

Artificial Intelligence and Personal Data

25 May 2023

Does General Data Protection Regulation Protection Personal Data Against Artificial Intelligence?

Artificial Intelligence ("AI") has revolutionized the way personal data is analyzed, predicted, and used to influence human behavior, making it a valuable asset. AI has an ability to automate decision-making processes in complex situations without affecting the emotions and resulting in more accurate and impartial decisions than those made by humans. Algorithmic decisions, however, may still contain errors or bias, leading to negative impacts on individuals under constant surveillance and evaluation. Nonetheless, the increasing use of AI and its contribution to the economy is an undeniable reality. Accordingly, governments are investing in AI and implementing policies to encourage its use. Concerns about AI use have been primarily centered on potential violations of fundamental rights and freedoms resulting from the use of personal data.

Personal data protection and privacy issues in terms of AI uses are closely scrutinized by data protection authorities. Especially with the release of the revised version advanced chatbot known as ChatGPT, discussions about AI and personal data have become more frequent. Thus, Italy showed reaction against to usage of the ChatGPT and became the first country to block the ChatGPT for the children under the age of 13 through Italian Data Protection Authority's ("Garante") decision. Before ChatGPT, there were decisions made by the authorities for different AI based softwares like Clearview AI. For the Clearview, the United Kingdom's Data Protection Authority ("ICO") launched an investigation and imposed an administrative fine in amount of £7,552,800 for collecting images from online sources to establish a global facial recognition database. In addition to ICO, Garante and Greek data protection authorities imposed administrative fines and banned Clearview AI from processing biometric data in the EU. In the same vein, the decision made by the French Data Authority is also available.

In this article, we will focus on personal data and privacy issues within the framework of artificial intelligence regulations, especially in Turkey and Europe Union ("EU").

What is AI? What are the differences between Machine Learning and Deep Learning?

AI refers to the ability of computer systems to imitate human cognitive abilities, such as learning, reasoning, and self-correction. Thanks to AI, computers are now capable of carrying out tasks that once required human intelligence, such as speech recognition, natural language processing, computer vision, machine learning, and robotics. The potential applications for AI are limitless, ranging from improving healthcare and increasing efficiency in manufacturing and logistics to providing more personalized and efficient services. AI achieves these feats by utilizing advanced algorithms, machine learning, and neural networks that enable computers to learn from data, recognize patterns, and make predictions or decisions based on that data. The two primary subfields of AI are machine learning ("ML") and deep learning ("DL"), both of which involve training algorithms to make predictions or decisions based on data. ML algorithms learn patterns in data without being explicitly programmed, while DL is a more complex subfield involving the training of deep neural networks with multiple layers. The primary differences between ML and DL are the complexity and scale of the models that can be learned. While ML algorithms are generally simpler and require less computing power than deep learning algorithms, they may not be as effective at handling complex tasks.

In order to ensure accurate results, AI requires data that is accurate, up-to-date, and complete, and the quantity and quality of data play a crucial role in AI's effectiveness. the feeding of data from various sources and the increase in the amount of data, however, can lead to unpredictable outcomes for individuals. Furthermore, incomplete, or

incorrect data can result in unwanted consequences for individuals as well. Consequently, data protection regulations have become a growing concern in AI development. Compliance with data protection regulations is a significant issue for both the agenda and administrative authorities.

AI Regulations in the World

Governments worldwide have been developing AI-related legislation and regulations to promote AI's development and deployment while addressing its risks and challenges. Many countries have all developed comprehensive AI strategies that include funding for AI research and development, developing industry standards, and promoting usage of AI in all areas, especially in the public domain. Some of the countries that make regulations in the field of AI and where Turkey closely follows its developments and directs its own strategies are given in the table below.

Country	Significant Steps Towards to AI Legislation
Canada	The Pan-Canadian Artificial Intelligence Strategy was declared by the Canadian government, comprising of funding for AI research and development, the cultivation of AI expertise, and the formation of standards and legal structures for AI.
China	China set a goal in 2017 to establish itself as a global leader in the field of artificial intelligence by 2030. Since then, China has formulated a comprehensive strategy for AI that involves investing in research and development, creating industry standards, and promoting the use of AI in government and commercial sectors.
Japanese	The Japanese government introduced the Society 5.0 initiative with the objective of fostering the growth of AI and other emerging technologies to establish a society that is more centered on human needs.
South Korea	South Korea announced a plan in 2020 to invest \$1 billion in AI research and development with a specific focus on healthcare, smart cities, and other related applications by 2025.
United States	The United States has not yet enacted comprehensive federal legislation on AI, but several bills related to AI have been introduced in the United States Congress. In addition, several states have passed laws regulating the use of AI in government and commercial applications (see, Algorithmic Accountability Act, National AI Initiative Act, Automated Decision-Making Accountability Act, Consumer Privacy Act, Fair Credit Reporting Act).

