, as denial of benefits, tax assessments, eligibility determinations, the inability to explain algorithmic reasoning undermines both accountability and the right to effective remedy. Romania’s public administration faces particular challenges in achieving algorithmic transparency. Many AI systems are procured from private vendors under contracts that protect proprietary algorithms as trade secrets. Public officials often lack the technical expertise to evaluate or explain AI system operations. Citizens have limited means to challenge automated decisions, and judicial review mechanisms have not yet adapted to address algorithmic decision-making.

Data Breaches and Cybersecurity Vulnerabilities. The interconnected nature of digital government platforms creates significant cybersecurity risks. Centralized

⁹ Andrew D. Selbst et al., Fairness and abstraction in sociotechnical systems, in *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 2019, pp. 59–68.

¹⁰ Karen Yeung, Algorithmic Regulation: A Critical Interrogation (May 23, 2017). TLI Think! Paper 62/2017, Regulation & Governance, Forthcoming, King’s College London Law School Research Paper no. 2017-27, Available at SSRN: <https://ssrn.com/abstract=2972505>.

¹¹ Sandra Wachter, Brent Mittelstadt, Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, *International Data Privacy Law*, vol. 7, no. 2, 2017, pp. 76–99.

databases containing comprehensive citizen information present attractive targets for cyberattacks. Romania¹² has experienced multiple data breaches affecting government systems, exposing personal information of millions of citizens. AI systems introduce additional vulnerabilities through their complexity, dependence on cloud infrastructure, and potential for adversarial attacks that manipulate model behavior. The concentration of personal data in AI training datasets means that a single breach can expose vast quantities of sensitive information.

Romania's Implementation of GDPR and the EU AI Act in Public Sector Digitalization

Romania has invested heavily in digitalizing public services¹³ (health, education, administration) under its National Recovery and Resilience Plan (PNRR)¹⁴.

As an EU member it fully applies the GDPR (Regulation (EU) 2016/679), implemented by national Law 190/2018 and is beginning to implement the EU AI Act. This report examines how GDPR compliance is carried out in Romanian healthcare, education, and public administration, outlines national measures (existing or proposed) for the EU AI Act, surveys examples of AI/digital tools in public services and their legal treatment and discusses challenges and impacts on citizens' privacy, trust, and administrative efficiency.

GDPR Compliance in Public Administration. Romanian public bodies, from central ministries to city halls, are explicitly designated in national law as "public authorities" subject to GDPR (Law 190/2018 defines processing for public-interest tasks)¹⁵. In practice, all government agencies must have DPOs, register data flows, and follow ANSPDCP directions. For example, public-sector GDPR compliance often involves frequent audits by ANSPDCP, if violations are found, public entities receive remediation plans with strict timelines (*e.g.*, 90 days to remedy)¹⁶. Breaches in the public sector (*e.g.*, leaked employment or tax records) must be reported to ANSPDCP within 72 hours, and indeed the Authority regularly publishes sanctions against state bodies that neglect privacy.

¹² National Supervisory Authority for Personal Data Processing, Annual Activity Report 2022, Bucharest, 2023.

¹³ Maria Albu, Local Administration in The Era of Digitalization: From E-Government to Smart Governance. Case Study: Alba Iulia Smart City, in *Annales Universitatis Apulensis – Series Jurisprudentia*, nr.28/2025, pp. 9-19.

¹⁴ Romania Country Commercial Guide at <https://www.trade.gov/country-commercial-guides/romania-digital-economy> [accessed on: 05.02.2026].

¹⁵ ROMANIA Data Protection Laws of the World <https://www.dlapiperdataprotection.com/index.html?t=law&c=RO> [accessed on: 05.02.2026].

¹⁶ *Ibidem*.

Compliance in government IT projects is also emphasized. Large digitalization projects (like new e-Government portals and the national government cloud) include GDPR assessments. A U.S. trade report notes that as an EU member, “Romania adheres to GDPR, which imposes strict data privacy and protection requirements” and that aligning systems with these rules often requires significant investment in security and legal expertise. In recent years, key initiatives, such as a secure government private cloud (launched 2025), explicitly build in privacy and security audits¹⁷. Nonetheless, legacy issues (fragmented databases, varying technical capacity across ministries) mean ANSPDCP still finds gaps. As one summary notes, Romania’s regulators maintain “high standards” and require extensive privacy measures for public institutions¹⁸ (including employee monitoring and CCTV rules).

