International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

Audit Trails and AI Transparency: Regulatory Compliance under the EU AI Act

Mara Grivokostopoulou[1], Athanasios Davalas[2] and Maria Tsiogka[3]

[1]Internal Auditor

[2]Academic Program Director Artificial Intelligence, eLearning, University of the Aegean.

[3]e-learning Lecturer, University of the Aegean.

DOI: 10.46609/IJSSER.2026.v11i02.031 URL: https://doi.org/10.46609/IJSSER.2026.v11i02.031

Received: 2 January 2026 / Accepted: 10 February 2026 / Published: 10 march 2026

ABSTRACT

Audit trails serve as pivotal technical mechanisms for ensuring transparency and traceability, both of which are critical for compliance with the European Union's AI Act. This paper provides an analysis of the regulatory imperatives regarding operational transparency, automated event logging, and human oversight within the context of high-risk artificial intelligence systems. It scrutinizes the fundamental technical attributes of audit trails, the challenges inherent in their implementation, and the organizational and institutional prerequisites necessary for their effective integration. Furthermore, the study presents indicative tools and technological solutions—such as the ELK stack, Apache Kafka, and explainability techniques like SHAP and LIME—demonstrating their capacity to support compliance, transparency, and oversight. The analysis suggests that these mechanisms do not merely facilitate regulatory adherence but also enhance operational reliability, accountability, and the continuous monitoring of artificial intelligence systems throughout their lifecycle.

Keywords: AI Act, AI Transparency, Audit Trails, Regulatory Compliance, Traceability

Acknowledgement: "*This special edition constitutes the work of students from the AI programs of the Lab ICT Heron and the CE-LLC of the University of the Aegean"*

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

1. Introduction

1.1. Background and importance of transparency in artificial intelligence and audit trails

In an era where artificial intelligence models increasingly influence decision-making in sensitive sectors such as healthcare, the economy, and public administration, the demand for transparency and accountability transcends mere technical necessity; it becomes fundamental to maintaining trustworthy governance. The integration of AI into critical decision-making processes renders the assurance of transparency imperative. Given the "black box" nature characterizing many AI models, both regulators and users have raised significant concerns regarding the opacity of automated decision-making processes (European Union, 2024; Hartmann et al., 2024). Within this context, audit trails—defined as detailed records of an AI system's operations and decisions—emerge as indispensable tools for ensuring traceability and compliance (AuditBoard, 2024). In response to these challenges, the European Union has established a horizontal regulatory framework through the Artificial Intelligence Act (AI Act), aiming to foster trustworthy and human-centric artificial intelligence (Manheim et al., 2024).

1.2. Overview of the AI Act

The AI Act stipulates that transparency is achieved when AI systems are developed and operated in a manner that guarantees sufficient traceability and explainability. This includes the obligation to inform users when they are interacting with an AI system, while also providing clear information regarding the system's capabilities and limitations (Manheim et al., 2024). However, compliance with these requirements is far from trivial. Many high-risk AI systems rely on complex algorithms, which complicates the task of explaining their decisions and monitoring their actions effectively.

1.3 Purpose and objectives of the article

The present study scrutinizes the role of audit trails—records that document the critical actions and decisions of an AI system in chronological order—as a primary mechanism for enhancing transparency. By doing so, it underscores the importance of transparency in cultivating trust in artificial intelligence and offers guidance for organizations aiming to develop legally compliant and reliable AI systems (Fang et al., 2024). The objective is to delineate the technical characteristics, implementation challenges, and best practices regarding design, operation, and oversight, specifically within the context of regulatory compliance with the AI Act.

2. Regulatory Framework of the AI Act

2.1. Key provisions on transparency, recording, and traceability

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

The European Union's regulatory framework for artificial intelligence introduces a risk-based classification system, imposing escalating transparency and oversight requirements commensurate with the potential impact of the system in question (European Union, 2024). The AI Act explicitly prohibits specific AI applications deemed to pose an unacceptable risk (e.g., social scoring systems), while simultaneously mandating strict obligations for high-risk AI systems (HRAIS). Among these obligations, transparency and traceability occupy a central position (ECIIA, 2025; European Commission, 2025).

