

İş Yerlerinde Üretken Yapay Zeka Araçlarının Kullanımı: KVKK Kapsamında Dikkat Edilmesi Gereken Hukuki ve Teknik Hususlar

Giriş

Üretken Yapay Zeka ("ÜYZ") araçları günümüzde çalışanların e-posta hazırlama, metin düzenleme, özet çıkarma, araştırma yapma ve içerik oluşturma gibi pek çok iş sürecinde sıklıkla kullandığı araçlardan biri haline gelmiştir. İş hayatında verimliliği artırması ve iş süreçlerini hızlandırması nedeniyle yaygınlaşan ÜYZ araçları, aynı zamanda kişisel verilerin korunması, bilgi güvenliği, ticari sırların korunması ve yurt dışına veri aktarımı bakımından da önemli hukuki ve teknik riskleri beraberinde getirmektedir.

Kişisel Verileri Koruma Kurumu ("Kurum") tarafından Kasım 2025 tarihinde yayımlanan "Üretken Yapay Zeka ve Kişisel Verilerin Korunması Rehberi" ve Mart 2026 tarihinde yayımlanan "İş Yerlerinde Üretken Yapay Zeka Araçlarının Kullanımı" dokümanlarında, ChatGPT, Claude, Gemini gibi kamuya açık üretken yapay zeka sistemlerinin iş süreçlerinde kullanımı ile ilgili dikkat edilmesi gereken hususlar ortaya konulmuştur. Kurum'un yaklaşımı, üretken yapay zeka araçlarının kullanımının kategorik olarak yasaklanmasından ziyade, kullanım senaryolarına bağlı risklerin belirlenmesi ve uygun hukuki, idari ve teknik tedbirlerle yönetilmesi yönündedir.

1. ÜYZ Araçlarının Kullanımı Tek Başına KVKK'ya Aykırı Değildir

Öncelikle belirtmek gerekir ki, iş yerinde ChatGPT, Claude, Gemini gibi üretken yapay zeka araçlarının kullanılması tek başına 6698 sayılı Kişisel Verilerin Korunması Kanunu'na ("KVKK") aykırılık teşkil etmemektedir.

Ancak hukuki değerlendirmenin, yalnızca ÜYZ araçlarının kullanılmasına değil;



göre yapılması önem arz etmektedir.

2. En Önemli Risk: ÜYZ Araçlarına Kişisel Veri Girilmesi

Günlük iş akışında çalışanlar çoğu zaman işlerini hızlandırmak amacıyla çeşitli belgeleri doğrudan ÜYZ araçlarına yükleyebilmekte veya metinleri olduğu gibi sisteme yapıştırabilmektedir. Örneğin şirketlerde insan kaynakları departmanı tarafından aday özgeçmişleri ChatGPT vasıtasıyla değerlendirilebilmekte, hukuk departmanı tarafından sözleşme taslaklarının incelenmesinde Claude kullanılabilmektedir. Bu kapsamda kişilerin kimlik bilgileri, sağlık bilgileri ve finansal verileri gibi kişisel verilerin ÜYZ araçlarına yüklenmesi konusu gündeme gelmektedir. Bu bilgilerin ÜYZ araçlarına aktarılması KVKK kapsamında kişisel veri işlenmesi sonucunu doğurabilecek ve somut olaya göre çeşitli hukuki yükümlülükleri gündeme getirebilecektir.

3. Yurt Dışına Veri Aktarımı Boyutu Dikkatle Değerlendirilmelidir

ChatGPT, Claude, Gemini gibi ÜYZ araçlarının bulut tabanlı bir hizmet olmaları nedeniyle sisteme girilen bilgilerin yurt dışındaki altyapılarda işlenmesi konusu gündeme gelmektedir. Bu nedenle çalışanlar tarafından ÜYZ araçlarına kişisel veri içeren içerikler yüklenmesi halinde KVKK'nın 9. maddesi kapsamında yurt dışına kişisel veri aktarımına ilişkin hükümlerin değerlendirilmesi gerekmektedir. Bu kapsamda şirketlerin genel olarak ÜYZ kullanım senaryolarını değerlendirmesi, hangi verilerin sisteme girilebileceğini politikalarla belirlemesi ve çalışanlara sunması, gerekli aktarım mekanizmalarının mevcut olup olmadığını incelemesi ve veri işleme süreçlerini hukuki açıdan analiz etmesi önem taşımaktadır.

