KOYUNCUOĞLU & KÖKSAL

İŞYERLERİNDE ÜRETKEN YAPAY ZEKÂ ARAÇLARININ KULLANIMININ KVKK KAPSAMINDA DEĞERLENDİRİLMESİNE İLİŞKİN BİLGİ NOTU

I. GİRİŞ

Üretken yapay zekâ sistemleri; metin, görsel, ses ve yazılım kodu gibi içeriklerin oluşturulmasını sağlayan ve farklı sektörlerde iş süreçlerini etkileyen teknolojiler arasında önemli bir yer edinmiştir. Kullanım kolaylığı ve kısa sürede çıktı üretebilme kapasitesi nedeniyle bu araçlar işyerlerinde bilgiye erişim, içerik üretimi ve destekleyici faaliyetler kapsamında giderek daha yaygın kullanılmaktadır.

Bu kapsamda, Kişisel Verileri Koruma Kurumu ("Kurum"), üçüncü taraflarca sunulan ve kamuya açık üretken yapay zekâ araçlarının iş yerlerinde kullanımına ilişkin genel bir çerçeve sunmak, farkındalık oluşturmak ve bilinçli kullanımı teşvik etmek amacıyla hazırlanan "***İş Yerlerinde Üretken Yapay Zekâ Araçlarının Kullanımı***" başlıklı dokümanı yayımlamıştır.

II. ÜRETKEN YAPAY ZEKÂ

Kurum, *Üretken Yapay Zekâ*'yı; büyük veri kümeleriyle eğitilen, kullanıcı istem veya komutlarına (prompt) yanıt olarak metin, görsel, video, ses veya yazılım kodu üretebilen ve geleneksel sınıflandırma yöntemlerinden farklı olarak istatistiksel örüntülere dayanarak insan üretimine benzer yeni içerikler oluşturabilme kapasitesine sahip sistemler olarak tanımlamaktadır. Bu araçların; pazarlama, eğitim, sağlık, hukuk ve yazılım gibi alanlarda taslak hazırlama, özetleme ve fikir geliştirme gibi amaçlarla kullanımlarının iş süreçlerine hız ve verimlilik katabildiği belirtilmiştir.

Ancak Kurum aynı zamanda, *Gölge Yapay Zekâ* olarak tanımlanan bir riskin de altını çizmektedir. Bu kavram, Üretken Yapay Zekâ araçlarının kullanılmakta olduğu kurumun bilgisi, onayı veya denetimi dışında ilgili kurum çalışanları tarafından kullanılması durumunu ifade etmektedir. Çalışanların zaman kazanma ve verimlilik artışı beklentisiyle toplantı notları, rapor taslakları, iç yazışmalar veya müşteri bilgileri gibi kamuya açık olmayan bilgileri üçüncü taraf üretken yapay zeka araçları ile paylaşabilmesi bu tür kullanımlara örnek olarak sayılmıştır. Bu tür durumlarda hangi üretken yapay zeka araçlarının hangi amaçlarla kullanıldığı, bu araçlara hangi veri türlerinin girdi olarak sunulduğu ve elde edilen çıktıların iş süreçlerinde nasıl değerlendirildiğine ilişkin kurumsal görünürlük ve denetim imkanları sınırlı kalabilmektedir.

III. ORTAYA ÇIKABİLECEK RİSKLER

Gölge Yapay Zekâ araçlarının kurumsal denetim dışında kullanılması, veri işleme süreçlerinin takibini imkânsız kılarak hukuki uyum ve olaylara müdahale kabiliyetini zayıflatmaktadır. Kurum bu doğrultuda şu riskleri belirlemiştir:

