Leadership's Role in Protecting Personal Data in the Age of Artificial Intelligence

Andrei Constantin TÎRNOVANU[1]
Gabriela-Elena STAN[2]
Maria Mihaela DUCA[3]
Marius IOSIF[4]

Abstract

The rapid development of Artificial Intelligence generates significant benefits for organizations, but also increased risks for the protection of personal data. The ability of AI systems to collect, analyses, and correlate large volumes of information raises issues regarding confidentiality, transparency, and respect for fundamental rights. Compliance with the General Data Protection Regulation (EU) 2016/679 is an essential regulatory framework, but effective protection depends directly on the involvement of organizational leadership.

The article explores the importance of leadership in the integrating data protection principles into strategies and decision-making processes regarding the use of Artificial Intelligence. Emphasis is placed on the importance of managerial responsibility, organizational culture, and ethical data governance. The paper argues that leadership is a determining factor in transforming legal obligations into real and sustainable protection of personal data in the digital age.

Keywords: *Artificial Intelligence, leadership, personal data, data governance, privacy.*

JEL classification: M12, K22, O33

DOI: 10.24818/RMCI.2026.1.123

1 Introduction

Artificial Intelligence (AI) has made its way into people's daily lives as an algorithmic mechanism designed to make many tasks easier that only humans could do before. From virtual assistants and recommendation systems to decision-making algorithms in crucial areas, AI has become a widespread presence, whose manifestations far exceed early vision of intelligence machines.

[1] Andrei Constantin Tîrnovanu, Bucharest University of Economic Studies, tirnovanuandrei17@stud.ase.ro
[2] Gabriela-Elena Stan, Bucharest University of Economic Studies, stangabriela21@stud.ase.ro
[3] Maria Mihaela Duca, Bucharest University of Economic Studies, ducamaria21@stud.ase.ro
[4] Marius Iosif, Dunarea de Jos University of Galați, Romania, iosif.marius89@yahoo.com

AI is currently considered the most powerful driver of social change (Niță, 2021) constantly evolving and generating fundamental changes in all spheres of human activity. During its evolution, it has experienced both periods of decline, driven by people's fears about transparency and safety, and periods of remarkable success, marked by interest in algorithmic decision-making, machine learning, systems, and cognitive services (Cath et al., 2018). Significant advances in processing massive amounts of information, analyzing, and predicting human behavior have been accompanied by impressive developments in related fields such as robotics, computer vision, autonomous systems etc.

The recent computational explosion of Artificial Intelligence systems is not an accident, but stemmed from the confluence between crucial technological advancements in machine learning and the gigantic amount of data available. This process, named "datafication", entails turning ever more facets of social and economic life into quantifiable data, which can then be mined algorithmically. Thus, the phenomenon of AI spread is much more complex than a purely technological issue and it creates an ever-accelerating dissemination of data-based services and products in public and private sectors, regardless of the industry domain.

From a legal perspective, AI has become the subject of fundamental debates on the protection of human rights. The reasons why legal practitioners have deemed it necessary to analyze and regulate intelligent systems lie in the ability of these technologies to interact with users, provide automatic responses to their needs, and perform tasks by processing personal data or data that falls between the line of personal data and non-personal data. It is precisely this fundamental feature of AI that can infringe on fundamental rights, creating significant risks in terms of confidentiality, transparency, and non-discrimination.

Experimentation and progress in some sectors of society can provoke a response similar to conservation in others. However, beyond the regulatory framework, the effective protection of personal data in the age of AI depends decisively on the human factor at the top of organizations. This paper aims to analyze the essential role of leadership in integrating data protection principles into strategies and decision-making processes regarding the use of AI, pleading for a managerial vison that transforms legal compliance from a formal obligation into an authentic and sustainable organizational culture.

2 Literature review

2.1 Personal data protection – conceptual framework

The rise of numerous smart applications and devices, which rely on the use of massive amounts of personal data, has led to frequent data leaks caused by a lack of control over data collection and storage. These transparency and management issues have led to a decline in the level of trust that users place in digital platforms (Guo & Zhang, 2025).

