İş Yerlerinde Üretken Yapay Zekâ Kullanımına Dair KVK Rehberi

A. Giriş

Üretken Yapay Zekâ ("**ÜYZ**"), büyük ölçekli veri kümeleri üzerinde eğitilen ve kullanıcı tarafından sunulan istem veya komutlara (prompt) yanıt olarak metin, görsel, video, ses ya da yazılım kodu gibi farklı formatlarda içerikler üretebilen yapay zekâ sistemlerini ifade etmektedir. Bu sistemler, bilgiye erişim, içerik üretimi ve diğer destekleyici faaliyetler kapsamında iş yerlerinde giderek daha yaygın biçimde kullanılmaktadır.

Kişisel Verileri Koruma Kurumu ("**Kurum**"), bu gelişmelere ilişkin olarak bu yapay zekâ araçlarının iş yerlerinde kullanımına ilişkin genel bir çerçeve sunmak amacıyla *İş Yerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı* başlıklı bir doküman yayınlamıştır.

İlgili dokümana buradan ulaşabilirsiniz.

B. Kişisel Verilerin Korunması Mevzuatı Kapsamındaki Değerlendirme

Çalışanlar tarafından ÜYZ araçlarının, e-posta ve metin taslaklarının hazırlanması, belgelerin özetlenmesi ve çeşitli konularda iş materyali üretimi gibi süreçlerinde kullanılması sırasında çoğu zaman farkında olmaksızın kişisel veri niteliği taşıyan bilgiler ilgili sistemlere aktarılmaktadır. ÜYZ sistemleri aracılığıyla gerçekleştirilen bu kişisel veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun ("**KVK Kanunu**") kapsamında hukuka uygun olması önem arz etmektedir.

Bu çerçevede, bir çalışanın ÜYZ aracına müşteri bilgisi, çalışan verisi veya kurum içi yazışma içeriği girmesi, başlı başına bir kişisel veri işleme faaliyeti teşkil etmekte olup ilgili veri işleme faaliyeti bakımından veri sorumlusu işveren olmaktadır.

KVK Kanunu'nun 12'nci maddesi uyarınca veri sorumluları, kişisel verilerin güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakla yükümlüdür. Bu kapsamda, çalışanlar tarafından ÜYZ araçlarının kullanımı sırasında kişisel veri paylaşılması veri ihlali riskini artırmakta ve veri sorumlusu işverenin sorumluluğuna yol açabilmektedir.

Özellikle kurumsal kontrol dışında kullanılan ve Gölge Yapay Zekâ (Shadow AI) olarak adlandırılan ÜYZ araçları, kişisel verilerin hukuka aykırı şekilde işlenmesi, yetkisiz kişilerce erişilebilir hâle gelmesi veya amaç dışı kullanılması gibi riskler doğurmaktadır.

C. Veri Sorumluları Tarafından ÜYZ Araçlarının Kullanımına İlişkin Alınması Gereken Tedbirler

Kurum tarafından yayımlanan dokümanda, ÜYZ araçlarının sağladığı faydalar belirtilmekle birlikte bu araçların kullanımına ilişkin esasların açık ve kapsamlı şekilde belirlenmesi gerektiği vurgulanmaktadır.

Bu kapsamda veri sorumlularına aşağıdaki tedbirler önerilmektedir:

(i) ÜYZ araçlarının iş süreçlerinde kullanımına ilişkin olarak; hangi araçların hangi amaçlarla kullanılabileceğini, bu araçlara girdi olarak sunulabilecek veri türlerini ve elde edilen çıktılara ilişkin kullanım esaslarını belirleyen kurumsal bir politika oluşturulması,

(ii) ÜYZ araçlarıyla etkileşim sırasında mümkün olduğunca anonimleştirilmiş ve genelleştirilmiş verilerin kullanılması;

LBF Partners
Esentepe Mah. Büyükdere Cad. No:108/1 K:7 34394 Şişli İstanbul Türkiye

özellikle sağlık verileri, müşteri verileri ve finansal bilgiler gibi hassas veriler bakımından temkinli hareket edilmesi,

(iii) Kullanımına izin verilen ÜYZ araçlarının gizlilik politikalarının incelenerek, verilerin işlenme amaçları, aktarım süreçleri ve saklama sürelerinin değerlendirilmesi,

(iv) Harici platformlara erişimin sınırlandırılması, ÜYZ araçlarına yalnızca kurumsal cihazlar üzerinden erişim sağlanması ve erişim kontrolü mekanizmalarının uygulanması,

(v) ÜYZ kullanımına ilişkin politika ve kuralların çalışanlara duyurulması ve düzenli eğitim ve farkındalık faaliyetlerinin yürütülmesi.

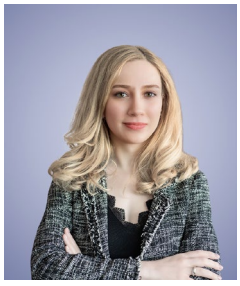
Söz konusu tedbirler, veri sorumlularının 6698 sayılı KVK Kanunu m. 12 kapsamındaki veri güvenliğini sağlama yükümlülüğünün yanı sıra 7418 sayılı Siber Güvenlik Kanunu m. 7 ve ilgili hükümleri çerçevesindeki yükümlülüklerinin yerine getirilmesi bakımından da kritik önem taşımaktadır.

D. Sonuç

Kurum'un bu dokümanı tek başına yeni bir yükümlülük yaratmamakla birlikte, mevcut yükümlülüklerin ÜYZ kullanım senaryolarına uygulanma biçimini netleştirmesi ve Kurum'un denetim gündeminde bu alanın giderek daha fazla yer edinmekte olduğuna işaret etmesi bakımından dikkatle değerlendirilmelidir. Kurum, bu araçların kullanımının topyekûn yasaklanmasını değil, kullanım koşullarının netleştirilmesini, gerekli güvenlik önlemlerinin alınmasını ve çalışanlar nezdinde farkındalık oluşturulmasını esas alan bir yaklaşımın benimsenmesi gerektiğini vurgulamaktadır.

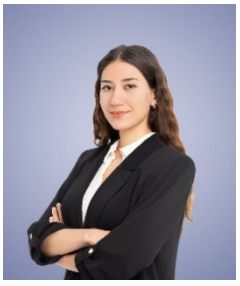
Henüz bir kurumsal ÜYZ politikası oluşturmamış olan veri sorumlularının, bu dokümanı bir uyum başlangıç noktası olarak ele almaları yerinde olacaktır. Bu kapsamda veri sorumlularının iş yerlerinde ÜYZ araçlarına ilişkin kurumsal bir politika oluşturması ve veri güvenliği ve erişim kontrolüne ilişkin esasları belirlemesi veri güvenliğinden kaynaklanan yükümlülüklerin yerine getirilmesi açısından da önem arz etmektedir.

Daha fazla bilgi ve destek için bizimle iletişime geçebilirsiniz.



Elif Çopur Çelebi
Ortak

e.copur@lbfpartners.com



Büşra Karabudak
Avukat

b.karabudak@lbfpartners.com