DENTONS

AI & GDPR MONTHLY UPDATE

Special edition: AI implementation

January 2025

Grow | Protect | **Operate** | Finance

Starting February 2, 2025, the first obligations under the AI Act will take effect—namely, the ban on prohibited practices and obligations related to AI literacy. This special issue is designed to prepare you for the steps necessary to implement the AI Act, should you plan to deploy artificial intelligence tools. You can read more about the AI Act in one of our previous newsletters. Read more (in CZ).

Preparing for the first obligations coming into effect on February 2, 2025

1. Employee training and AI literacy

To ensure sufficient level of AI literacy, it will likely be necessary to provide **training for employees and all potential AI users across your company**, or another form of user education on the functionality and risks of artificial intelligence. The aim should be to ensure, to the greatest extent possible, a sufficient level of AI literacy among potential users.

2. Assessment of prohibited practices

The AI Act outlines a list of prohibited practices that will be explicitly banned starting February 2, 2025. To **evaluate potential prohibited AI practices**, it is advisable to assess whether your use of AI could fall under any of these defined prohibitions. These include, for instance, AI systems that use subliminal techniques, exploit human vulnerabilities, or enable biometric categorization to infer sensitive attributes such as race or other sensitive criteria.

Implementation of AI Act obligations

1. AI team

Depending on the size of your organization, it is advisable to start with appointing a dedicated team responsible for artificial intelligence across your company. This team should have expertise in AI and should be integrated with other relevant departments, such as Risk and Compliance, DPO, IT and Security, Legal, and Business teams managing AI use cases, as well as Management, depending on your organizational structure.

2. Mapping: Catalogue of AI systems and identification of use cases

As a next step, it is essential to map the systems, applications and tools you use, including whether you currently integrate or plan to implement AI systems. This mapping should consider both new AI tools but also existing tools or applications, particularly those licensed from third parties. This process will help you create a catalog of your AI systems. Concurrently, it is advisable to define and map use cases—i.e., scenarios detailing how AI is used currently or will be used. This step not only helps in selecting the appropriate solutions (since different AI systems/models are suited for different purposes) but is also a critical part of regulatory compliance.

3. Gap analysis: AI assessment, legal risks and GDPR data processing evaluation

In the next step, evaluate whether your system meets the AI Act's definition of an AI system and whether its intended uses fall into a high-risk category under the AI Act. Simultaneously, assess whether personal data is being processed—for example, whether users can upload personal or confidential data into the AI system (e.g., via prompts) or whether you use customized systems that enable fine-tuning of your data. Additional legal risks, such as intellectual property issues or sector-specific regulations, should also be considered.

4. GDPR compliance

If using AI involves processing personal data, it is crucial to implement numerous steps to ensure GDPR compliance. In particular, consider conducting a DPIA (Data Protection Impact Assessment), assessing the compatibility of data processing purposes and data subject legitimate expectations, ensuring an adequate level of security and meeting contractual obligations with the system provider (if not developed internally), as well as implementing measures to ensure transparency and processes to exercise the rights of subjects.

5. Implementation, additional measures and documentation

In the final phase of the project, the focus shifts to implementing the steps required by legal regulations. During this phase, it will be particularly appropriate to implement a wide range of measures, including those ensuring compliance with the AI Act, GDPR, and measures to mitigate the risks of infringing third-party intellectual property rights. This phase will also include the implementation of the necessary documentation.

From a documentation perspective, this will primarily involve a risk management system, an internal policy on the use of artificial intelligence, records of completed security audits, technical and contractual documentation of the AI system provider, as well as privacy notices and measures to ensure AI transparency.

6. AI Governance, monitoring and updates

As is often the case with similar projects, in the case of AI implementation, it will also be necessary to regularly review and update the adopted measures and documentation as needed, particularly in light of the ongoing evaluation of these measures and documentation, as well as the development of technology and legislation.

For more information, please don't hesitate to contact our TMT team!

Klíčové kontakty

Zdeněk Kučera
Partner, Praha
D +420 236 082 283
Email

Štěpánka Havlíková
Seniorní advokátka, Praha
D +420 236 082 264
Email

Jiří Maršál
Advokátní koncipient, Praha
D +420 236 082 454
Email

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you. **www.dentons.com**