AI Legislation in European Union

EU has been at the forefront of developing regulations and guidelines and conducting studies for AI in recent years. ~~The timeline showing the developments in the EU is given below. Although the AI Law, which was proposed to the~~ European Commission ("**Commission**") as a draft a long time ago, caused some controversy because it is not aligned with the General Data Protection Regulation ("**GDPR**"), which regulates personal data and privacy issues, it was approved by the Commission on 11 May 2023.



Conflict with AI Act and GDPR

Commission proposed the AI Act in April 2021, which is a regulation aimed at establishing a unified legal framework for the development and deployment of AI in the EU. The main focus of the act is to ensure the ethical and

responsible use of AI technology. The proposed regulation applies to all AI systems that are developed, deployed, or used in the EU, regardless of where the user or developer is located. It covers AI systems that interact with natural persons, such as chatbots and personal assistants, as well as those used in critical infrastructure. GDPR was drafted at a time when the technology of AI was not yet at today's level of advancement. Therefore, concerns have arisen regarding the compatibility of the GDPR, which was designed to be in line with the existing technology, and the AI Act, which is brought in for the increasingly growing and developing AI. While the GDPR is a comprehensive data protection law that covers all types of data processing activities in the EU, including those involving AI systems. Therefore, both laws are complementary and will apply to AI systems in the EU.

High-Risk AI Systems: The AI Act defines high-risk AI systems and requires developers to conduct risk assessments, implement safety measures, and provide documentation to users. Certain uses of AI that threaten fundamental rights are prohibited. These requirements impact GDPR compliance for high-risk AI systems that process personal data. A rigorous assessment for transparency, traceability, and human oversight is required before deploying high-risk AI applications. However, there are uncertainties within the scope of GDPR regarding the limitations stipulated by the AI Act on high-risk AI usage and their implementation. It is unclear how the features introduced by the AI Act can be applied within the GDPR framework. For instance:

- Article 12 of the AI Act regulates high-risk AI systems has to be designed and developed with enabling the automatic recording of events ('logs'); however, this may result in personal data storage without fulfilment of obligation to inform as per GDPR. Additionally, compliance rules in Article 61 of AI Act for post-market monitoring may cause to violate of GDPR's data minimization and transfer mechanisms, leading to concerns about obtaining consent and exercising the right to erasure.^{[1] [2]}
- The AI Act sets different requirements for public and private entities, especially regarding the processing of real-time biometric data and social scoring, which is different from the GDPR's approach. The GDPR applies to all data controllers, whether they are public or private, who process personal data, without making any distinction between them.
- Data controllers must take technical and organizational measures to protect data subject rights and implement data protection principles, such as data minimization. Nonetheless, AI Act's Article 10 stipulates high-quality, representative, error-free, and complete training datasets for high-risk AI systems. By its nature, AI needs to work with as complete and accurate datasets as possible in order to produce the most accurate results possible. The uncertainty of how to apply both of these articles simultaneously is unclear. The AI Act should consider privacy-enhancing techniques that adhere to GDPR's protection by default requirement.^[3]

Monitoring: In order to ensure the responsible use of AI, the AI Act requires developers and operators of AI systems to establish monitoring mechanisms to detect and prevent instances of high-risk AI behavior. These mechanisms should be proportionate to the risks posed by the AI system and should consider the potential impact on fundamental rights and the public interest. However, the monitoring of AI behavior may have implications for personal data protection and privacy under the GDPR. Given that AI systems often process large amounts of personal data, monitoring their behavior may involve collecting and analyzing additional data, which could pose risks to data protection and privacy if the monitoring mechanisms are not appropriately designed and implemented.

While the GDPR addresses the use of AI systems for tracking and processing data, it only applies to individual forms of profiling, leaving a gap in coverage for AI-driven manipulation that could collectively impact segments of society. The GDPR tends to be interpreted as individualistic regarding tracking systems, unlikely AI Act. The AI Act does not cover this gap, but a possible solution could be introducing a broader ban on certain techniques that allow for such manipulation.

The AI Act's requirements for transparency and explainability may also conflict with the GDPR's provisions on the right to erasure and the right to object. AI systems may be designed to process large amounts of personal data, making it difficult to ensure transparency and explainability while respecting individual rights.