EU AI Act: National Strategy and Legislative Measures. With the EU AI Act now in force, Romania is drafting national measures to implement it. In July 2024, the government approved a National AI Strategy 2024–2027, which serves as a roadmap for AI adoption and governance. The Strategy proposes creating a dedicated authority under the Digitalization Agency (ADR) to oversee AI implementation, and calls for national guidelines on safe AI use¹⁹. Separately, Parliament is considering draft laws on AI. One proposal (PL-x 184/2025) would establish substantive rules for “responsible AI” in both private and public spheres. Key provisions under discussion include in public administration, any AI system used in decision-making must be transparent and subject to regular independent audits, fully automated decisions (without human oversight) would be prohibited, in judiciary and law enforcement, AI could not be the sole basis for judicial rulings or enforcement decisions, in healthcare, AI tools for diagnostics/treatment would need scientific validation and official approval *etc.* As sanctions we found abusive or illegal AI use (*e.g.*, violating these rules) would carry heavy penalties, proposed fines range up to €20 million and even criminal sanctions²⁰.

These proposals mirror EU AI Act obligations but go further in places (*e.g.*, criminal penalties). They have raised legal debates, as experts note some draft provisions may overlap or conflict with the EU Act’s regime. Officially, Romania

¹⁷ Romania Digital Transformation: Launch of Major Procurement for Government Private Cloud Migration <https://www.trade.gov/market-intelligence/romania-digital-transformation-launch-major-procurement-government-private> [accessed on: 05.02.2026].

¹⁸ Data Privacy Management in Romania - Compliance & Law, <https://responsum.eu/privacy-management-in-romania/> [accessed on: 05.02.2026].

¹⁹ Romania and the EU AI Act: Ready or Just Warming Up? | International Network of Privacy Law Professionals <https://inplp.com/latest-news/article/romania-and-the-eu-ai-act-ready-or-just-warming-up/> [accessed on: 05.02.2026].

²⁰ *Ibidem.*

has not yet designated its national authorities under the AI Act as required. To comply, Member States must name a “market surveillance” body, a “notification” authority, and a fundamental rights authority. Romania has notified the EU that agencies like the Ombudsman and Data Protection Authority will monitor high-risk AI systems²¹, but as of late 2025, no single national AI supervisory body has been formally established, despite an EU deadline of Aug 2025. In short, Romania’s approach is evolving, the government has set strategy and is working on laws, but institutional and regulatory steps remain to be finalized.

As a study case, several high-profile digital services illustrate AI and data use in government. In 2024-2025, Romania launched its Government Private Cloud project, migrating dozens of state IT systems into a secure centralized cloud²². This aims to improve efficiency, resilience and security of citizen services (tax filing, business registrations, *etc.*) while ensuring personal data are better protected. Another example is the ongoing rollout of a digital ID (eID) for citizens, which will replace paper documents with secure electronic identification. By law this system is built with GDPR safeguards (data encryption, user consent). On the AI front, McKinsey reports that over half of Romanian civil servants have already begun using AI tools (*e.g.*, automated text summarizers, translation, chatbot assistants) in their daily work²³. Some municipalities and agencies are piloting chatbots for citizen inquiries, always with disclaimers that personal requests still go to human agents. In administrative law enforcement and benefits, no fully automated AI decisions exist, cases must be reviewed by officials. These steps reflect how GDPR and draft AI laws influence practice like any use of AI by a public agency is planned with a DPIA and human supervision, and citizens are informed when an AI tool (like a virtual assistant) is involved.