Articles 12, 13, and 14 of the AI Act define the core requirements for the functional transparency of AI systems.

According to Article 12, high-risk AI systems must incorporate automatic logging mechanisms throughout their lifecycle. This requirement is designed to ensure sufficient traceability of the system's operations relative to its intended purpose. The logged records must facilitate the identification of hazardous situations, post-market surveillance, compliance verification, and oversight by both providers and regulatory authorities (European Union, 2024; ECIIA, 2025). As noted by Deloitte (2023, p. 3), users are obligated to maintain automatically generated records to the extent that such records are under their control (record-keeping). For specific applications, such as biometric identification systems, the records must explicitly capture the time of use, the reference database utilized, the input data processed, and the identity of the individuals verifying the results. Additionally, providers of high-risk AI systems are required to retain technical documentation and logs for a period of up to 10 years, enabling regulators to reference specific points in the system's operation in the event of errors or malfunctions (ECIIA, 2025).

Article 13 establishes transparency and information obligations for both providers and users. Providers must notify users when they are interacting with AI systems and supply clear instructions for use. In the case of high-risk systems, providers are required to disclose the system's capabilities and limitations, information necessary for safe and appropriate use, and potential risks associated with its deployment. Furthermore, the Regulation imposes transparency and information requirements on users, which are directly linked to the safety and responsible use of AI systems (Deloitte, 2023). This aligns with the general principle of the AI Act, which posits that individuals must be aware they are interacting with an AI system and understand its impact on decisions affecting them.

Moreover, Article 14 sets out human oversight requirements for high-risk AI systems, ensuring that their decisions can be monitored, interpreted, and, when necessary, reviewed or overruled (European Union, 2024). As Deloitte (2023, p. 3) observes, providers must implement a robust post-market monitoring system to ensure continued compliance throughout the system's lifetime. The aim of this provision is to prevent excessive reliance on automated decisions and mitigate

ISSN: 2455-8834

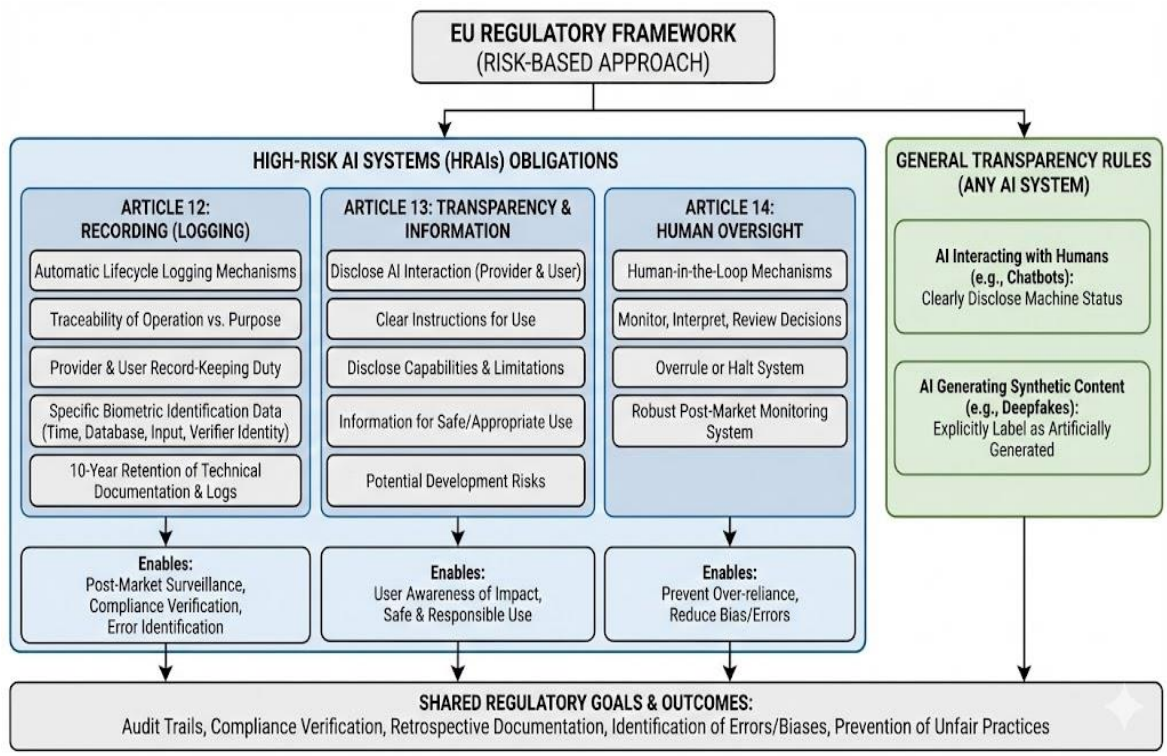
Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