In this context, in April 2016, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) was adopted, following the growth of the global population, the development of information technologies, the excessive use of personal information appearing on various social networks, and the procedure for storing and processing personal data. It regulates the processing of personal data relating to individuals in the EU by a natural person, company, or organization. According to Article 4(1) of the aforementioned Regulation, personal data is any information relating to an identified or identifiable natural person.

Purtova (2018) emphasizes that the definition is intentionally very broad in order to cover as many practical situations as possible. Furthermore, according to Hoofnagle et al. (2019), Article 4(1) states that the concept includes objective data, such as income, and subjective data, for example assessments, regardless of whether they are sensitive or ordinary, public or private, digital or on paper. A person is identifiable not only when they are directly named, but also when they can be distinguished by identification number, location data, combination of attributes such as age, area, profession, etc. (Supriyadi, 2023). Data is genuinely non-personal if there is no longer a reasonable risk of re-identification. The literature shows that this benchmark is increasingly difficult to achieve in the era of big data (Finck & Pallas, 2020). Pseudonymization does not remove data from the scope of the GDPR. It remains personal data as long as it can be reattributed to a person with additional information (Mourby et al., 2018).

The term "data" has often been described in the literature as a "contemporary raw material, a kind of post-industrial oil, and its free flow is a necessary condition for the convergence of globalization and digitalization" (Hervé, 2021). Data is at the core of AI's functioning, its value increasing through what it offers, namely: detailed and accurate information, including confidential information. Privacy and personal data protection are two interrelated terms that are often used interchangeably. However, they are in fact two different concepts. Privacy refers generally to the protection of an individual's personal space, while data protection refers to limitations or conditions on the processing of data relating to an identified or identifiable person. Naturally, this leads to the conclusion that the right to privacy derives from the right to intimate, family, and private life, which implies that no one may interfere in a person's intimate, family, and private life without their consent, which must be expressed explicitly and freely (Bădescu, 2023). It has also been emphasized that the principles underlying the right to personal data protection reflect certain key values inherent in the European legal order: confidentiality, transparency, autonomy, and non-discrimination (McDermott, 2017). In other words, it can be accepted that the right to data protection could serve as a guarantee not only for confidentiality, but also for all other fundamental rights.

Recent literature identifies a series of risks that AI systems generate in relation to personal data. Karami et al. (2024) and Alhitmi et al. (2024) point out

that marketing-based AI personalization was based on wide-ranging consumer profiling, where online habits of consumers were calculated to create consumer surrogates using purchase history and contextual data; this creates a tension between hyper-personalization and the protection of privacy. We must take into consideration that many business are moving to online and the volume of activities and data are exponentially increasing, creating both opportunities and vulnerabilities for companies and people (Cristache et al., 2024).

In the area of healthcare, Costina & Corobană (2021) show how researchers conclude that the GDPR was implemented at medical clinics in Romania, highlighting a tendency to mix up medical consent for patients with legal basis for data processing. The authors emphasize that, although patients express their consent for medical treatment, data processing is in fact based on Article 6(1)(b) and (c) of the GDPR (necessity for the execution of a contract and fulfillment of legal obligations), not of consent. Their analysis focuses on the challenges posed by the GDPR in the absence of advanced technologies. However, the complexity of these issues is amplified when Artificial Intelligence systems are integrated. These systems not only store medical data, but also analyze and correlate it to make automated clinical decisions (Udegbe et al., 2024).

While debates on data protection involve both technical and legislative considerations, they also underscore the critical importance of leadership in addressing the risks posed by Artificial Intelligence, as increasingly documented in recent literature. This is in part corroborated by the previously mentioned examples from marketing and medicine, which demonstrate that the problem cuts across disciplines. Although the regulatory framework provides the necessary tools for data protection, its effective implementation poses significant challenges in practice, and the integration of AI exponentially amplifies these difficulties. It becomes clear that the human factor at the top of organizations is what makes the difference between formal compliance and real data protection.