Key Challenges in Integrating Regulations. Romania’s digital transformation faces several hurdles in applying GDPR and AI rules, like Technical and Infrastructure Gaps. Romania ranks low on the EU Digital Economy and Society Index, indicating shortfalls in broadband coverage and IT infrastructure²⁴. Government reports and OECD reviews note that limited internet in rural areas and outdated legacy

²¹ *Ibidem.*

²² Romania Digital Transformation: Launch of Major Procurement for Government Private Cloud Migration <https://www.trade.gov/market-intelligence/romania-digital-transformation-launch-major-procurement-government-private> [accessed on: 05.02.2026]

²³ Martin H. Thelle et al., The opportunity of AI in public administration in Romania, Capturing the benefits of AI in public administration, *An implement Consulting Group by Google*, October 2024.

²⁴ Cristian Constantin FRANCU, Ștefan SAVA, Global Perspectives on Digital and AI Legislation: A Comparative Study of Data Protection, AI Governance, and Healthcare Innovations with a Focus on Romania, DOI: 10.2478/picbe-2025-0191, *Proceedings of the 19th International Conference on Business Excellence 2025*, Sciendo, pp. 2469-2481.

systems hinder seamless data sharing and secure cloud adoption²⁵. Public sector IT projects often suffer delays, as slower connectivity and old hardware complicate GDPR compliance (*e.g.*, harder to encrypt or update aging servers).

Widespread lack of digital literacy impedes regulation. For example, fewer than 25% of Romanians use any e-government service (EU average is 75%)²⁶. In schools and local offices, many staff members still have only basic IT skills, so GDPR concepts (data subject rights, DPIAs) are not fully understood. Studies report that even after GDPR became law, many institutions did not implement all requirements²⁷. Similarly, public servants may lack training on AI/ML risks. The OECD and EU note persistent deficits in Romania's "digital skills" and the need for user-centered design²⁸.

Fragmentation of rules creates uncertainty. Romania's own AI draft law and the EU AI Act cover similar ground, experts warn some national provisions (like criminal sanctions) may conflict with EU rules. At present, Romania's AI Act implementation relies on existing authorities (*e.g.*, ANSPDCP for data rights, Ombudsman for discrimination), but the formal designation of AI supervisory bodies was delayed²⁹. This transitional gap makes compliance responsibilities unclear for AI developers and public agencies. Likewise, new local laws on topics like telework or e-commerce must be carefully aligned with GDPR, requiring constant legal review.

Public trust is a challenge. Surveys show Romanian citizens are very cautious about data-driven tools. About 70% are "very" or "moderately" concerned about how AI accesses their data³⁰. Most insist on human oversight (*e.g.*, over 60% prefer to interact with a real person rather than a chatbot for government services). These attitudes pressure officials to proceed carefully. Mistrust also applies to public-sector

²⁵ AI in Romania: The potential for the public sector | McKinsey, <https://www.mckinsey.com/industries/public-sector/our-insights/the-transformative-potential-of-ai-in-romania-public-sector> [accessed on: 05.02.2026].

²⁶ *Ibidem* [accessed on: 08.02.2026].

²⁷ Anisoara Belbe, Implementation and Application of GDPR In Romanian Educational Institutions, in *The Annals of the University of Oradea. Economic Sciences* TOM XXXI, 1st Issue, July 2022, pp. 160-171.

²⁸ AI in Romania: The potential for the public sector | McKinsey, <https://www.mckinsey.com/industries/public-sector/our-insights/the-transformative-potential-of-ai-in-romania-public-sector> [accessed on: 08.02.2026].

²⁹ Romania and the EU AI Act: Ready or Just Warming Up? | International Network of Privacy Law Professionals <https://inplp.com/latest-news/article/romania-and-the-eu-ai-act-ready-or-just-warming-up/> [accessed on: 08.02.2026].

³⁰ Study: Romanians do not trust AI without human intervention, <https://www.romaniajournal.ro/business/study-romanians-do-not-trust-ai-without-human-intervention-seven-out-of-ten-prioritise-data-protection/> [accessed on: 08.02.2026].

data use: any news of a data leak (like a hospital breach) erodes confidence that GDPR is enforced.

Ensuring compliance can be costly. Businesses and agencies must invest in new systems, security audits, and legal staff. A U.S. report notes GDPR compliance “requires significant investment” in data systems and monitoring³¹. Romania’s public budgets are constrained, so modernization projects (cloud migration, smart classrooms) sometimes run behind schedule. Limited funding can leave smaller agencies struggling to install recommended encryption or hire qualified DPOs.