the risk of biased or erroneous outcomes resulting from algorithmic use. This aligns with recent scholarly discourse emphasizing that AI should function as a complementary tool rather than a substitute for human judgment. Dwivedi (2025) argues that maintaining a balance between human ingenuity and AI capabilities is critical, and audit trails serve as the technical mechanism enabling this "supervised autonomy," thereby preventing over-reliance on automated systems.

In addition to provisions for high-risk AI systems, the AI Act establishes general transparency rules for specific applications, regardless of risk category. For instance:

- AI systems interacting with humans (e.g., chatbots) must clearly disclose that the user is communicating with a machine (ECIIA, 2025).
- AI systems generating synthetic content (e.g., deepfakes) are required to explicitly label the content as artificially generated to prevent misleading the public (ECIIA, 2025).

These provisions ensure a baseline level of transparency for all AI algorithms, even those not classified as high-risk, rendering audit trails an essential tool for documenting compliance, retrospectively interpreting decisions, identifying errors or biases, and preventing unfair practices (European Union, 2024). A schematic overview of these regulatory obligations and transparency rules is presented in **Figure 1**.



ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

2.2 Technical analysis of compliance requirements

Beyond the institutional analysis of these provisions, it is essential to examine how the requirements of the AI Act can be met in practice. Specifically, Articles 12, 13, and 14—concerning logging, transparency, and human oversight—can be technically implemented through the appropriate integration of audit trails. The technical integration of such tools is a prerequisite for organizations to achieve operational compliance with traceability, transparency, and oversight obligations.

Audit trails provide chronologically ordered, tamper-proof, and technically documented records of an AI system's operations and decisions, thus constituting a practical tool for implementing Article 12 on event logging (European Union, 2024). At a technical level, they can automatically record critical processes such as data input and output, model activation, user choices, and decision flows, thereby contributing to the system's overall traceability.

Furthermore, they serve as a means of implementing Article 13 by supporting transparency through the accessible and structured recording of decisions. This allows sufficient information to be provided to users—for example, regarding the capabilities, limitations, and potential impacts of the system. Transparency extends beyond backend logging to user-facing documentation. Innovative approaches, such as the "Startup Idea Evaluator," demonstrate how AI can generate automated, comprehensive reports (e.g., Scorecards, SWOT analyses). This capability practically fulfills the transparency requirements of Article 13 by providing end-users with understandable explanations of the system's decision-making logic (Davalas et al., 2025).

Technical documentation through audit trails also enhances compliance with Article 14, which concerns human oversight. Maintaining auditable and readable records facilitates independent verification of system operation by competent authorities and supports the possibility of human intervention in critical cases (ECIIA, 2025; ISACA, 2024).

Audit trails play a crucial role in documenting the compliance of high-risk AI systems with the European Union's AI Act, particularly Articles 12, 13, and 14. They support independent decision documentation and enhance accountability, making them an integral part of a broader control ecosystem. Furthermore, compliance should not be limited to the initial development phase but must cover the entire lifecycle, including post-market monitoring. This is critical for continuous assessment, addressing unforeseen risks, and ensuring ongoing compliance with regulatory requirements (ECIIA, 2025).

3. Understanding Audit Trails in Artificial Intelligence Systems

3.1 Definition, scope, and importance of audit trails

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

Audit trails refer to the chronological recording of all actions and decisions taken by an artificial intelligence system (AuditBoard, 2024). They constitute a critical element of transparency and accountability, enabling auditors, regulators, and other stakeholders to analyze the decision-making processes of AI algorithms. An audit trail in an AI system includes detailed records of its operations, ranging from data input and processing to final decisions and subsequent actions. These trails cover all stages of the system's lifecycle, ensuring traceability from development through to post-release operation (Hartmann et al., 2024).

