BRANDI
RECHTSANWÄLTE

DATA PROTECTION AT DEEPSEEK

Information on data protection I May 2025

Introduction

The AI tool DeepSeek has caused quite a stir and made headlines in recent months. When the Chinese provider of the tool unveiled its latest AI model in January 2025, the question of whether China had achieved a breakthrough in the field of artificial intelligence led to a drop in the price of technology shares of American companies. DeepSeek has since been seen as a competitor to ChatGPT, the product of the leading American provider OpenAI. Shortly afterwards, the media reported on a data leak at DeepSeek, as a result of which a large number of data records were said to have been accessible on the internet without being secured.

Many companies are currently faced with the question of whether and how they can use DeepSeek in a data protection-compliant manner. This article contains an overview of the key legal requirements and a data protection classification of the various framework conditions of DeepSeek, which ultimately results in an assessment of the data protection-compliant usability of DeepSeek.

Possible uses of DeepSeek

The "DeepSeek R1" model is an AI-based chatbot with which users can converse and which is based on a large language model. DeepSeek can be used in a variety of ways. For example, users can chat with the AI, upload files or use it for web searches. The tool is provided by Hangzhou DeepSeek Artificial Intelligence Co., Ltd. in China. As part of the wide range of possible uses, the user submits a query to the tool by entering data into the system. The tool processes this data and generates an answer to the question posed. The use of the tool therefore goes hand in hand with the processing of various data.

General legal requirements for the use of AI tools

The use of AI is associated with opportunities, including the development of new products and services, innovation and easier access to information as well as the analysis of large amounts of data in a short period of time. However, there are risks associated with its use, for example with regard to privacy, freedom of expression and data protection, automated decisions that are influenced by the wrong factors, imprecise and incorrect results, manipulation and a lack of transparency. In order to properly exploit the benefits of AI while minimizing the risks, a strong legal framework and a close examination of the legal requirements for the specific use of AI are therefore needed.

The AI Regulation (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13.06.2024 laying down harmonized rules on artificial intelligence) establishes comprehensive rules for AI, which are intended to ensure compliance with fundamental rights and at the same time promote innovation. The regulation came into force on August 1, 2024; the first provisions have been applicable since February 2, 2025. The AI Regulation follows a risk-based approach: AI practices that pose an unacceptable risk under the Regulation will be banned. At the next level of high-risk systems, comprehensive specific requirements apply, for example regarding the quality and accuracy of the data used, cybersecurity, technical documentation and risk management. Transparency obligations apply to AI systems with limited risk, while the establishment of and compliance with voluntary codes of conduct is recommended for AI systems with low risk. AI models with a general purpose are subject in particular to information and documentation obligations.

Insofar as personal data is processed when using AI, the provisions of data protection law must also be observed, in particular the General Data Protection Regulation (GDPR). A legal basis for the processing of personal data is therefore also required in the context of AI use. The purposes of data processing must be defined in advance. The other general requirements also apply, for example with regard to data security, information obligations and data minimization. Automated decision-making, which has a wide range of applications in the field of AI, is subject to the restrictions set out in Art. 22 GDPR.

Data protection assessment of the framework conditions for DeepSeek

In order to evaluate the use of DeepSeek in terms of data protection law, its framework conditions must be taken into account, in particular the terms of use, the privacy policy and the DeepSeek Open Platform Terms of Service.

Data processing by DeepSeek and purposes of data processing

According to DeepSeek's privacy policy, all user data, such as prompts, uploaded documents, chat histories and other content, are processed by DeepSeek for various purposes. These may also contain personal data. The purposes of data processing are only described by DeepSeek in very general terms. The purposes of data processing include analyzing the use of DeepSeek and training the AI. However, according to the provider's terms of use, the user can object to the use of the data for training the AI.

DeepSeek thus uses the information entered not only for the purpose of responding to the user's specific request, but also for its

own purposes, which are in any case not specifically recognizable to the user in advance. This will generally be problematic when entering personal data with regard to the requirement of purpose limitation pursuant to Art. 5 (1) (b) GDPR, namely if the purposes of the processing of personal data can neither be specifically determined in advance nor the users can be informed accordingly about the purposes of the data processing and the data is processed by DeepSeek for purposes other than the original purposes.

Data processing in third countries
The data is stored on servers in China. In this respect, DeepSeek's privacy policy points out that the provider may be obliged under Chinese law to transmit data to the secret service and security authorities.
The Chinese security authorities' access options are generally considered to be very far-reaching. Although DeepSeek makes general reference to only transferring data to China from certain countries in compliance with the applicable data protection law, it does not mention any specific measures that are implemented for this purpose. In view of this, it is doubtful that the data transfer to DeepSeek in China complies with the principles of Art. 44 et seq. GDPR and an adequate level of data protection can be ensured.