In summary, Romania must continue bridging gaps in technology, skills, and legal alignment to fully integrate GDPR and the AI Act into its digital agenda.

Impacts on Citizens: Privacy, Trust, and Efficiency. The interplay of GDPR and AI rules shapes Romanian citizens’ experiences in three key ways, like Data Privacy and Rights, citizens benefit from strong legal guarantees. Under GDPR, individuals can access and delete their data held by any public agency, and special rules protect sensitive health or student records. For instance, when using telemedicine or school portals, citizens must give explicit consent for data processing, and agencies publish transparency notices online. Trust in AI and Services, Romanian citizens are wary but pragmatic. Recent surveys³² indicate a strong demand that any AI in healthcare, education, or administration be “strictly governed by law” with human oversight. Citizens recognize the benefits of digitalization on the other hand, they appreciate that online tax filing or e-health portals can save time. Importantly, trust hinges on transparency, officials communicate how personal data are used and allow complaint channels. Effective oversight (e.g., ANSPDCP’s high-profile actions) helps build confidence that violations have consequences. Administrative efficiency, digital tools promise and deliver faster services. Under GDPR and AI rules, projects must meet privacy standards, but when designed properly they greatly improve efficiency. In practice, citizens experience this as shorter wait times and one-stop services. For instance, the rollout of digital ID and e-signatures has enabled fully online applications for permits and benefits. Over time, harmonizing GDPR and AI Act compliance is expected to enhance service quality by ensuring systems are robust: a well-regulated, secure digital infrastructure both protects citizens and makes agencies more responsive.

In conclusion, Romania’s public sector is rapidly evolving its digital landscape under the twin imperatives of privacy and innovation. GDPR has been embedded

³¹ Romania – Digital Economy, <https://www.trade.gov/country-commercial-guides/romania-digital-economy> [accessed on: 08.02.2026].

³² Study: Romanians do not trust AI without human intervention, <https://www.romaniajournal.ro/business/study-romanians-do-not-trust-ai-without-human-intervention-seven-out-of-ten-prioritise-data-protection/> [accessed on: 08.02.2026].

via national laws, DPOs, and sector-specific rules in healthcare, education, and administration. The AI Act's requirements are being addressed through a national AI strategy, draft legislation, and ongoing institutional reforms. Early case studies, from e-health records to AI chatbots, illustrate both the promise and complexity of these changes. Key challenges remain in skills, infrastructure, and legal clarity. As Romania continues its digital transformation, the impact on citizens will depend on maintaining trust and rights while harnessing technology for better, faster public services.

General Conclusions

The rapid digitalization of Romania's public administration, driven by the National Recovery and Resilience Plan (PNRR), presents a fundamental paradox. While AI and digital tools (such as the Government Private Cloud and ROeID) offer significant improvements in administrative efficiency and citizen services, they introduce profound risks to fundamental privacy rights. The concentration of vast amounts of personal data in centralized systems creates unprecedented vulnerabilities regarding data breaches and unauthorized processing.

Romania occupies a complex transitional space regarding regulatory compliance, like the General Data Protection Regulation is well-established within the public sector. Public authorities are explicitly subject to the law, mandated to appoint Data Protection Officers (DPOs), and face active auditing and sanctions from the National Supervisory Authority (ANSPDCP) for non-compliance. Implementation of the EU AI Act is still evolving. While the government has approved a National AI Strategy (2024–2027) and is drafting legislation that may impose stricter penalties than the EU itself, formal institutional structures, such as designated supervisory bodies, were delayed beyond EU deadlines.

Successful governance is hindered by outdated legacy IT systems, limited rural connectivity, and a significant lack of digital literacy among public servants, which complicates the practical application of privacy laws. Sustainable digital governance requires moving beyond reactive compliance to a proactive *Privacy by Design* approach. To maintain public trust, AI systems must ensure transparency and retain human oversight for critical administrative decisions.