- Kurumsal kayıt dışı kullanım, hangi verinin hangi amaçla kullanıldığının tespitini imkânsız kılabilecektir. Bu durum, olaylara müdahaleyi zorlaştıracağından ve mevzuata uyumun kanıtlanamaması riskini doğuracağından, **denetlenebilirlik ve hesap verebilirliğe ilişkin riskler** doğurabilecektir.
- Kurumsal değerlendirme ve doğrulama süreçlerinden geçmeden kullanılan Üretken Yapay Zekâ araçları hatalı, yanıltıcı veya ön yargılı çıktılar üretebilecektir. Bu çıktılara dayanarak alınan kararlar, iş süreçlerinde hatalara, kuruluş hedefleri, kalite standartları veya etik ilkelerle uyumsuz sonuçlara yol açabileceğinden, **karar kalitesi ve doğruluğa ilişkin riskler** doğurabilecektir.
- Kaynak kod, ürün tasarımları, iş stratejileri ve ticari sırlar gibi rekabet açısından hassas bilgilerin harici Üretken Yapay Zekâ araçlarıyla paylaşılması, bu verilerin model geliştirme süreçlerinde kullanılması veya yetkisiz kişilerin erişime açılmasına sebebiyet verebileceğinden **fikri mülkiyet ve ticari sırların korunmasına ilişkin riskler** doğurabilecektir.
- Doğruluğu ve güvenilirliği teyit edilmemiş üretken yapay zekâ çıktılarının kullanılması, hatalı bilgilendirme veya düşük kaliteli içerik nedeniyle kuruluşun güvenilirliğini zedeleyerek **kurumsal itibar ve güven kaybına ilişkin riskler** doğurabilecektir.
- Kurumsal kontrol dışında kullanılan Üretken Yapay Zekâ araçları, güvensiz API'ler, kişisel cihazlar veya denetimsiz entegrasyonlar üzerinden saldırı yüzeyini genişletebilir. Bu durum, zararlı yazılımlar, yetkisiz erişim ve veri kaybı gibi tehditleri artırarak **bilgi güvenliği ve kurumsal sistemlerin bütünlüğünü etkileyebilecek siber güvenlik risklerini arttırabilecektir**.
- Kurumsal kontrol dışında kullanılan Üretken Yapay Zekâ araçlarıyla kişisel verilerin paylaşılması hukuka aykırı şekilde işlenmesine, yetkisiz kişiler tarafından erişilmesine veya amaç dışı kullanılmasına yol açabileceğinden ve bu çıktılar üzerinden üçüncü kişiler tarafından erişilebilir hâle gelebileceğinden **kişisel verilerin korunmasına ilişkin riskler** doğurabilecektir.

IV. DİKKATE ALINMASI GEREKEN HUSUSLAR

Üretken Yapay Zekâ araçlarının iş süreçlerinde yaygınlaşması, kurumsal yaklaşımların gözden geçirilmesini zorunlu kılmaktadır. Kurum, kullanımın tamamen yasaklanmasının gerçekçi olmadığını ve bu tür katı yaklaşımların çalışanları "kontrol dışı" kullanıma (Gölge Yapay Zekâ) itebileceğini

değerlendirmektedir. Bu nedenle, yasaklama yerine yönlendirme, denge ve farkındalık temelli bir yaklaşımın benimsenmesi gerektiğini ifade etmektedir. Bu doğrultuda Kurum, iş yerlerinde Üretken Yapay Zekâ araçlarının kullanımına ilişkin olarak şirket, kurum ve kuruluşlar tarafından dikkate alınabilecek bazı hususlara değinmektedir:

- **Üretken Yapay Zekâ araçlarının iş süreçlerindeki sınırlarını belirlemek adına, hangi araçların, hangi faaliyetlerde kullanılacağı, sisteme girilebilecek bilgi türleri, çıktıların kullanım esasları ve veri güvenliği kurallarının netleştirildiği kurumsal politikaların oluşturulmasını öngörmektedir.** Bu kapsamda kuruluşlar, kişisel veri, ticari sır veya kurumsal açıdan hassas bilgi içermemesi şartıyla üretken yapay zekâ araçlarının fikir geliştirme çalışmalarını destekleme, metinlerin dilsel açıdan gözden geçirilmesi veya internet ortamındaki içeriklerin özetlenmesi gibi amaçlarla kullanımına izin verebilirler.

