
# ENSURING THE RIGHT TO PRIVACY AND DATA PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE

**Gavharoy Qavulova**
**Student, Fergana State University,**
**Fergana, Uzbekistn**
**e-mail: alfargoniy.uz@gmail.com**
**https://doi.org/10.5281/zenodo.18859025**

**ARTICLE INFO**

Received: 26th February2026
Accepted: 27th February 2026
Online: 28th February 2026

**KEYWORDS**

*Artificial Intelligence, Privacy, Data Protection, GDPR, Ethical AI, Digital Literacy, Personal Data Security*

**ABSTRACT**

*The rapid advancement of artificial intelligence (AI) has revolutionized the collection, storage, and analysis of personal data across multiple sectors, including healthcare, finance, and public administration. While AI provides numerous benefits, it also poses significant risks to individual privacy and data security. AI systems often rely on large datasets containing sensitive personal information, which can be susceptible to unauthorized access, misuse, or breaches. Ensuring the right to privacy in the AI era requires a comprehensive approach combining robust legal frameworks, technological safeguards, and ethical guidelines. Legal instruments such as the European Union's General Data Protection Regulation (GDPR) establish principles of transparency, accountability, and informed consent that are critical for protecting personal data. Technological measures, including encryption, anonymization, and privacy-enhancing technologies, further mitigate potential risks..*

The rapid development and widespread adoption of artificial intelligence (AI) technologies have significantly reshaped the ways in which personal data is collected, stored, processed, and analyzed. AI systems are increasingly integrated into everyday applications, ranging from healthcare and financial services to public administration and social media platforms. These technologies enable organizations to derive insights from vast amounts of data, improve decision-making processes, and offer personalized services. However, alongside these benefits, the expansion of AI also brings serious challenges and risks related to the protection of individual privacy and data security. AI algorithms frequently depend on extensive datasets that contain sensitive personal information, such as medical records, financial transactions, and behavioral patterns, making them potentially vulnerable to misuse, unauthorized access, or accidental breaches (Zuboff, 2019).

In this context, safeguarding the right to privacy requires a multi-layered approach that combines strong legal frameworks, advanced technological solutions, and clear ethical standards. Legal instruments such as the European Union's General Data Protection Regulation (GDPR) provide a foundation for protecting personal data by enforcing principles

like transparency, accountability, and informed consent (Voigt & Von dem Bussche, 2017). Technological safeguards, including data encryption, anonymization, and privacy-enhancing technologies, can reduce the risks associated with large-scale AI-driven data processing (Ohm, 2010). Furthermore, ethical guidelines for AI development emphasize the importance of minimizing data collection, preventing discriminatory outcomes, and ensuring that individuals maintain meaningful control over their personal information (Floridi et al., 2018).

In addition, public awareness and digital literacy play a critical role in empowering individuals to understand how their data is used and to exercise their rights effectively. Organizations and policymakers must work together to create transparent, accountable, and secure systems that balance innovation with fundamental human rights. By integrating legal, technological, and ethical measures, it becomes possible to ensure that AI development advances society without compromising the privacy and security of individuals' personal data (Wachter et al., 2017).

Legislation such as the European Union's General Data Protection Regulation (GDPR) has established a foundation for protecting personal data by enforcing principles of transparency, accountability, and informed consent (Voigt & Von dem Bussche, 2017). Additionally, privacy-enhancing technologies (PETs), including data anonymization, encryption, and secure multi-party computation, offer practical solutions to mitigate risks posed by AI-driven data processing (Ohm, 2010). Organizations must implement these measures alongside comprehensive privacy policies to ensure compliance and protect individuals' rights.

Moreover, fostering public awareness about data privacy and digital literacy is essential to empower individuals to control how their information is used. Ethical AI development should prioritize user consent, minimize data collection, and prevent discriminatory outcomes (Floridi et al., 2018). International cooperation is also crucial, as AI systems often operate across borders, necessitating harmonized standards for privacy protection (Wachter et al., 2017). In conclusion, safeguarding the right to privacy and data protection in the era of AI requires a multi-faceted approach that integrates legal, technological, and ethical strategies to ensure that technological advancement does not compromise fundamental human rights.

## References:

1.Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.
2.Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.
3.Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57(6), 1701–1777.
4.Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28, 689–707.
5.Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.