Uygulamada en çok gözden kaçan risklerden biri, ÜYZ araçlarının kullanımının aynı zamanda bir yurt dışına veri aktarımı niteliği taşımasıdır.

4. Risk Sadece Kişisel Verilerle Sınırlı Değildir

ÜYZ araçlarına aktarılan içerikler her zaman kişisel veri niteliğinde olmayabilir. Bu kapsamda ticari sırlar, sözleşme taslakları, fiyatlandırma çalışmaları, şirket stratejileri, müşteri listeleri, finansal planlamalar ve şirket içi yazışmalar gibi bilgilerin ÜYZ araçları ile paylaşılması, yalnızca KVKK bakımından değil, ticari sırların korunması, bilgi güvenliği, fikri mülkiyet hakları ve çalışanın sadakat yükümlülüğü açısından da çeşitli hukuki sonuçlar doğurabilecektir. Ayrıca konunun iş hukuku bakımından da bizzat ifa ve iş görenin özen borcu kapsamında da değerlendirme gerektirdiği kuşkusuzdur.

Dolayısıyla ÜYZ kullanımına ilişkin değerlendirme yalnızca kişisel verilerin korunması perspektifiyle sınırlı tutulmamalıdır.

5. "Gölge Yapay Zeka" (Shadow AI) Riski

Kurum'un Mart 2026 tarihli dokümanında özellikle dikkat çekilen konulardan biri de "Gölge Yapay Zeka (Shadow AI)" kavramıdır. Bu kavram, çalışanların kurumun bilgisi veya onayı olmaksızın ChatGPT, Gemini, Claude gibi yapay zeka araçlarını iş süreçlerinde kullanmasını ifade etmektedir.

Bu nedenle Kurum, yasaklayıcı bir yaklaşım yerine kontrollü kullanım ve etkin yönetim anlayışını önermektedir. Başka bir ifadeyle, amaç çalışanların ÜYZ araçlarını kullanımını tamamen engellemek değil hangi araçların, hangi amaçlarla ve hangi veri kategorileriyle kullanılabileceğini açık kurallarla belirleyerek bu kullanımın güvenli ve denetlenebilir şekilde gerçekleştirilmesini sağlamaktır.

6. Bilgi Güvenliği Açısından ÜYZ Araçlarının Kullanımında Dikkat Edilmesi Gereken Riskler

- 1 **Bu durum aşağıdaki riskleri beraberinde getirebilmektedir:**
 - Çalışanların hangi yapay zeka araçlarını hangi amaçlarla kullandığı kurum tarafından takip edilemeyebileceğinden, kurumsal denetim ve yönetim mekanizmalarının etkinliği zayıflayabilmektedir.
- 2
 - ChatGPT gibi araçlara hangi kişisel verilerin veya şirket bilgilerinin aktarıldığının tespit edilememesi, veri işleme faaliyetlerinin kontrolünü güçleştirebilmekte ve veri güvenliği risklerini artırabilmektedir.
- 3
 - Olası bir veri ihlali veya yetkisiz veri paylaşımı gerçekleşmesi hâlinde, olayın kaynağının, kapsamının ve etkilenen verilerin tespit edilmesi zorlaşabilmekte, bu durum ihlal yönetim süreçlerini olumsuz etkileyebilmektedir.
- 4
 - Kurum tarafından belirlenen bilgi güvenliği politikaları, erişim kontrolleri ve yapay zekâ kullanımına ilişkin kurumsal kuralların çalışanlar tarafından denetim dışı araçlarla aşılması, hem KVKK kapsamındaki yükümlülüklerin yerine getirilmesini hem de şirketin bilgi güvenliği yönetimini zora sokabilmektedir.

Hukuki risklerin yanında, ÜYZ araçlarının kullanımının çeşitli bilgi güvenliği riskleri de bulunmaktadır. Özellikle hizmet sağlayıcısı nezdinde yaşanabilecek veri ihlalleri, hesapların kimlik avı saldırıları sonucunda ele geçirilmesi, resmi olmayan veya sahte ChatGPT uygulamalarının kullanılması, çalışanların kişisel hesapları üzerinden kurumsal bilgileri paylaşması, sisteme yüklenen bilgilerin kontrolsüz şekilde üçüncü taraflarla paylaşılabilmesi şirketler açısından önemli güvenlik riskleri oluşturmaktadır.