2.2 Leadership

Leadership has increasingly become a critical factor in how organizations respond to the complex challenges generated by digital transformation and the rapid expansion of Artificial Intelligence. In environments where large volumes of personal data are constantly collected, processed, and analyzed, leaders are expected not only to guide organizational performance but also to ensure responsible and ethical decision-making regarding data governance. Effective leadership therefore extends beyond traditional management responsibilities and involves the ability to align technological innovation with legal compliance, ethical principles, and organizational values.

Leadership involves influencing employees' behaviors in order to achieve organizational objectives. For this reason, it represents an essential component of organizational agility, particularly in the context of the digital era, which generates numerous transformations to which all members of the organization must adapt.

Through effective leadership, organizations are better positioned to respond to change and navigate complex environments. Leadership is therefore vital in managing organizational change, as it can facilitate the successful implementation of new initiatives by providing guidance, support, and strategic direction toward the desired future state of the organization (Musaigwa, 2023).

Different leadership styles influence employees' attitudes, behaviors, and performance within organizations, which is particularly important in environments shaped by rapid technological change and digital transformation. Servant leaders support and guide their employees by prioritizing their development and encouraging a culture of service and collaboration, often acting as role models who provide training and mentorship (Năstase, 2010). Transformational leaders, on the other hand, play a key role in fostering innovation and creativity by motivating employees to explore new ideas, take initiative, and assume responsibility for their outcomes. Such leaders inspire employees to identify alternative approaches to their work and contribute to organizational adaptability. Overall, leadership plays a crucial role in shaping employee performance and organizational change, as leaders are well positioned to influence the perspectives and actions of their employees and guide organizations through evolving technological and operational challenges (Musaigwa, 2023).

In contemporary organizations characterized by rapid technological development and increasing digitalization, leadership plays a crucial role in guiding organizational adaptation to complex and uncertain environments. Modern leadership perspectives emphasize that effective leadership involves clear communication, the ability to motivate employees, and the creation of trust within the organization. These elements are particularly important in areas such as cybersecurity and data protection, where employees' awareness and responsible behavior significantly influence organizational resilience (Popa et al., 2022).

The rapid expansion of digital technologies and data-driven systems has significantly transformed how organizations collect, process, and utilize information. While these developments support innovation and operational efficiency, they also expose organizations to increased risks related to information security and the protection of personal data. The growing number of cybersecurity incidents and data breaches has intensified concerns about how sensitive information is managed and safeguarded within organizational environments (Halim et al., 2023).

In this context, leadership plays a fundamental role in establishing responsible practices for handling data. Leaders influence not only strategic decision-making but also the ethical climate within organizations. When leaders actively promote ethical values and accountability, they contribute to the development of policies and practices that prioritize data privacy and responsible information management. Such leadership approaches encourage transparency, strengthen regulatory compliance, and support the creation of trust between organizations and their stakeholders, which has become increasingly important in the digital and AI-driven economy (Halim et al., 2023).

Overall, leadership plays a decisive role in shaping how organizations address the challenges associated with digitalization, cybersecurity, and the protection of personal data. By promoting ethical values, encouraging employee awareness, and integrating responsible data governance practices into organizational strategies, leaders contribute to building resilient and trustworthy institutions. In the context of Artificial Intelligence, where technological capabilities evolve rapidly and regulatory requirements continue to expand, leadership becomes essential for balancing innovation with accountability.

3 Methodology

This study adopts a qualitative research methodology, based primarily on the systematic analysis of relevant legal, managerial, and interdisciplinary literature. The research draws on academic contributions in the fields of artificial intelligence, leadership, data governance, and privacy law, with the objective of identifying the essential role of the human factor at the top of organizations in integrating data protection principles into AI-driven strategies. By reviewing both classical and recent scholarly sources, the paper establishes a conceptual foundation that allows for an informed examination of the interaction between technological innovation, ethical leadership, and regulatory compliance.

In addition to the literature review, the methodology includes a doctrinal legal analysis of the European regulatory framework governing privacy in the digital economy. Particular attention is paid to Regulation (EU) 2016/679 (General Data Protection Regulation**)**, specifically regarding the processing of personal data and the rights of natural persons. These legislative instruments are examined in relation to their impact on AI-integrated organizational processes, with a focus on core legal concepts such as informed consent, pseudonymization, and the distinction between personal and non-personal data. The legal analysis is complemented by references to sectoral challenges, specifically in healthcare and marketing, enabling a critical assessment of the tension between hyper-personalization, medical innovation, and the fundamental right to confidentiality.

