

INFORMATION NOTE ON CHATBOTS (EXAMPLE OF CHATGPT)

An information note regarding chatbots (e.g., ChatGPT) was published by the Personal Data Protection Authority on November 8, 2024.

This information note, issued by the Personal Data Protection Authority, provides an overview of chatbots, explaining their purpose, the types of personal data they process, and how artificial intelligence chatbot applications can be evaluated from the perspective of personal data security. It also addresses the key considerations to be taken into account during their development.

You can access the full text of the information note published by the Personal Data Protection Authority via the link provided below:

Link to the Document: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/967c7518-2a4c-4318-9c97-01dcac2591f3.pdf>

In the Information Note prepared by Koyuncuoğlu Köksal Law Firm, we present a brief summary of the Authority's work along with our evaluations and insights.

1. Definition of Chatbots

Chatbots are software programs designed to mimic human conversation, operating through an interface to execute commands given by users and provide instant responses. These bots process and analyze user inputs to perform tasks, thereby enabling quick and efficient access to information or solutions. Chatbots can interact with users through either voice or text-based communication and gain functionality by interpreting commands using natural language processing (NLP) techniques.

What sets chatbots apart, particularly advanced ones, is their ability to engage in a continuous learning and development process by leveraging information obtained from previous interactions with users. This capability enhances their adaptability and effectiveness over time.

2. Advantages and Applications of AI-Powered Chatbots

AI-powered chatbots not only understand user commands but also analyze context, intent, and emotional state to deliver a personalized experience. These artificial intelligence capabilities enable chatbots to be utilized across a wide range of fields, from customer support and information retrieval to programming code generation and content creation. Examples of such chatbots include ChatGPT, Siri, Alexa, and Gemini.

The primary application areas of AI-powered chatbots include:

- **Customer Support Services:** They provide quick solutions by answering frequently asked questions.
- **Question Answering:** They allow users to access information rapidly and efficiently.
- **Code Writing and Programming:** They offer support in programming languages tailored to users' needs.
- **Information Retrieval and Content Creation:** They assist users by enabling fast access to information and generating content.
- **Translation and Sentiment Analysis:** They perform translations across different languages and analyze emotional states.

3. Personal Data Processing and Data Security in Chatbots

AI-powered chatbots require extensive data processing to enhance user experience and improve performance. This data encompasses all interactions users have with the chatbot and is processed for various purposes. The types of data processed may vary depending on the purpose of the application but generally include the following:

- **Account Information:** Usernames, contact details, account credentials, and transaction history.
- **User Inputs:** Message content provided to the chatbot, file uploads, and feedback.
- **Device Information:** User IP addresses, browser types, device details, and access timestamps.
- **Other Content Data:** Additional data such as cookies and social media information.

This data is processed to provide users with a better experience, ensure security, and comply with legal requirements.

4. Risks to Data Security in Chatbots and Necessary Precautions

Ensuring data security in AI-powered chatbot applications is of critical importance. Failure to do so may compromise user privacy. In this context, the primary security risks and the precautions that should be taken are as follows:

- **Transparency and Information Disclosure:** Users must be adequately informed about what data the chatbot processes, the purposes for which this data is used, and with whom it is shared.
- **Ensuring Data Security:** Technical and administrative measures must be implemented to ensure the secure processing of personal data. In particular, necessary cybersecurity precautions should be taken to prevent data breaches.
- **User Awareness:** Users should avoid sharing excessive information and understand the data processing limitations of the chatbot. This awareness can act as a safeguard against cyberattacks.
- **Special Protection for Child Users:** Additional security measures, such as age verification, should be applied for child users. Proactive protection in data processing activities involving children is essential to ensure their safety.

5. Principles to Follow During the Development of Chatbots

The development of AI-powered chatbots must comply with the Personal Data Protection Law (Law No. 6698) and international data security standards. To ensure that these applications are designed in a way that protects user privacy and security, the following fundamental principles should be considered:

- **Risk Assessment:** Risk analyses regarding personal data security should be conducted before initiating data processing activities.
- **Compliance with Legal Regulations:** All data processing activities must be carried out in accordance with applicable legal frameworks.
- **Transparency and Accountability:** The application should provide transparent information to users, enabling them to maintain control over their personal data.
- **Technical and Administrative Security Measures:** Technical and administrative measures must be implemented to ensure data security and prevent data breaches.
- **Protection of Child Users:** Necessary measures, such as age verification, should be taken to ensure the safety of child users. A proactive approach should be adopted to prevent negative experiences for children.

Chatbots should be designed in a transparent and secure manner, adhering to international certifications. Secure methods of data communication must be prioritized throughout the development process.

6. Evaluation

Our institution's information note clearly emphasizes the necessity of adopting an approach that complies with the Personal Data Protection Law (KVKK) and international standards during the development and use of AI-powered chatbots. Transparency and awareness are particularly significant from the perspective of users. It is expected that users are informed from the outset and made aware of potential risks and consequences. In this regard, the following measures are essential:

- Providing a clear and comprehensible privacy notice.
- Regularly reviewing and updating security measures.
- Raising user awareness to prevent excessive data sharing.
- Ensuring special protection for children.
- Taking swift action in the event of a data breach.
- Adopting international best practices for data security and privacy.

We present this information for your attention.

Sincerely,

Koyuncuoğlu & Köksal Law Firm

The explanations provided in our study are based on the current legislation of the Republic of Turkey and the public announcements made by the relevant official authorities. In cases of uncertainty, we recommend seeking our opinion and support before taking any final actions. Otherwise, our Law Firm cannot be held responsible for any actions taken or the consequences thereof based on the explanations provided herein.