Based on the limitations and gaps identified in the text, here are concrete proposals for future research: investigate the direct correlation between digital literacy levels and citizens' trust in automated government decisions (*e.g.*, tax assessments), moving beyond legal analysis to capture the user experience, conduct a multi-year study tracking the practical enforcement of Romania's upcoming AI laws (2024–2027) to determine if strict proposed penalties (up to €20M) are effectively applied

or remain symbolic, compare Romania's digital governance with other EU nations facing similar rural connectivity gaps to identify best practices for maintaining data privacy despite aging legacy infrastructure.

References

- AI in Romania: The potential for the public sector | McKinsey, <https://www.mckinsey.com/industries/public-sector/our-insights/the-transformative-potential-of-ai-in-romania-s-public-sector> [accessed on: 05.02.2026].
- Al-Kasasbeh Hisham Hamed, Albalawee Nasir, Al-Khawaja Haneen A., Qtaishat Ali Khaled, *Legal Challenges of Using AI and Big Data in Public Administration: Administrative Liability, Data Protection, and Public Services Efficiency* in International Journal of Sustainable Development and Planning, vol. 20, no. 6, June, 2025, pp. 2639-2650.
- Belbe Anisoara, Implementation and Application of GDPR In Romanian Educational Institutions, in *The Annals of the University of Oradea. Economic Sciences* TOM XXXI, 1st Issue, July 2022, pp. 160-171.
- Cavoukian Ann, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, Canada 2011.
- Data Privacy Management in Romania – Compliance & Law, <https://responsum.eu/privacy-management-in-romania/> [accessed on: 05.02.2026].
- European Commission, The Artificial Intelligence Act. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.
- European Data Protection Board, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 2018.
- Francu Cristian Constantin, Sava Ștefan, Global Perspectives on Digital and AI Legislation: A Comparative Study of Data Protection, AI Governance, and Healthcare Innovations with a Focus on Romania, DOI: 10.2478/picbe-2025-0191, *Proceedings of the 19th International Conference on Business Excellence 2025*, Sciendo, pp. 2469-2481.
- Gellert, R. M. (2015). Understanding data protection as risk regulation. *Journal of Internet Law*, 18(11), 3-15.
- National Supervisory Authority for Personal Data Processing, Annual Activity Report 2022, Bucharest, 2023.
- Romania and the EU AI Act: Ready or Just Warming Up? <https://eurocloud.org/news/article/romania-and-the-eu-ai-act-ready-or-just-warming-up/> [accessed on: 26.01.2026].
- Romania Data Protection Laws of the World <https://www.dlapiperdataprotection.com/index.html?t=law&c=RO> [accessed on: 05.02.2026].
- Romania Digital Transformation: Launch of Major Procurement for Government Private Cloud Migration <https://www.trade.gov/market-intelligence/romania-digital-transformation-launch-major-procurement-government-private> [accessed on: 05.02.2026].
- Romania – Digital Economy, Romania Country Commercial Guide at <https://www.trade.gov/country-commercial-guides/romania-digital-economy> [accessed on: 05.02.2026].
- Selbst Andrew D. et al., Fairness and abstraction in sociotechnical systems, in *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 2019, pp. 59-68.
- Study: Romanians do not trust AI without human intervention, <https://www.romaniajournal.ro/business/study-romanians-do-not-trust-ai-without-human-intervention-seven-out-of-ten-prioritise-data-protection/> [accessed on: 08.02.2026].
- Thelle Martin H. et al., The opportunity of AI in public administration in Romania, Capturing the benefits of AI in public administration, *An implement Consulting Group by Google*, October 2024.

- Wachter Sandra, Brent Mittelstadt, Luciano Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, *International Data Privacy Law*, vol. 7, no 2, 2017, pp. 76-99.
- Yeung Karen, Algorithmic Regulation: A Critical Interrogation (May 23, 2017). TLI Think! Paper 62/2017, Regulation & Governance, Forthcoming, King's College London Law School Research Paper No. 2017-27, Available at: SSRN: <https://ssrn.com/abstract=2972505> [accessed on: 25.01.2026].
- Zarsky Tal, The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making, *Science, Technology, & Human Values*, vol. 41, no 1, 2016, pp. 118-132.