Building on the insights derived from both the literature review and the legal analysis, the paper adopts an interpretive approach aimed at evaluating how leadership styles, such as transformational and servant leadership, influence organizational adaptation and employee behaviour. The final part of the research analyses the transition from formal legal compliance to an authentic and sustainable organizational culture of accountability. Through this lens, the study explores how leadership acts as a central pillar in ensuring the trustworthy implementation of AI technologies by balancing innovation with ethical responsibility and strategic risk management.

4 Discussions

Over the last few decades, personal data protection has evolved to become a fundamental right within the European legal order, positioning Europe as a global leader in privacy and data protection. According to Hustinx (2014), this leadership

role has developed progressively, first within the Council of Europe, and then mainly within the structures of the European Union, leading to the distinct recognition of both the right to privacy and the right to personal data protection as independent fundamental rights in the Charter of Fundamental Rights of the European Union.

According to Mănescu (2021) several aspects related to the processing of data by national security institutions and law enforcement authorities are underscored. These institutions enjoy the benefits of the exceptions provided to the general principles of the GDPR, based on special legislation such as Directive no. 680/2016. However, as the author points out, "the exceptions we refer to are not unlimited freedom, but rather a temporary limiting and reasonable derogation from the general principles governing access to personal data." This observation is essential to understanding the balance that leaders must maintain between security and privacy.

From this viewpoint, organizations are challenged to strike a delicate balance between the economic value of data and respect for the rights of data subjects, between technological innovation and regulatory compliance, and between operational efficiency and cybersecurity. This balance cannot be achieved without strong leadership capable of integrating economic, legal, and ethical considerations into a coherent strategic vision. In the field of healthcare, AI is a key factor for innovation in ways that were previously unimaginable, and is now widely used in healthcare, diagnosis, and treatment. The evolution of robotics and Artificial Intelligence can offer countless opportunities in medical science, leading to significant reductions in the costs and time required to maintain patients' lives.

The use of such modern technologies could substantially improve medical diagnosis, surgery, disease prevention and treatment, as well as provide support for the rehabilitation and long-term care of people who are suffering or elderly to enable them to take care of themselves. For example, some studies have demonstrated that these intelligent applications have been able to diagnose more cancer patients than physicians, in a much more efficient manner (Khalid et al., 2023; Saeidnia et al., 2025). Robots have also been used to produce medicines in a considerably shorter time, especially during the COVID-19 pandemic, and voice assistants have been able to detect diseases such as depression and dementia through voice analysis (Kuroda et al., 2025; Gómez-Zaragozá et al., 2025, Cristache et al, 2025).

However, the most frequently used AI-based medical techniques were those that enabled remote patient monitoring (e.g., during the COVID-19 pandemic), the establishment of an electronic medical registry of patients that helped to update patient health status more quickly and efficiently, and smart devices that assisted surgeons in operations requiring precision. In addition, in recent years, researchers have been trying to develop smart prostheses controlled by neural impulses, which are stimulated by AI (Hussain et al., 2020).

While there are many advantages that could improve people's quality of life, all these smart systems can only be developed by using large amounts of personal data, which is analyzed and generates responses based on medical history and identification data. "They ensure the safeguarding of confidential patient

information from unauthorized access, exploitation, or revelation" (Mohammed et al., 2026). The analysis of this data can be performed both in the medium and long term, with each person becoming the subject of the research report. This data may include weight, age, social environment etc., but also the name or other direct identification data of the person. In general, names should not be included in such a research process, but should be anonymized when the data is transmitted to the researchers. Furthermore, regardless of whether the name is included in the final data register that is sent to the researchers, the patient's consent must be obtained for the collection and processing of data prior to any medical intervention, including general consultation. Therefore, data controllers need to be constantly vigilant and protect, detect, and resolve leaks or potential leaks of personal data that could infringe on patients' right to privacy. In a complementary sense, leaders are the ones who transform legal obligations of vigilance into a living organizational culture, ensuring that personal data protection is not just a technical process, but a fundamental ethical commitment to patient confidentiality (Cristache et al., 2025).