Appointment of a representative in the EU
Pursuant to Art. 27 (1) GDPR, any controller or processor offering goods or services to data subjects in the EU but not established in the EU must appoint a representative within the EU. The representative shall be appointed by the controller or processor to act as a contact point in addition to or in place of the controller or processor, in particular for supervisory authorities and data subjects in all matters relating to data processing.
It is not clear from the publicly available information whether DeepSeek has appointed a representative in the EU. Since a representative in the EU is not named in DeepSeek's general terms and conditions, the existence of such a representative can be doubted in any case. A number of German state data protection authorities have initiated coordinated investigation proceedings against the provider in this regard. The proceedings began on February 14, 2025 and initially serve to clarify the question of whether the provider of DeepSeek has appointed a representative in the European Union. The data protection supervisory authorities of Rhineland-Palatinate, Baden-Württemberg, Thuringia, Saxony-Anhalt, Hesse, Bremen and Berlin are involved.

Transparency of data processing
In view of the general description of the purposes of data processing, the unclear protective measures with regard to data transfer to China and the lack of a contact point for questions about data processing in the EU, there is a general lack of transparency in the processing of personal data by DeepSeek. This leads to ambiguities and legal uncertainties when using the tool.

Summary of the deficits in the framework conditions of DeepSeek
In particular, there are deficits due to the processing of personal data for DeepSeek's own purposes, the transfer of data to China and the lack of transparency and enforcement options for data subjects' rights.

Opinions and investigations by data protection supervisory authorities

In view of the data protection issues, various data protection supervisory authorities have now also commented on DeepSeek and initiated investigations.

The State Commissioner for Data Protection (LfD) of Lower Saxony assumes that, according to the current state of knowledge, the requirements of the AI Regulation and the GDPR in particular are not being complied with when using DeepSeek. There are legal concerns with regard to the processing of personal data and data that is subject to special confidentiality protection due to trade and business secrets. The LfD Lower Saxony justifies this, among other things, with the provider's registered office outside the EU and the lack of a representative in the EU, which makes it difficult or even impossible to exercise the rights of data subjects. Data breaches and misuse of data are in fact very difficult to prevent and punish. Overall, the LfD Lower Saxony recommends avoiding the installation of DeepSeek and other AI systems originating from insecure third countries and their configuration files in any IT environment connected to the internet in order to limit the risk of data leaks or misuse.
DeepSeek is also the focus of regulatory authorities outside Germany. The Polish Data Protection Authority (UODO) advises caution when using DeepSeek. On February 6, 2025, the Greek Data Protection Authority (HDPA) announced an investigation into DeepSeek. The Luxembourg supervisory authority makes recommendations for the use of DeepSeek and draws attention to risks.
The Italian data protection authority also sees a data protection risk in the use of DeepSeek and has therefore submitted a request to DeepSeek (see the authority's press release dated 28.01.2025). The authority requested information about which personal data is collected from which sources and for which purposes, what the legal basis for the processing is and whether the data is stored on servers in China. The request also related to what information is used to train the AI and how registered and unregistered users are informed about the data processing.
On January 1, 2025, the Italian authority demanded that the provider of DeepSeek restrict the processing of Italian users' data (see the authority's press release dated 30.01.2025). According to the authority, the order was issued in response to the notification received from the provider, the content of which was deemed inadequate. The provider had stated that it did not operate in Italy and that European legislation was therefore not applicable to it. The authority has initiated an investigation.

Conclusion

The use of DeepSeek is associated with various risks from a data protection perspective. This is primarily due to the transfer of data to China, the processing of data by DeepSeek for its own purposes and the lack of transparency.
It is therefore recommended at this time not to use the tool with personal data or other confidential information unless data transmission to the provider cannot be ruled out. As DeepSeek is currently the subject of investigations by various supervisory authorities, further developments remain to be seen.

In general, before introducing and using an AI model, it must be ensured that no data worthy of protection can flow out. This can be achieved, for example, by creating a separate, secure IT environment. In a closed, local system, the use of a company's own data for AI training and other purposes of the provider can also be avoided in principle. Companies should make their employees aware of the risks associated with the use of DeepSeek and other AI tools and provide information on data processing. In cases of doubt, the data protection officer should be consulted.

Johanna Schmale

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Lawyer

T +49 521 96535 - 883
F +49 521 96535 - 113
E johanna.schmale@brandi.net