The necessity of such mechanisms is underscored by research utilizing SWOT analysis on AI in critical decision-making contexts, such as startup valuation. These studies identify "opacity" as a fundamental weakness of AI systems, highlighting that audit trails are essential for mitigating this risk and ensuring that algorithmic outputs are not perceived as arbitrary "black boxes" (Davalas et al., 2022).

By recording the operational progress of AI systems, audit trails can support the identification of algorithmic bias. In the context of independent audits, such as bias audits, operational records are used to highlight algorithmic patterns related to protected characteristics, such as age or gender (Hartmann et al., 2025). Similarly, methodologies utilizing such logs have been implemented to uncover unfair treatment in credit rating systems, highlighting their contribution to diagnosing unlawful deviations (Fang et al., 2024). It is worth noting that audit trails are inherent technical features of the AI systems themselves, whereas bias audits are external evaluation procedures that utilize, but do not include, such records. This distinction is critical for the proper interpretation of compliance tools (Hartmann et al., 2025).

An effective audit trail system functions as part of a broader AI control ecosystem, which includes various types of controllers and controls. Although these subsystems may operate independently in terms of institutional position, they are functionally interdependent within a common ecosystem of transparency and oversight (Hartmann et al., 2024). This holistic approach reinforces and enables the practical implementation of transparent and accountable oversight, contributing significantly to regulatory compliance and strengthening user confidence in AI systems.

3.2 Key technical features of audit trails

The technical implementation of audit trails in AI systems is a critical step towards enhancing traceability, explainability, and compliance with the AI Act. A fully functional audit trail is not limited to the chronological recording of events; rather, it requires a combination of technical features, security mechanisms, recording tools, and analysis methods. Key technical features include time stamping, data logging, identification, and metadata (AuditBoard, 2024). These

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

features constitute the fundamental technical requirements for compliance with Article 12 of the AI Act regarding the recording and traceability of AI systems (European Union, 2024).

3.3 Audit trail implementation tools and explainability techniques

Implementing effective audit trails in AI systems requires a synthesis of logging software tools, documentation standards, and explainability techniques. To automate logging, solutions such as the ELK Stack (Elasticsearch, Logstash, Kibana) and Apache Kafka are widely used, enabling continuous data flow and real-time storage. ELK facilitates the monitoring and visualization of event flows, while Kafka supports real-time event logging, thereby enhancing the traceability and integrity of log files (Eisenberg et al., 2025; Khandelwal, 2024).

Scientifically structured documentation of methodological choices and results is enhanced by integrating recognized standards, such as Model Cards and Datasheets for Datasets. These provide transparent and standardized information about the functionality, limitations, and potential biases of AI systems. The use of these standards meets the transparency requirements of Article 13 of the AI Act, providing users with the information necessary for proper use (Pistilli et al., 2023; Hartmann et al., 2024).

Technical explainability completes the suite of compliance tools. Explainability techniques such as SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) enhance the interpretability of algorithmic decisions, contributing to a better understanding of their operation and strengthening user trust (Zderic, 2025; Panigutti et al., 2023). For example, in credit rating systems, audit trails enable retrospective monitoring of the system's inputs, decisions, and outputs. Through documented recording, it becomes possible to identify deviations or irregular patterns, enhancing transparency and compliance with the accountability requirements of the AI Act.

3.4 Technical security and integrity mechanisms to protect audit trails

Protecting the integrity and confidentiality of audit trails is a critical parameter for compliance with both the AI Act and the General Data Protection Regulation (GDPR). Due to their sensitive nature, audit trails must be shielded from alteration, deletion, or unauthorized access to ensure their reliability and legal validity.

To effectively manage associated risks, the following security techniques are implemented:

- **Immutable storage:** This ensures that records cannot be modified or deleted after their initial creation. Solutions using databases such as immudb enable the implementation of this feature, providing an unalterable history of operations. Furthermore, recent research

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

highlights Blockchain technology as a robust mechanism for ensuring data integrity and simplifying compliance in digital government contexts (Davalas & Angelaki, 2025).