The collection and processing of personal data are becoming strategic elements for the development of the digital economy. Particular attention must be paid to respect for human rights when data controllers or smart devices (independently) collect information about medical history or identification data. In such a context, the standards adopted by European Union authorities must strike a balance between protecting fundamental freedoms enshrined in the Treaties and preserving privacy.

Personal data relating to health are defined in Article 35 of Regulation no. 679/2016 as a set of data revealing information about past, present, or future physical/mental health of a patient. In particular, this refers to information resulting from a test or "examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test". Technological development and the management of patients by a care team consisting of both human medical staff and automated means require a balance to be struck between the protection and exchange of personal data.

Consequently, in order to develop the most effective technologies for patient care and treatment, it is necessary to store data (most often personal, as symptoms and medical history are individualized for each research subject) and process it in a medical analysis to obtain the desired results. In order to ensure legal protection for both the doctor and the patient, the consent of the data subject is required for the processing of data.

In Romania, one of the main problems regarding the right to personal data confidentiality is the assimilation of the patient's informed consent with the consent regarding the processing of personal data in the General Data Protection

Regulation. The two are integral parts of the right to privacy, but also of data protection, and although there is a distinction between informed consent and consent to processing personal data, they work closely together. According to Costina & Corobană (2021, p. 912), health data must be processed "not only for the medical intervention, but also in order to establish the right diagnosis and to decide on the course of action that is to be performed, on the recommended medical intervention." In other words, consent to the processing of personal data is expressed primarily for each consultation, and not health analysis can be performed without it. Obtaining such consent must take into account information regarding the identity of the data controller, the purpose of each operation for which the patient has given consent, the possibility of withdrawing consent at any time, with some exceptions (both in relation to medical research studies and medical procedures to be performed), without encountering technical difficulties, and information about the use of patient data for automated decision-making, if applicable.

In this regard, due to the confusing use of certain procedures related to patient protection and trust in the medical system, people have developed a reluctance to use AI technologies in healthcare. Distrust in the protection of personal data privacy rights has contributed to the formation of several external and internal factors that lead to patients' strong rejection of AI-based medical care and diagnosis, namely: the ability to provide effective care, lack of empathy for people and their needs (the impression that they will always be faced with a screen where they will always be entering their symptoms in order to receive treatment), the perception that the AI system will not be able to give a degree of subjectivity to each symptom, which manifests itself uniquely for each individual, and including a distrust of medical professionals who have made mistakes in their diagnoses over time.

Leadership in healthcare plays a crucial role in protecting personal data, being responsible for creating and implementing effective cybersecurity strategies that prevent data breaches and maintain patient trust. According to Balogun (2025), leaders must allocate adequate resources, promote an organizational culture focused on risk awareness, and ensure ongoing employee training in information security. Leadership must develop clear data governance policies, monitor compliance with GDPR regulation, and manage risks through proactive assessments and ongoing audits.

In an era of GDPR, a strong healthcare strategy is characterized by compelling leadership that interacts as a multidimensional approach to data protection, with intelligent systems from advanced technologies, such as AI for threat detection, blockchain for secure exchanges, and continuous verification-based security. Such multidimensional approach is becoming increasingly relevant in the context of the unprecedented digital acceleration post-pandemic. The COVID-19 pandemic has forced organizations in all fields, including healthcare, to adopt digital solutions at a faster pace than would have been possible under normal circumstances. This accelerated transition has brought with it major challenges in

terms of data security, especially given that a large proportion of healthcare staff have had to work remotely or use personal devices to access patient information (Șișu et al., 2022).

Another important factor of this approach is to select the right technology stack for each specific organization. Data security is definitely one of them; there is no single answer. Each health facility, according to its needs and characteristics must assess what technologies to adopt. Such a decision obviously starts with the leaders, and they should know their own organization better than anyone else.