Although, the AI Act and the GDPR are complementary laws that will both apply to AI systems in the EU. the AI Act's requirements for high-risk AI systems and transparency will have implications for GDPR compliance, particularly in cases where personal data is processed by AI systems. However, the exact impact of the AI Act on GDPR

compliance will depend on the specific provisions of the regulation and how they are implemented in practice. The above-mentioned regulations under the AI Act have been evaluated in comparison to the obligations set forth by GDPR. The primary focus of fulfilling these obligations should be on "data governance and management." In AI systems where personal data of the data subject can be linked with other individuals' data or processed for different purposes, the data generated by AI can reveal information about the data subject that they did not share or wish to share. This is especially likely to occur in AI systems that use ML or DP methods. Since it is not possible to make hypothetical notifications for unforeseen data by the system developer, and the data generated by the AI system cannot be entirely predicted by a data controller, the fulfillment of the obligation to inform, which requires clear and explicit data processing conditions, may not be in line with GDPR. In addition, as explained above, AI is a system that creates new results by analyzing existing data, producing correlations on the data rather than establishing logical cause-effect relationships. Therefore, the results generated by AI may not always be accurate. This situation may result in a breach of many obligations under GDPR, such as compliance with general principles (in particular data minimization), data processing conditions.

There is also a lack of clarity on how GDPR and AI Act provisions will be enforced in practice, particularly in cases where AI systems process personal data. This may lead to confusion and uncertainty for businesses and organizations trying to comply with both regulations. In order to prevent any potential non-compliance with GDPR provisions arising from the use of AI, it is imperative to adopt an appropriate data governance and management model. Within this framework, it is crucial to ensure that the personal data of data subjects is not commingled with data belonging to others, and that other data sets created for different purposes are not used in conjunction with such data.

Despite the publication of guidelines and opinions by the EU Data Protection Authority, it is necessary to clarify GDPR regulations on a legal basis, taking into account current developments in AI. The scope of GDPR and related regulations, such as the AI Act, are subject to considerable interpretation. This may lead to the prevention of the use of AI systems utilizing personal data or the breach of privacy. Therefore, it is expected that secondary regulations should be enacted, or necessary amendments should be made to GDPR to ensure compliance with the AI Act. Furthermore, it is essential to review the provisions of the AI Act that are incompatible with GDPR.

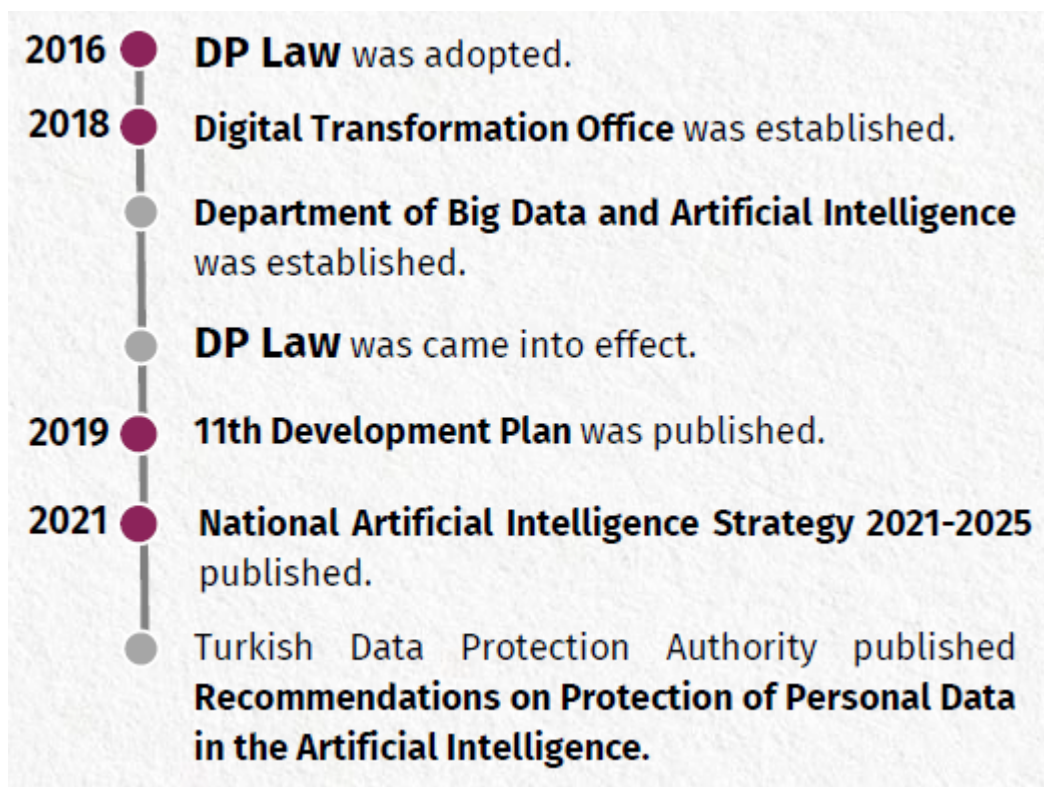
AI Regulation in Turkey and Data Protection

Although Turkey is a pioneer in technology and has developed artificial intelligence and similar chatbots, Turkey does not have a specific law or regulation dedicated solely to AI, but it has taken some steps to regulate AI in certain sectors. One of the most significant developments in this area is the adoption of the Turkish Personal Data Protection Law ("**DP Law**") in 2016, which regulates the processing of personal data in Turkey, including data processed by AI systems. Within the scope of DP Law, Turkish Data Protection Authority published [Recommendations on Protection of Personal Data in the Artificial Intelligence](#) in 2021. It includes some recommendations for using AI in data protection, including making privacy impact assessments where high-risk AI uses, taking specific measures for special categories of personal data, and determining data controller and data processor. In addition to the DP Law, there are sector-specific regulations that address AI-related issues. For example, the Turkish Ministry of Health has issued guidelines for the use of AI in healthcare, which include requirements for data protection, transparency, and informed consent.

