

## **SOHBET ROBOTLARI (CHATGPT ÖRNEĞİ) HAKKINDA BİLGİ NOTU**

Kişisel Verileri Koruma Kurumu tarafından 8 Kasım 2024 tarihinde sohbet robotları (chatgpt örneği) hakkında bilgi notu yayımlanmıştır.

Kişisel Verileri Koruma Kurumu'nun yayınladığı bu bilgi notu, sohbet robotunu tanımlarken sohbet robotunun ne işe yaradığı, hangi kişisel verileri işlediği ve kişisel veri güvenliği açısından yapay zekâ sohbet robotu uygulamalarının nasıl değerlendirilebileceği ve geliştirilirken nelere dikkat edileceği konularını ele almıştır.

Kişisel Verileri Koruma Kurumu'nun bilgi notunun tamamına aşağıda paylaştığımız linkten ulaşabilirsiniz.

Bağlantı Linki: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/967c7518-2a4c-4318-9c97-01dcac2591f3.pdf>

Koyuncuoğlu Köksal Avukatlık Bürosu olarak hazırladığımız Bilgi Notumuzda ise, Kurumun çalışması hakkında kısa, özet bilgiler ve değerlendirmelerimiz sunulmaktadır.

### **1. Sohbet Robotu (Chatbot) Tanımı**

Sohbet robotları, bir arayüz ile kullanıcıların kendisine verdiği komutları yerine getirmek ve anında yanıt vermek amacıyla tasarlanan, insan konuşmasını taklit eden yazılımlardır. Bu robotlar, kullanıcı girdilerini anlamlandırıp analiz ederek bir işlem yapar, böylece hızlı ve verimli bir bilgi edinme veya çözüm sunma imkânı sağlar. Sohbet robotları, sesli ya da yazılı iletişim seçenekleriyle kullanıcıya hitap edebilir ve doğal dil işleme (NLP) teknikleri sayesinde kullanıcı tarafından verilen komutları anlamlandırarak işlevsellik kazanır. Özellikle, kullanıcılarla önceki etkileşimlerinden elde ettikleri bilgi ile süreklilik arz eden öğrenme ve gelişme sürecine sahip olmaları, onları diğer sohbet robotlarından ayırmaktadır.

### **2. Yapay Zekâ Destekli Sohbet Robotlarının Avantajları ve Kullanım Alanları**

Yapay zekâ destekli sohbet robotları, yalnızca kullanıcı komutlarını anlamakla kalmaz, aynı zamanda bağlam, niyet ve duygusal durumu analiz ederek kişiselleştirilmiş bir deneyim sunar. Bu yapay zekâ özellikleri, robotların müşteri desteğinden bilgi aramaya, programlama kodu yazmaya ve içerik oluşturmaya kadar çok çeşitli alanlarda kullanılabilmesini sağlar. ChatGPT, Siri, Alexa ve Gemini gibi örnekler...

Yapay zekâ destekli sohbet robotlarının başlıca kullanım alanları:

- Müşteri destek hizmetleri: Sıkça sorulan soruları yanıtlayarak hızlı çözümler sunar.
- Soru cevaplama: Kullanıcıların bilgiye hızla ulaşmasını sağlar.
- Kod yazma ve programlama: Kullanıcıların ihtiyaçlarına göre programlama dili desteği sağlar.
- Bilgi arama ve içerik oluşturma: Hızlı bilgi edinme ve içerik üretme işlevleriyle kullanıcıyı destekler.
- Çeviri ve duygu analizi: Farklı dillerde çeviri yapar ve duygu durumunu analiz eder.

### **3. Sohbet Robotlarında Kişisel Veri İşleme Süreci ve Veri Güvenliği**

Yapay zekâ sohbet robotları, kullanıcı deneyimini iyileştirmek ve performansını artırmak için geniş kapsamlı veri işleme süreçlerine ihtiyaç duyar. Bu veriler, kullanıcının sohbet robotuyla gerçekleştirdiği tüm etkileşimleri içerir ve çeşitli amaçlarla işlenir. İşlenen veri türleri, uygulamanın amacına göre değişiklik göstermekle birlikte genelde aşağıdakileri kapsar:

- Hesap bilgileri: Kullanıcı adı, iletişim bilgileri, hesap kimlik bilgileri ve işlem geçmişi.
- Kullanıcı girdileri: Sohbet robotuna sağlanan mesaj içerikleri, dosya yüklemeleri, geri bildirimler.
- Cihaz bilgileri: Kullanıcının IP adresi, tarayıcı türü, cihaz bilgileri ve erişim zamanları.
- Diğer içerik verileri: Çerezler, sosyal medya bilgileri gibi diğer veriler.

Bu veriler, kullanıcılara daha iyi bir deneyim sunmak, güvenlik sağlamak ve yasal gereklilikleri yerine getirmek amacıyla işlenir.