In this sense, McCoy (2025) suggests doing regular security audits and risk assessments to spot weaknesses, checking if things are following the rules, and making it easier for different departments to communicate. Șișu et al. (2022) complement this recommendation by emphasizing the ability to adapt to new digital solutions. The technical capability of the selected solutions, the willingness of employees to embrace new technologies, how much effort it will take everyone to run them, and their overall attitude toward all this effort are equally, if not more important workloads.

Workforce resistance to change is a common barrier to implementing new security technologies. Such resistance might have several causes: fear of change, the perception that new processes are bureaucratic and lengthy, or simply the comfort with previous means of functioning. Semyonov-Tal (2024) reinforces this reality in the medical context, demonstrating that doctors, while aware of the importance of confidentiality, often choose the quickest route to perform their medical procedures, even if this involves violating protocols.

A major aspect mentioned by Sandhu et al. (2026) is that leaders need to build an organizational culture where AI is not seen as an autonomous agent, but as a legal and ethical actor that requires constant monitoring, clear accountability principles, and protection of customers and patients trust.

Although the medical field provides a broad and conducive framework for analyzing leadership in data protection, due to the extreme sensitivity of health information and the relationship of trust between doctors and patients, the challenges identified are not specific to this sector exclusively. On the contrary, organizations in various fields face similar problems regarding the collection, processing, and security of personal data. A comparative analysis of cases from other sectors (e.g., the WhatsApp and Paytm case from 2025; the Air Canada case from 2024; or the Samsung – Shadow AI leaks case from 2023) reveals common patterns and offers valuable lessons about the cross-cutting nature of ethical leadership in data protection.

The faithful leaders with an ethical approach to the management of information security not only ensure lower susceptibility to data breaches but also promote risk reporting at all levels (Halim et al., 2023, Antohi et al, 2021). Governance teams proactively initiate compliance projects by directly involving business line stakeholders, which turns GDPR requirements from bureaucratic obligations into sustainable competitive advantages (Vojvodic & Hitz, 2019). As the principal countermeasure to governance failures, which may elicit harsh

sanctioning by supervisory authorities, leadership commitment toward a culture of accountability is more critical than ever.

5 Conclusions

Leadership plays a decisive role in integrating GDPR compliance. It does so not only as a legal obligation, but as a foundational element of organizational culture, thereby facilitating the transition from basic technical oversight to ethical information governance.

In this context, leadership represents the key link between legal requirements and their practical implementation within organizations. While regulatory frameworks such as the GDPR establish the formal obligations regarding the protection of personal data, it is the responsibility of leaders to translate these obligations into operational policies, internal procedures, and everyday organizational practices. Effective leaders ensure that compliance mechanisms are not treated as isolated legal constraints, but rather as integrated components of organizational governance that guide decision-making, risk management, and the responsible use of Artificial Intelligence systems.

The unpredictable and highly technical nature of AI contributes to mistrust regarding the purposes for which certain algorithms have been used and the need to collect and process such large volumes of data in the implementation of privacy policies and the enhancement of personal data protection. Therefore, leaders have an essential responsibility to build trust between patients, doctors, technology developers, and regulators. Ethical leadership involves integrity, transparency, and social responsibility. These are important qualities for transforming mistrust into trust and suspicion into collaboration.

Beyond regulatory considerations, leadership also plays a significant economic role in shaping how organizations leverage data and Artificial Intelligence as strategic resources. In the contemporary digital economy, data has become a critical asset that supports innovation, operational efficiency, and competitive advantage. However, the value generated by AI-driven technologies depends largely on the ability of leaders to manage these resources responsibly and strategically. By promoting a culture of accountability, investing in employee awareness, and encouraging responsible data management practices, leaders contribute not only to protecting personal information but also to strengthening organizational performance and long-term sustainability.

Ethical considerations must be a top priority in the development of AI systems. It is essential to recognize that AI technologies can impact people's right to privacy and raise issues regarding data confidentiality. Leaders need to internalize ethical principles in all phases of AI system development and implementation, from data collection to algorithm training to production deployment and ongoing monitoring. Leadership at this stage of digitalization extends beyond traditional skills, requiring a deep understanding of legal dynamics, emerging technological risks, and ethical imperatives.