- **Log file encryption:** Symmetric encryption renders data inaccessible without the corresponding key, protecting audit trails from leakage or malicious modification. The use of certified encryption algorithms ensures compliance with Article 32 of the GDPR.
- **Distributed decryption mechanisms ("secret sharing schemes"):** Access keys are distributed among multiple parties (e.g., technical team, legal advisor, external auditor) such that collaborative access is required. This approach prevents arbitrary or abusive access, enhancing accountability and institutional transparency.
- **Tamper-evident logging:** Any alteration to the log data must leave an indelible mark, ensuring that unauthorized actions can be detected.

The proper implementation of these techniques protects audit trails from internal or external threats, enabling them to document regulatory compliance and support the oversight process. In high-risk environments, such as those described in the AI Act, the accuracy, integrity, and security of logs are not merely operational requirements; they are legal obligations.

3.5 Regulatory documentation and interoperability

The function of audit trails is not limited to technical monitoring; it is inextricably linked to meeting the regulatory requirements of the AI Act. Their existence serves traceability, accountability, and transparency, as defined in Articles 12–14 of the Regulation (European Union, 2024). Additionally, they support the continuous monitoring of the system's operation (Article 61) and the possibility of conducting external audits (Article 71).

A typical example of the application of compliance tools is the "LLM Checker," developed by LatticeFlow AI in collaboration with ETH Zurich and INSAIT Bulgaria. This tool evaluates general-purpose models for robustness, biased output, and auditability, assigning a compliance score based on AI Act requirements. Its assessments revealed serious weaknesses in popular LLMs, such as prompt hijacking, indicating the need for technical transparency and traceability mechanisms at an early stage. This initiative, recognized by the European Commission, offers a working example of the holistic implementation of Articles 12–14 of the AI Act (Reuters, 2024).

Beyond the AI Act, audit trails serve as a point of convergence for European Union regulatory requirements. Specifically, they contribute to interoperable compliance with the GDPR (Article 5.2 – accountability), the NIS2 Directive (information systems security), and the DSA Regulation (responsibility of digital service providers), strengthening the coherence of the

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

regulatory documentation system (European Commission, 2025; ISACA, 2024). Moreover, recent research underscores that integrating robust cybersecurity measures into AI tools is critical for compliance with frameworks like GDPR and the NIS2 Directive. This compliance is not merely a legal obligation but a strategic asset that enhances the reliability of the tools and fosters trust among stakeholders (Davalas et al., 2025).

4. Transparency and Compliance: Challenges in Implementing the AI Act Regulation

4.1 Challenges in complying with the requirements of the AI Act Regulation

Despite progress in the technical development of explainability tools such as SHAP and LIME, the practical application of the AI Act's principles faces significant institutional, organizational, and operational obstacles.

One of the most decisive challenges lies in the absence of institutionalized and operationally mature technical standards and clear guidelines. This reinforces regulatory uncertainty and hinders the practical implementation of compliance obligations (ECIIA, 2025; Manheim et al., 2024). Although the transparency requirements of Article 13 stipulate the need for understandable and adequate information for users, existing explainability tools have not yet reached a level of maturity that supports their widespread operational use (Pavlidis, 2025; Salih et al., 2024).

The asymmetry of capabilities between large and small organizations presents another obstacle. Large technology companies possess sufficient resources to develop transparency and accountability mechanisms, whereas smaller companies often struggle to meet the same requirements (Fang et al., 2024). This discrepancy creates a regulatory gap that jeopardizes the equitable application of the Regulation.

Furthermore, compliance is affected by institutional tensions surrounding trade secret protection. Many AI providers are concerned that disclosing technical information (e.g., algorithms) for transparency purposes may harm their competitiveness (Holst et al., 2024). The absence of clear regulations balancing transparency with intellectual property protection reinforces reservations regarding the implementation of the AI Act.