Bu nedenle ÜYZ araçlarının kullanımının yalnızca hukuki değil, aynı zamanda siber güvenlik perspektifiyle de değerlendirilmesi, kullanılmasına izin verilen araçların ve hesap türlerinin belirlenmesi, erişim yetkilerinin sınırlandırılması ve uygun teknik kontrollerin uygulanması gerekmektedir.

7. Çıktıların Kullanımı

ChatGPT ve diğer üretken yapay zeka kullanımında dikkate alınması gereken riskler yalnızca sisteme girilen verilerle sınırlı değildir. Bu sistemler gerçeğe aykırı, eksik, güncelliğini yitirmiş veya bağlamından kopuk çıktılar üretebilmekte, kimi zaman belirli önyargıları çıktılara yansıtabilmektedir.

Bu risk özellikle işe alım, çalışan performansının değerlendirilmesi, terfi, ücretlendirme, disiplin süreçleri veya iş sözleşmesinin sona erdirilmesi gibi kişiler üzerinde önemli sonuçlar doğurabilecek süreçlerde daha kritik hale gelmektedir. Yapay zeka çıktılarının bu tür kararlarda kullanılması halinde, çıktıların yetkin kişiler tarafından doğrulanması ve nihai kararın yalnızca yapay zeka tarafından üretilen sonuca dayandırılmaması önem taşımaktadır.

Bu çerçevede şirketlerin, üretken yapay zeka tarafından oluşturulan çıktıların doğruluğunun ve uygunluğunun insan gözetimi altında kontrol edilmesini sağlayacak mekanizmalar oluşturması ve özellikle kişiler hakkında hukuki veya benzeri önemli sonuçlar doğuran karar süreçlerinde KVKK kapsamında ilgili kişilerin haklarını ayrıca gözetmesi gerekmektedir.

8. Şirketler Hangi Önlemleri Almalıdır?

Kurum'un rehberleri ve sektördeki iyi uygulamalar birlikte değerlendirildiğinde şirketler tarafından asgari düzeyde aşağıdaki tedbirlerin hayata geçirilmesi önerilmektedir:

1.	ÜYZ araçlarının kullanımına ilişkin yazılı bir kurumsal politika oluşturulması.
2.	Çalışanlara ÜYZ araçlarına hangi bilgilerin girilemeyeceğinin açık şekilde bildirilmesi.
3.	Kişisel verilerin, ticari sırların ve gizli şirket bilgilerinin sisteme yüklenmesinin yasaklanması.
4.	Çalışanlara düzenli farkındalık eğitimleri verilmesi.
5.	ÜYZ araçlarının kullanımının yurt dışına veri aktarımı bakımından değerlendirilmesi.
6.	Erişim kontrolleri, log kayıtları ve veri kaybını önleme (DLP) çözümleri gibi teknik tedbirlerin uygulanması.
7.	Mevcut KVKK uyum dokümantasyonunun Üyz araçlarının kullanımını da kapsayacak şekilde güncellenmesi.

Sonuç

ÜYZ araçları, iş süreçlerinde önemli verimlilik sağlayan bir teknoloji olmakla birlikte, iş hukuku gibi diğer alanlar yanında, kişisel verilerin korunması, bilgi güvenliği ve kurumsal yönetim bakımından dikkatle yönetilmesi gereken çeşitli riskler barındırmaktadır.

Kurum'un da vurguladığı üzere, esas mesele ChatGPT'nin, Claude'nin, Gemini'in kullanılması değil, bu kullanımın hangi verilerle, hangi kurallar çerçevesinde ve hangi teknik ve idari tedbirler altında gerçekleştirildiğidir.

Bu nedenle şirketlerin, ÜYZ araçlarının kullanımını tamamen yasaklamak yerine çalışanlar için açık kullanım kuralları belirlemesi, hangi bilgilerin sisteme aktarılabilceğini netleştirmesi, gerekli hukuki ve teknik önlemleri alması ve kullanım süreçlerini düzenli olarak gözden geçirmesi önem taşımaktadır.

Sonuç olarak, ÜYZ araçlarının güvenli ve hukuka uygun şekilde kullanılabilmesi teknolojinin sunduğu verimlilikten yararlanılırken kişisel verilerin, ticari sırların ve kurumsal bilgilerin korunmasına yönelik etkili bir yönetim modelinin oluşturulmasına, ayrıca üretken yapay zeka tarafından oluşturulan çıktıların doğruluğunun ve uygunluğunun insan gözetimi altında değerlendirilmesine bağlıdır.