In this regard, leadership must be understood not only as a managerial function, but also as a governance mechanism capable of integrating legal, technological, and ethical considerations into a coherent organizational strategy. Leaders who actively support accountability, transparency, and responsible data governance contribute to strengthening institutional resilience in the face of increasing digital risks. By fostering a culture in which legal compliance and ethical responsibility are embedded in everyday decision-making processes, leadership becomes a central pillar in ensuring sustainable and trustworthy implementation of Artificial Intelligence technologies.

The analysis presented in this paper reveals several concrete courses of action for leaders in the medical field and beyond, steerqing the implementation of responsible and effective practices in the protection of personal data in the context of the expanding use of AI. Leaders should integrate data protection into their organizational strategy as a central pillar of corporate governance. This implies that decisions regarding data collection, processing, and storage should be made with the direct involvement of boards of directors and executive teams, and that data protection should be considered as important as financial performance and operational efficiency. Interdisciplinary collaboration with experts in law and cybersecurity is becoming indispensable in an ever-changing technological and regulatory landscape.

References

1. Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. *Cogent Business & Management*, 11(1), Available at: https://doi.org/10.1080/23311975.2024.2393743 [Accessed 1 March 2026].
2. Antohi, V. M., Ionescu, R. V., Zlati, M. L., Mirica, C., & Cristache, N. (2022). Approaches to health efficiency across the European space through the Lens of the health budget effort. *International Journal of Environmental Research and Public Health,* 19(5), 3063.
3. Bădescu, M. (2023). *Drept constituțional și instituții politice, ediția a XV-a*, Bucharest: Hamangiu Publishing House.
4. Balogun, A. Y. (2025). Strengthening compliance with data privacy regulations in US healthcare cybersecurity. *Asian journal of research in computer science*, 18(1), 154-173.
5. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. *Science and engineering ethics*, 24(2), 505-528.
6. Costina, L., & Corobană, A. (2021). GDPR impact on the Romanian health clinics. In *Proceedings of the International Conference on Business Excellence*, 15(1), 908-916.
7. Cristache, N., Pricopoaia, O., Năstase, M., Șișu, J. A., Tîrnovanu, A. C., & Matiș, C. (2024). The metaverse, a new frontier for innovative business models. *Technological Forecasting and Social Change*, 209, 123838.

8. Cristache, N., Florea, N. V., Năstase, M., Croitoru, G., Fortea, C., & Tureatca, M. V. (2025). The influence of political, social and economic factors on the acceptance of technology in the workplace in the context of industrial revolution 4.0. *Amfiteatru Economic*, 27(68), 76-92.
9. Cristache, N., Croitoru, G., & Florea, N. V. (2025). The influence of knowledge management on innovation and organizational performance. *Journal of Innovation & Knowledge,* 10(5), 100793.
10. Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11-36.
11. Gómez-Zaragozá, L., Altozano, A., Llanes-Jurado, J., Minissi, M. E., Raya, M. A., & Marín-Morales, J. (2025). Detecting depression through speech and text from casual talks with fully automated virtual humans. *Artificial Intelligence in Medicine*, Available at: https://doi.org/10.1016/j.artmed.2025.103305 [Accessed 5 March 2026].
12. Guo, Y. X., & Zhang, X. (2025). The Impact Mechanism of Algorithmic Transparency on User Trust in Intelligent Recommendation Systems of Internet Platforms. *Journal of Computers*, *36*(3), 335-348.
13. Halim, Z., Durya, N. P. M. A., Kraugusteeliana, K., Suherlan, S., & Alfisyahrin, A. L. (2023). Ethics-based leadership in managing information security and data privacy. *Jurnal Minfo Polgan*, 12(2), 1819-1828.
14. Hervé, A. (2021). Data Protection and Artificial Intelligence: the European Union's Internal Approach and its possible Promotion through Trade Agreements. *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*, 193-197.
15. Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & communications technology law*, *28*(1), 65-98.
16. Hussain, J. S., Al-Khazzar, A., & Raheema, M. N. (2020). Recognition of new gestures using myo armband for myoelectric prosthetic applications. International Journal of Electrical & Computer Engineering (2088-8708), 10(6).
17. Hustinx, P. (2015). European leadership in privacy and data protection. In A. Rallo Lombarte & R. García Mahamut (Eds.), *Hacia un nuevo régimen europeo de protección de datos / Towards a new European data protection regime*. Tirant lo Blanch.
18. Karami, A., Shemshaki, M., & Ghazanfar, M. (2024). Exploring the ethical implications of AI-powered personalization in digital marketing. *Data Intelligence*, 3.
19. Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in biology and medicine*, *158*, Available at: https://doi.org/10.1016/j.compbiomed. 2023.106848 [Accessed 5 March 2026].
20. Kuroda, T., Ono, K., Onishi, M., Murakami, K., Shoji, D., Kosuge, S., Ishida, A., Hieda, S., Takahashi, M., Nakashima, H., Ito, Y., & Murakami, H. (2025). Utility of artificial intelligence-based conversation voice analysis for detecting cognitive decline. *PloS one*, 20(6), Available at: https://doi.org/10.1371/journal.pone.0325177 [Accessed 5 March 2026].
21. Musaigwa, M. (2023). The role of leadership in managing change. *International review of management and marketing*, 13(6), 1.