Finally, there is a lack of institutional support and ongoing training for organizations regarding both technical options and compliance policies. Compliance teams are required to implement regulatory requirements without a clear support framework, leading to fragmented practices and defensive strategies (Manheim et al., 2024). The successful implementation of the AI Act cannot rely solely on technical solutions; it requires the integration of a coherent organizational governance model, which includes documented oversight procedures, internal control

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

mechanisms, defined roles, and clear responsibilities for each stage of the system's lifecycle (Manheim et al., 2024).

For example, international literature recommends integrating compliance frameworks, such as the Unified Control Framework (UCF), which allows for the coordination of regulatory requirements and the definition of clear roles and responsibilities through standardized oversight procedures (Eisenberg et al., 2025). Although the UCF does not originate from the AI Act, it is a tool that can be adapted to the EU regulatory framework, enhancing organizational maturity and preventive compliance.

The effective integration of audit trails as compliance tools therefore requires a holistic approach that incorporates not only technical solutions but also institutional guidance, governance policies, and human intervention (ECIIA, 2025; Pavlidis, 2025). Without this comprehensive adaptation, the AI Act risks remaining a theoretical construct devoid of practical application.

4.2 Shortcomings and Uncertainties in the Implementation of the Regulatory Framework

Although audit trails are closely linked to the requirements of the AI Act, as discussed in subsection 3.5, significant regulatory and institutional gaps remain that hinder systematic and meaningful compliance. While the regulatory framework has established clear principles of transparency and control for AI systems, the absence of defined technical and institutional tools prevents its uniform application across the European market (ECIIA, 2025; Manheim et al., 2024). A primary issue lies in the vagueness of definitions and scope. Concepts used to define risk categories (such as "general-purpose AI" or "high-risk system") are not always sufficiently defined, making it difficult for many providers to determine whether and how the Regulation's obligations apply to them (Renieris et al., 2024; Manheim et al., 2024).

At the same time, the lack of mandatory institutionalization of third-party access—such as by independent researchers or social actors—to audit logs or technical data creates gaps in transparency and independent evaluation. The institutional disconnect between the Regulation's requirements and the actual possibility of external control limits the practical enforcement of the AI Act's provisions. Consequently, the regulatory framework risks remaining at the level of theoretical provisions, unaccompanied by adequate practical control tools or an effective accountability mechanism (Hartmann et al., 2024).

The situation is further complicated by the lack of mature technical standards and guidelines that would enable the implementation of the Regulation's requirements at a technical and operational level (ECIIA, 2025). Although the AI Act provides for the publication of specific implementing texts and standards by European standardization bodies (such as CEN and CENELEC), the relevant procedures are still ongoing (European Commission, 2025). This transitional phase

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

causes significant uncertainty for compliance teams, which are required to design and implement control policies without a clear technical roadmap.

Significant challenges are also faced by small and medium-sized enterprises (SMEs) and startups, which lack the necessary technical and human resources to develop transparency and auditability systems. Although the Regulation encourages innovation, the complexity and cost of compliance can act as a deterrent for companies without access to specialized tools and expertise (Fang et al., 2024). This inequality of access creates the risk of establishing a new regulatory gap, wherein only large companies have the capacity to meet the requirements.

Finally, it should be noted that large technology companies have lobbied to limit or weaken provisions on transparency and mandatory access to critical information on AI systems, particularly regarding general-purpose systems (Corporate Europe Observatory, 2025). The argument of intellectual property protection or trade secrets is often used as an obstacle to the full implementation of access and documentation requirements, as providers express concerns that disclosing sensitive information could undermine their competitive advantage and discourage investment in innovation (Holst et al., 2024).

Overall, the existence of institutional gaps, delays in the development of technical standards, the absence of robust independent oversight mechanisms, and the disproportionate burden on small organizations create an enforcement landscape that, despite good intentions, undermines meaningful compliance with the transparency and accountability principles of the AI Act. The effective integration of audit trails as compliance mechanisms requires the development of clear regulatory guidance, institutional guarantees for third-party access to critical data, and support for companies that do not yet have the expertise or resources to implement such mechanisms.

