

WRITTEN BY



KRISTÍNA MASCHKANOVÁ  
Attorney  
Čechová & Partners

ČECHOVÁ & PARTNERS  
advokáti a právniky

# PRIVACY IN THE AGE OF AI

The rapid development of artificial intelligence (AI) technologies presents both opportunities and significant challenges, particularly in the area of privacy and personal data protection. As AI systems become more integrated into everyday life, the potential for privacy breaches increases, raising several legal questions.

This article examines the challenges related to AI and privacy, focusing on the existing privacy legislation in Slovakia and providing an outlook on the forthcoming EU legislation.

## THE IMPACT OF AI ON PRIVACY

AI technologies, ranging from machine learning algorithms to predictive analytics, offer remarkable benefits, including improved efficiency, innovation and decision-making processes. However, these advances come at a cost, particularly in terms of the potential breach of personal privacy. AI technologies, by their very nature, thrive on data and often rely on large amounts of data, including personal information, to function effectively. This reliance on data makes information a valuable asset for the development of AI, leading to potential privacy and data security breaches, in particular unauthorized access and misuse of personal information. Today, it is more than necessary to focus on the measures needed to ensure the privacy of individuals in the context of the current legal framework and the development of AI technologies.

For instance, facial recognition technologies can track individuals without consent, and predictive analytics can reveal sensitive information and inadvertently violate personal privacy. Furthermore, the opaque nature of some AI algorithms, often referred to as 'black boxes', makes

it difficult to understand how personal data is being used or the extent to which it influences the output of these systems. This lack of transparency not only hinders users' understanding of how their data is being processed, but also complicates regulatory efforts to protect privacy.

Another important concern is 'group privacy'. AI's ability to analyze and identify patterns in large data sets can lead to stereotyping of certain groups, potentially leading to discrimination and bias. This presents a complex challenge, as the issues at stake go beyond individual privacy.

## EXISTING PRIVACY AND DATA PROTECTION LEGAL FRAMEWORK

Slovakia, like other EU member states, currently adheres to the General Data Protection Regulation (GDPR), which provides a framework for the protection of personal data. The GDPR imposes strict requirements on data processing, in particular ensuring that personal data is processed lawfully, fairly and transparently. Additionally, it grants individuals the right to rectify their data and to have personal data deleted and no longer processed if it is no longer necessary for the purposes for which it was collected or otherwise processed.

Although the GDPR includes some terms related to information technology, it does not include 'artificial intelligence' or terms expressing related concepts such as intelligent systems,

autonomous systems, machine learning or even big data. This reflects the fact that the GDPR focuses on challenges that were present at the time the GDPR was drafted, rather than on emerging issues related to AI.



**It is more than necessary to focus on the measures needed to ensure the privacy of individuals in the context of the current legal framework and the development of AI technologies.**

The GDPR generally prohibits the use of data for purposes other than those for which it was originally collected. Article 5 requires data to be "collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes" and "adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed".

The GDPR also restricts the use of personal data to make automated decisions about individuals. Article 22 provides for the right of the data subject not to be subject to a decision which is based solely on automated processing, including profiling. In addition, Articles 13-15 require that individuals be provided with meaningful information about the process used in automated decisions. This means that companies using AI systems must be able to explain how the AI system makes decisions that have a significant impact on individuals. The information provided should be sufficiently comprehensive to enable the individual to understand the reasons for the decision. In practice, this is currently a significant constraint for companies developing AI systems.

In addition to the protection of personal data, privacy will also play an important role in the use of AI systems. The latter is currently regulated in the Civil Code, according to which every natural person has the right to the protection of his or her personality, in particular life and health, civil honor and human dignity, as well as privacy, his or her name and expressions of a personal nature.

## THE FORTHCOMING EU LEGISLATION - AI ACT

The EU is in the process of introducing the AI Act, a pioneering piece of legislation aimed specifically at governing AI systems, addressing privacy and data protection challenges by setting clear

requirements for their development, deployment, and use. The AI Act should ensure that AI systems are safe, transparent, traceable, non-discriminatory and environmentally friendly. Key provisions are expected to include transparency obligations, ensuring that individuals are aware when they are interacting with AI and can understand how their data is being processed. The draft AI Act categorizes AI systems by risk level and bans those posing unacceptable risks, such as those manipulating humans or vulnerable groups.

The draft is under review in the European Parliament, with a full plenary vote expected in April 2024. Additionally, the Council of Europe is working on a Convention on AI to establish a legal framework for AI systems.

## CONCLUSION

To effectively address the privacy challenges posed by AI, a multifaceted legal approach is necessary. This should include not only specific legislation, such as the AI Act, but also the ongoing adaptation of existing laws. In particular, this includes increasing the transparency of AI systems, strengthening consent mechanisms, facilitating data minimization, ensuring accountability for compliance with data protection laws, including the implementation of effective data protection measures and remediation of data breaches, and promoting the ethical use of AI.