22. Mănescu, D. M. (2021). Personal Data between Individual Protection and the General Interest. *Resilience and Economic Intelligence Through Digitalization and Big Data Analytics*, 465.
23. McCoy, E. (2025). How Cybersecurity Leadership Became the New Critical Managerial Competency in Healthcare Administration. *Health Economics and Management Review*, 6(2), 50-59.
24. McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1), Available at: https://doi.org/10.1177/2053951716686994 [Accessed 1 March 2026].
25. Mohammed, U., Tijjani, M. M., & Salman, R. Data Privacy and Security Challenges In Electronic Health Records. *IJSART,* 12(01), 98-106.
26. Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 34(2), 222-233.
27. Năstase, M. (2010). Developing a strategic leadership approach within the organizations. *Revista de Management Comparat Internaţional*, 11(3), 454-460.
28. Niţă, G. (2021). Impactul inteligenţei artificiale în prelucrarea datelor cu caracter personal. *Revista română pentru protecţia şi securitatea datelor cu caracter personal*, (02), 12-20.
29. Popa, I.-C., Năstase, M., & Popa, R.-G. C. (2022). Strategic cybersecurity management. In *Proceedings of the 16th International Management Conference: Management and resilience strategies for a post-pandemic future* (pp. 557-564). Bucharest University of Economic Studies.
30. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40-81.
31. Saeidnia, H. R., Firuzpour, F., Kozak, M., & Majd, H. S. (2025). Advancing cancer diagnosis and treatment: integrating image analysis and AI algorithms for enhanced clinical practice. Artificial Intelligence Review, 58(4), 105.
32. Sandhu, D., Sra, M. K., & Kaur, N. (2026). Cybersecurity and data protection in the age of AI: Leadership at the crossroads of law and ethics. *International Journal of Law, Policy and Social Review*, 8(1), 108-115.
33. Semyonov-Tal, K. (2024). Keeping medical information safe and confidential: a qualitative study on perceptions of Israeli physicians. *Israel Journal of Health Policy Research*, 13(1), 54.
34. Șișu, J., Năstase, M., Tîrnovanu, A., Mujaya, J., & Ito, S. (2023). Resilience through digitalization in organizations. In *Management and resilience strategies for a post-pande mic future. 16th International Management Conference (3-4 November 2022. Bucharest, Romania).* Available at: https://doi. org/10.24818/IMC/2022/02.08 [Accessed 5 March 2026].
35. Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, 3(1), 33-69.
36. Udegbe, F. C., Ebulue, O. R., Ebulue, C. C., & Ekesiobi, C. S. (2024). AI's impact on personalized medicine: Tailoring treatments for improved health outcomes. *Engineering Science & Technology Journal*, 5(4), 1386-1394.
37. Vojvodic, M., & Hitz, C. (2019). Governance Team Leadership and Business User Participation-Organizational Practices for Innovative Customer Engagement in Data Compliance Project. *Central European Business Review*, 8(2), 15-45.