5. Conclusions

The integration of audit trails as technical mechanisms for transparency, traceability, and accountability is a fundamental prerequisite for operational and regulatory compliance with the requirements of the AI Act, particularly regarding high-risk artificial intelligence systems. The analysis has demonstrated that their implementation is not merely a technical undertaking; it requires institutional maturity, organizational readiness, and sufficient expertise to ensure both operational and regulatory compliance.

Audit trails can act as a catalyst for establishing a coherent governance framework for artificial intelligence, grounded in transparency, accountability, and the protection of fundamental rights. Their integration into technological and organizational structures enables human oversight, independent documentation of decisions, and the prevention of unfair or erroneous outcomes.

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

Extensions of this approach include the targeted evaluation of applications in critical areas, such as healthcare and credit rating, where the existence of technical transparency mechanisms can enhance the social acceptance of AI and ensure compliance with European Union values. Beyond regulatory compliance, audit trails enhance the operational reliability of systems and enable their continuous adaptation to technical and institutional developments.

As the AI landscape evolves, meaningful transparency cannot be limited to legal provisions; it requires the conscious integration of principles of accountability, technical documentation, and auditable design at all stages of a system's lifecycle. Compliance with the AI Act is not only a challenge but also an opportunity to establish a responsible and human-centered artificial intelligence ecosystem in Europe.

References

- Aßmuth, A., Duncan, R., Liebl, S., and Söllner, M. (2024). A secure and privacy-friendly logging scheme. arXiv preprint arXiv:2405.11341. Available at: https://arxiv.org/abs/2405.11341 [Accessed: 7 Apr. 2025].
- AuditBoard (2024). What Is an Audit Trail? Everything You Need to Know. Available at: https://www.auditboard.com/blog/what-is-an-audit-trail/ [Accessed: 29 March 2025].
- Corporate Europe Observatory (2025). Setting the rules of their own game: How Big Tech is shaping AI standards. [online] Corporate Europe Observatory. Available at: https://www.corporateeurope.org/en/2025/01/setting-rules-their-own-game-how-big-tech-shaping-ai-standards [Accessed: 12 Apr. 2025].
- Davalas, A., & Angelaki, A. (2025). Digital Government Policies for Supporting Startups and Entrepreneurs. In M. Themistocleous et al. (Eds.), EMCIS 2024 (LNBIP 535, pp. 350–366). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-81322-1_24
- Davalas, A., Angelaki, A., & Charalabidis, Y. (2025). Startup Idea Evaluator: Supporting and Evaluating Early-Stage Startup Ideas Using ChatGPT. International Journal of Social Science and Economic Research, 10(1), 415-424. https://doi.org/10.46609/IJSSER.2025.v10i01.024
- Davalas, A., Charalabidis, Y., & Fenekoy, P. (2022). Startup Valuation with Artificial Intelligence: A SWOT Analysis. European Journal of Economics, 2(2), 13-20. https://doi.org/10.33422/eje.v2i2.154

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

- Deloitte. (2023). EU AI Act adopted by the Parliament: What's the impact for financial institutions? [Online]. Deloitte Luxembourg. Available at: https://www.deloitte.com/lu/en/Industries/investment-management/perspectives/european-artificial-intelligence-act-adopted-parliament.html [Accessed: 23 March 2025].

- ECIIA. (2025). The AI Act: Road to Compliance – A Practical Guide for Internal Auditors. European Confederation of Institutes of Internal Auditing (ECIIA). Available at: https://www.eciia.eu/publications/the-ai-act-road-to-compliance. Available upon request from professional auditing networks or institutional databases. [Accessed: 24 March 2025].

- Eisenberg, I.W., Gamboa, L. and Sherman, E. (2025). The Unified Control Framework: Establishing a Common Foundation for Enterprise AI Governance, Risk Management and Regulatory Compliance. [preprint] arXiv:2503.05937. Available at: https://arxiv.org/abs/2503.05937 [Accessed 8 Apr. 2025].

- European Commission. (2025). Regulatory Framework for Artificial Intelligence (AI) in the EU. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai [Accessed: 26 March 2025].

- European Commission. (2025). Shaping Europe's Digital Future: Regulatory Framework on Artificial Intelligence. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai [Accessed 12 Apr. 2025].