#### **4. Sohbet Robotlarında Veri Güvenliğinin Riskleri ve Alınması Gereken Önlemler**

Yapay zekâ sohbet robotları uygulamalarında veri güvenliğinin sağlanması yüksek önem arz eder. Aksi takdirde, kullanıcıların gizliliği risk altına girebilir.

Bu bağlamda, güvenlik riskleri ve alınması gereken önlemler şunlardır:

- Şeffaflık ve Bilgilendirme: Sohbet robotlarının hangi verileri işlediği, bu verilerin ne amaçla kullanıldığı ve kimlerle paylaşıldığı hakkında kullanıcıların yeterli bilgiye sahip olması gerekir.
- Veri Güvenliği Sağlama: Kişisel verilerin güvenli bir şekilde işlenmesi için teknik ve idari tedbirler alınmalıdır. Özellikle siber güvenlik açısından gerekli önlemler sağlanarak veri ihlallerinin önüne geçilmelidir.
- Kullanıcı Farkındalığı: Kullanıcılar aşırı bilgi paylaşımından kaçınmalı ve sohbet robotunun veri işleme sınırlarını anlamalıdır. Bu farkındalık, siber saldırılara karşı bir güvenlik önlemi işlevi görebilir.
- Çocuk Kullanıcılar İçin Özel Koruma: Çocuk kullanıcıların yaş doğrulama gibi ek güvenlik önlemlerine tabi tutulması gerekmektedir. Çocuklara yönelik veri işleme süreçlerinde proaktif koruma sağlanması önemlidir.

#### **5. Sohbet Robotu Geliştirme Sürecinde Uyulması Gereken İlkeler**

Yapay zekâ sohbet robotlarının geliştirilmesinde KVKK (6698 sayılı Kişisel Verilerin Korunması Kanunu) ve uluslararası veri güvenliği standartlarına uygun hareket edilmelidir. Bu uygulamaların, kullanıcı mahremiyetini ve güvenliğini sağlayacak şekilde tasarlanması için göz önünde bulundurulması gereken temel ilkeler şunlardır:

- Risk Değerlendirmesi: Veri işleme süreçlerinin başlamasından önce kişisel veri güvenliği açısından risk analizleri yapılmalıdır.
- Yasal Mevzuata Uygunluk: Tüm veri işleme süreçleri yasal mevzuatlarla uyumlu olarak gerçekleştirilmelidir.
- Şeffaflık ve Hesap Verebilirlik: Uygulama, kullanıcıların kişisel veriler üzerindeki kontrolünü koruyabilmesi için şeffaf bir şekilde bilgilendirme yapmalıdır.
- Teknik ve İdari Güvenlik Önlemleri: Verilerin güvenliğini sağlamak için teknik ve idari önlemler alınmalı, veri ihlallerinin önüne geçilmelidir.
- Çocuk Kullanıcıların Korunması: Özellikle çocuk kullanıcıların güvenliği için yaş doğrulama gibi gerekli önlemler alınmalı, olumsuz deneyimlerin önlenmesi için proaktif bir yaklaşım benimsenmelidir.

Sohbet robotları, uluslararası sertifikalara uygun, şeffaf ve güvenli bir şekilde tasarlanmalı; veri iletişimde güvenli yöntemler tercih edilmelidir.

## 6. Değerlendirme

Kurumumuzun bilgi notu, yapay zekâ sohbet robotlarının geliştirilmesi ve kullanılması sürecinde, KVKK ve uluslararası standartlara uygun bir yaklaşım benimsenmesi gerektiğini net bir şekilde vurgulamaktadır. Özellikle şeffaflık ve farkındalık, kullanıcılar nezdinde önemlidir. Kullanıcıları baştan aydınlatmış ve olası risk ve sonuçlar hakkında farkındalık yaratmış olmak beklenmektedir. Bu doğrultuda;

- Açık ve anlaşılır bir aydınlatma metni sunulması.
- Güvenlik önlemlerinin düzenli olarak gözden geçirilmesi.
- Kullanıcıların aşırı paylaşım yapmaması için bilinçlendirilmesi.
- Çocukların özel olarak korunması.
- Veri ihlali durumunda hızlı aksiyon alınması.
- Veri güvenliği ve mahremiyet açısından uluslararası en iyi uygulamaların benimsenmesi önemli olacaktır.

Bilgilerinize sunarız.

Saygılarımızla,

***Koyuncuoğlu & Köksal Avukatlık Bürosu***

\*Çalışmamızda yer verilen açıklamalar, Türkiye Cumhuriyeti'nin yürürlükte olan mevzuatı ve ilgili resmi mercilerin kamuya yaptığı bilgilendirmeler esas alınarak hazırlanmış olup, tereddütlü hususlarda nihai işlemler gerçekleştirilmeden evvel tarafımızdan görüş ve destek alınmasını tavsiye ederiz. Aksi takdirde, burada yer verilen açıklamalar temel alınarak yapılacak işlemler ve bunların sonuçlarıyla ilgili olarak Avukatlık Büromuz sorumlu tutulamaz.