In addition, the Digital Transformation Office of the Presidency of the Republic of Turkey ("**Digital Transformation Office**") was established as part of the Presidential Decree No. 1, which was published on 10 July 2018 in the Official Gazette numbered 30474. The Digital Transformation Office has several departments that focus on various technological developments and projects, including the Department of Big Data and Artificial Intelligence. This department aims to promote the implementation of AI and big data in Turkey, as well as to support the development of related policies and regulations. With Presidential Decree No. 2021/18, published in the Official Gazette dated 20 August 2021, and numbered 31574, [the National Artificial Intelligence Strategy 2021-2025](#) was published with the contribution of The Digital Transformation Office. National Artificial Intelligence Strategy 2021-2025 highlights important issues such as developing a robust AI ecosystem, enhancing human capital, supporting the development

and adoption of AI technologies, ensuring ethical and responsible use of AI, and creating a supportive legal and regulatory framework. Additionally, the strategy emphasizes the significance of data privacy, security, and ethics in AI applications.

11th Development Plan of the Presidency of the Republic of Turkey for the years 2019 to 2023 ("**11th Development Plan**") was published on 18 July 2019. In order to encourage the development of applications and services, such as artificial intelligence, advanced data analytics, simulation and optimization, product lifecycle, and production management systems that can be offered on industrial cloud platforms, the 11th Development Plan has laid out a framework for technology suppliers. Additionally, as part of the National Technology Initiative, development roadmaps have been established for artificial intelligence and big data technologies. These roadmaps aim to establish the necessary infrastructure and develop qualified human resources for AI's uses.



Overall,

It is possible that the Turkish legislator may take inspiration from the AI Act and use it as a model for future AI-related regulations in Türkiye. However, it remains to be seen how the AI Act will impact the DP Law specifically, like as GDPR. The Turkish legislator may need to make amendments to the DP Law or issue additional regulations to ensure that AI-related activities are compliant with both the DP Law and any future AI-related regulations that may be introduced in the EU. As per 11th Development Plan explains that the DP Law is expected to be updated based on the GDPR. Since several provisions of the DP Law have been expecting to be amended according with the GDPR; the issues mentioned under EU Section above regarding GDPR will also be noteworthy for Turkey in the same way.

References:

- Bogucki, A., Engler, A., Perarnaud, C., & Renda, A. (2022). The AI Act and Emerging EU Digital Acquis, Overlaps, Gaps and Inconsistencies (CEPS-IAI-EUI Report No. 49). Centre for European Policy Studies. Retrieved from https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-IAI-EUI_AI-Act-EU-Digital-Acquis-2022.pdf

- European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0205&from=EN>
- European Parliament. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. Retrieved from [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- Future of Privacy Forum. (2021, April 20). *GDPR and the AI Act interplay: Lessons from FPF's ADM case-law report*. Retrieved from <https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/>
- Presidency of the Republic of Turkey. (2021). *National Artificial Intelligence Strategy 2021-2025*. Retrieved from <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAIStrategy2021-2025.pdf>
- Republic of Turkey, Ministry of Development. (2019). *The Eleventh Development Plan (2019-2023)*. Retrieved from https://www.sbb.gov.tr/wp-content/uploads/2022/07/Eleventh_Development_Plan_2019-2023.pdf
- Turkish Personal Data Protection Authority. (2016). *Turkish Data Protection Law*. Retrieved from <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>
- Turkish Personal Data Protection Authority. (2022). *Recommendations on Protection of Personal Data in the Artificial Intelligence*. Retrieved from <https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler>

[1] Bogucki, A., Engler, A., Perarnaud, C., & Renda, A. (2022). The AI Act and Emerging EU Digital Acquis, Overlaps, Gaps and Inconsistencies. *Centre for European Policy Studies*.7

[2] Bogucki, Engler, Perarnaud, Renda (2022), p.9.

[3] Bogucki, Engler, Perarnaud, Renda (2022), p.9.

Related Attorneys

- [DR. E. SEYFİ MOROĞLU, LL.M.](#)
- [BURCU TUZCU ERŞİN, LL.M.](#)
- [CEYLAN NECİPOĞLU, Ph.D, LL.M.](#)