- European Union. (2024). Regulation (EU) 2024/1689 of 29 September 2024 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the EU, L 257. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 [Accessed: 14 March 2025].

- Fang, S., Chen, Z., & Ansell, J. (2024). Peer-induced Fairness: A Causal Approach for Algorithmic Fairness Auditing. arXiv preprint arXiv:2408.02558. Available at: https://arxiv.org/abs/2408.02558 [Accessed: 14 March 2025].

- Hartmann, D., de Pereira, J. R. L., Streitbörger, C., & Berendt, B. (2024). Addressing the Regulatory Gap: Moving Towards an EU AI Audit Ecosystem Beyond the AIA by Including Civil Society. arXiv preprint arXiv:2403.07904v3. Available at: https://arxiv.org/abs/2403.07904v3 [Accessed: 14 March 2025].

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

- Holst, L., Mayer, V., Lämmermann, L., Urbach, N., and Werder, K. (2024). The impact of the EU AI Act's transparency requirements on AI innovation. Conference paper presented at the 19th International Conference on Wirtschaftsinformatik (WI 2024), Vienna, Austria, 6–10 July. Available at: https://www.researchgate.net/publication/382027689 [Accessed 12 Apr. 2025].

- ISACA. (2024). Understanding the EU AI Act. ISACA White Paper. Available at: https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act [Accessed: 23 March 2025].

- Khandelwal, A. (2024). Leveraging Databricks engineering to build a robust data governance framework. DXC Technology. Available at: https://www.dxc.com [Accessed 16 Apr. 2025].

- Manheim, D., Martin, S., Bailey, M., Samin, M., & Greutzmacher, R. (2024). The Necessity of AI Audit Standards Boards. arXiv preprint arXiv:2404.13060v1. Available at: https://arxiv.org/abs/2404.13060v1 [Accessed: 14 March 2025].

- Panigutti, C., Hamon, R., Hupont, I., Fernández-Llorca, D., Fano Yela, D., Junklewitz, H., Scalzo, S., Mazzini, G., Sánchez, I., & Gómez, E. (2023). The role of explainable AI in the context of the AI Act. Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), pp. 1139–1150. Available at: https://doi.org/10.1145/3593013.3594069 [Accessed 7 Apr. 2025].

- Pavlidis, G. (2025). Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI. [online] arXiv. Available at: https://arxiv.org/abs/2502.14868 [Accessed 12 Apr. 2025].

- Pistilli, G., Muñoz Ferrandis, C., Jernite, Y., and Mitchell, M. (2023). Stronger together: On the articulation of ethical charters, legal tools, and technical documentation in ML. arXiv:2305.18615 [online]. Available at: https://doi.org/10.48550/arXiv.2305.18615 [Accessed 7 Apr. 2025].

- Reuters. (2024). EU AI Act checker reveals Big Tech's compliance pitfalls. Available at: https://www.reuters.com/technology/artificial-intelligence/eu-ai-act-checker-reveals-big-techs-compliance-pitfalls-2024-10-16/ [Accessed: 13 May 2025].

- Renieris, E.M., Kiron, D., & Mills, S. (2024). Organizations Face Challenges in Timely Compliance With the EU AI Act. MIT Sloan Management Review, June 2024. Available

ISSN: 2455-8834

Volume:11, Issue:02 "February(InfoPolis.Gr - Special Edition) 2026"

at: https://sloanreview.mit.edu/article/organizations-face-challenges-in-timely-compliance-with-the-eu-ai-act [Accessed: 14 Apr. 2025].

- Salih, A.M., Raisi-Estabragh, Z., Galazzo, I.B., Radeva, P., Petersen, S.E., Lekadir, K. and Menegaz, G. (2024). A Perspective on Explainable Artificial Intelligence Methods: SHAP and LIME. Advanced Intelligent Systems, 7(1), p.2400304. Available at: https://doi.org/10.1002/aisy.202400304 [Accessed 12 Apr. 2025].

- Zderic, M. (2025). What the EU AI Act means for AI software development: Everything you need to know. DECODE. [online] Available at: https://decode.agency/article/eu-ai-act-software-development/ [Accessed 6 Apr. 2025].