- **Üretken Yapay Zekâ araçları kullanılırken hassas bilgiler ve kişisel veriler konusunda çalışanların dikkatli bir yaklaşım benimsemesi gereklidir.** Bu kapsamda, Üretken Yapay Zekâ araçlarının veri toplama ve işleme süreçlerine ilişkin aydınlatma metinleri ile gizlilik politikalarının incelenmesi ve hangi verilerin hangi amaçlarla işlendiği konusunda bilgi sahibi olunması önem taşımaktadır. Ayrıca kişiyi doğrudan veya dolaylı olarak tanımlamaya elverişli kişisel verilerin ya da üçüncü kişilere ait bilgilerin bu araçlarla paylaşımının riskli olduğunun altı çizilmiştir. Bu nedenle, **Üretken Yapay Zekâ araçlarıyla etkileşim sırasında mümkün olduğunca anonimleştirilmiş ve genelleştirilmiş ifadelerin tercih edilmesi, özellikle sağlık verileri, finansal bilgiler ve hukuki süreçlere ilişkin hassas bilgiler söz konusu olduğunda daha temkinli bir yaklaşım benimsenmesi gerektiği vurgulanmaktadır.**

- Üretken yapay zekâ araçları tarafından üretilen çıktılara aşırı güven duyulması ve insan yargısının geri planda kalması, iş süreçleri bakımından dikkat edilmesi gereken bir risk olarak değerlendirilmektedir. Literatürde "otomasyon ön yargısı" olarak ifade edilen bu durum, kullanıcıların otomatik sistemler tarafından üretilen çıktıları yeterli sorgulama ve değerlendirme yapmadan doğru kabul etmesine yol açabilmektedir. Bu nedenle Kurum, **Üretken Yapay Zekâ çıktılarının nihai kararların dayanağı olarak görülmemesi, insan denetimi altında destekleyici unsur olarak değerlendirilmesi ve doğruluk, uygunluk ile bağlam açısından gözden geçirilmesi tavsiye edilmektedir.**

- Kurum, kontrol dışı kullanımı azaltmak için çalışanların yalnızca kuruluş tarafından belirlenen ve kullanım koşulları tanımlanmış araçlara erişmesini sağlayacak teknik ve idari yaklaşımları önermektedir. Bu kapsamda; **harici platformlara erişimin ağ düzeyinde sınırlandırılması, erişimin sadece kurumsal cihazlar üzerinden yapılması ve hangi çalışanların hangi yetkiyle**

bu araçları kullanabileceğinin rol temelli olarak belirlenmesi gibi tamamlayıcı tedbirlerin alınması risk yönetimini güçlendirecektir.

- Üretken Yapay Zekâ araçlarının iş süreçlerinde güvenli kullanımı için kurumsal politika ve yönlendirmelerin yanında çalışanlara riskler, kullanım amaçları ve dikkat edilecek hususlar hakkındaki eğitimlerin verilmesi, teknik ve hukuki farkındalığı da artıracağından faydalı olacaktır.

V. SONUÇ

Üretken Yapay Zekâ araçlarının iş süreçlerine entegrasyonunun kaçınılmaz bir gelişim olduğu, ancak bu sürecin kontrolsüz yönetiminin kişisel verilerin korunması yönünden ciddi hukuki ve teknik riskler barındırdığı açıktır.

Diğer yandan işyerlerinde verimlilik artışı da hedeflendiğinden üretken yapay zekâ kullanımının yasaklayıcı değil, yönlendirici ve şeffaf bir kurumsal politika ile benimsenmesi tavsiye edilmektedir.

Kişisel verilerin korunması ve ticari sırların güvenliği için verilerin anonimleştirilmesi, çıktıların mutlak suretle insan denetiminden geçirilmesi ve çalışanların bu süreçteki farkındalığının artırılması, KVKK uyum süreci açısından kritik ve gereklidir.

Kurumumuz da bu teknolojilerin ancak risk temelli bir yaklaşımla ve etik ilkeler çerçevesinde yapılandırılması halinde sürdürülebilir bir fayda sağlayabileceğini değerlendirmektedir.

Kılavuzun tamamına bağlantıdan ulaşabilirsiniz: (https://www.kvkk.gov.tr/Icerik/8674/is-yerlerinde-uretken-yapay-zeka-araclarinin-kullanimi)

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.*