BRANDI
RECHTSANWÄLTE

USE OF CHATBOTS BASED ON AI SYSTEMS

Information on data protection I September 2024

Introduction

The integration and use of AI systems in everyday working life and the provision of in-house AI applications, especially chatbots, is becoming increasingly important for companies. This includes translation tools or applications such as ChatGPT, which can be used to answer questions or generate texts. If personal data is processed as part of the use of the respective application, the data protection requirements of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) as well as the provisions of the new AI Regulation must be complied with in addition to other legal requirements. The new AI Regulation was published in the Official Journal of the EU on July 12, 2024 and entered into force on August 1, 2024. Most of the provisions of the new legal act will apply from August 2, 2026. However, various provisions must already be observed from February 2, 2025 or August 2, 2025.

The term "AI system" is legally defined in Art. 3 No. 1 of the AI Regulation. Accordingly, AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Own use of chatbots

If personal data is to be entered into a chatbot or another AI tool and processed by it, a legal basis is required for the data processing procedures that take place. In this respect, the data protection principle of prohibition with reservation of permission anchored in Art. 6 GDPR applies.

In order to justify the data processing procedures, the consent of the data subject pursuant to Art. 6 (1) (1) (a) GDPR comes into consideration, which, however, must meet various requirements in order to be effective. Difficulties may arise in this respect with regard to the characteristic "informed", as the transparent information of the data subjects may well pose challenges for the company that wishes to enter the data into the tool and is therefore obliged to provide information. This is sometimes due to the fact that in many cases it may not be easy for the company to compile the necessary information, given the complexity of the tools and the reluctance of the tool providers to disclose the specific data processing procedures and mechanisms of the application.

If, as part of the required balancing of interests, a company comes to the conclusion that its own interests in the use of the AI tool outweigh the interests, fundamental rights and freedoms of the data subject, the legitimate interest of the company pursuant to Art. 6 (1) (1) (f) GDPR may also be considered as a legal basis in individual cases. However, it is important to note that a decision must always be made on a case-by-case basis and that an overriding interest must not be assumed prematurely due to the risks associated with data processing. If the data processing procedures relate to employee data, a works agreement can also be considered.

Some providers of AI applications also offer the conclusion of a data processing agreement. If the provider of the chatbot acts as a processor for the responsible company and the data processing is secured by a corresponding agreement within the meaning of Art. 28 GDPR, Art. 6 (1) (1) (f) GDPR in conjunction with Art. 28 GDPR also applies in this respect as the legal basis. However, if the data subject has not given their consent and there is no other legal basis, the input of personal data into the chatbot must be ruled out for lack of a legal basis. In this case, however, it is conceivable to enter anonymized data in the tool, provided that it can be guaranteed that no conclusions can actually be drawn about a natural person.

In addition, the data subjects must be informed about the data processing in accordance with Art. 13 GDPR. In this respect, there are similar difficulties as with regard to informing consent.

In order to ensure the proper handling of chatbots within the company, it is advisable to create a policy on the proper handling of AI tools. This can regulate the following aspects, for example:

- Which applications may be used?
- What information may be entered in the applications?
- For what purposes may the applications be used?
- Are results generated by AI applications to be labeled separately?
- How and by whom are the generated results checked?
- How is the increased risk potential countered?
- How are the processes documented?

Offer of a chatbot

If a company itself offers a chatbot that answers questions about the company's products or contact persons, for example, care must

be taken to ensure that the tool is only trained with personal data if there is a legal basis for this. The same applies to the output of work results that contain personal data.

In addition to any information obligations under data protection law, there are also transparency obligations under the AI Regulation. According to Art. 50 of the AI Regulation, users of the tool must be informed in particular of the fact that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. In addition, providers of AI systems may have to comply with various monitoring, documentation and reporting obligations.

Decisions made by AI systems

If the tool used or offered is not exclusively a chatbot, but decisions are also made by the tool – for example about the conclusion of a contract – further transparency obligations and requirements that the AI Regulation places on high-risk AI systems must also be observed. These must be determined in more detail on a case-by-case basis.

From a data protection perspective, the provision of Art. 22 GDPR and the existing requirements for automated individual decisions must also be observed. In addition, it may be necessary to carry out a data protection impact assessment in accordance with Art. 35 GDPR.

Conclusion

When using chatbots based on AI systems and other AI applications, the general data protection requirements of the GDPR and the BDSG as well as the requirements of the new AI Regulation must be observed. This primarily concerns the principle of prohibition with reservation of permission and the resulting requirement of a legal basis for any processing of personal data in connection with the use of the AI application, as well as the various information and transparency obligations. The same applies if corresponding tools are offered to customers and interested parties for use via the company's homepage, for example. In addition to the legal obligation to disclose the use of AI tools, it is also advisable to disclose the use of AI in order to avoid accusations of misleading or non-transparency. Which obligations arise in detail depends on the functional scope of the respective tool and must be determined on a case-by-case basis. In order to ensure the proper handling of AI applications in the company, it is advisable to create an AI guideline within which various aspects can be regulated in a binding manner. We would be happy to support you with the concrete design.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net