SAYI: 56

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

VERİ & TEKNOLOJİ HUKUKU BÜLTENİ

EKIM 2025

GÜNCEL HABERLER

- Özel Sağlık Sigortaları Yönetmeliği'nde yapılan değişiklik ile KVKK ile daha uyumlu hale getirildi.
- Kişisel Verileri Koruma Kurumu Ekim ayını "Siber Güvenlik Farkındalık Ayı" ilan etti.
- Milli Eğitim Bakanlığı, "Yapay Zeka Etiği Tavsiyeleri" kitapçığını yayımladı.
- Kişisel Verilerin Korunması Kurumu Quishing hakkında bir bilgilendirme yayımladı.
- Ekim Ayı İçerisinde Bildirilen Kişisel Veri İhlalleri

GLOBAL GELİŞMELER

- Avrupa Veri Koruma Denetçisi (EDPS), AB kurumlarının üretken yapay zeka kullanımı ve kişisel veri işleme süreçlerine dair rehber yayımladı.
- Microsoft, yapay zekanın hukuk sektöründeki kullanımına yönelik yeni bir kaynak yayınladı: Microsoft 365 Copilot ile Hukuk Endüstrisi

DİJİTAL ÇAĞDA SİBER GÜVENLİK İHTİYACI

Günümüzde dijital dönüşüm, bireylerden kurumlara kadar herkesin yaşamının merkezinde yer alıyor. İnternetin ve teknolojinin sunduğu olanaklar sayesinde bilgiye erişim hızlandı, iletişim kolaylaştı ve iş süreçleri otomatikleşti. Ancak bu gelişmeler beraberinde ciddi riskleri de getirdi: kişisel verilerin çalınması, kimlik hırsızlığı, fidye yazılımları ve kurumsal veri ihlalleri artık gündelik hayatın bir parçası haline geldi. Bu nedenle siber güvenlik, sadece teknik bir konu değil, toplumsal ve ekonomik bir zorunluluk haline geldi.

Siber tehditler giderek daha karmaşık ve hedef odaklı bir hale geliyor. Artık sadece büyük şirketler değil, küçük işletmeler ve bireyler de bu tehditlerin potansiyel hedefleri arasında. Basit bir e-posta eki, güvenlik açığı bulunan bir yazılım veya zayıf bir parola bile büyük çaplı veri kayıplarına ve itibar zedelenmesine yol açabiliyor.

Güvenli bir dijital ekosistem oluşturmak, bilinçli kullanıcı davranışlarıyla başlar. Çalışan eğitimleri, güçlü parola politikaları, düzenli güvenlik testleri ve güncel yazılımlar siber riskleri en aza indirmede kilit rol oynar. Bununla birlikte, siber güvenliğe yapılan yatırımlar bir maliyet kalemi değil, sürdürülebilirliğin de teminatıdır.

GÜNCEL HABERLER

ÖZEL SAĞLIK SIGORTALARI YÖNETMELİĞİ'NDE YAPILAN DEĞİŞİKLİKLER VE KVKK İLE UYUMU

20 Ekim 2025 tarihinde Resmi Gazete'de yayımlanan değişiklikler ile KVKK ile uyum kapsamında bir takım düzenlemelere yer verildi. Bu düzenlemeler kapsamında saklama süreleri değiştirilmesi, sır saklama yükümlülüğünün geniletilmesi gibi hususlarda KVKK ile temas etmekte ve ona uyumlu hale getirilmeye çalışıldığı görülmektedir.

Yapılan düzenlemeler ile:

- Artık özel sağlık sigortalarındaki tüm kişisel veri işleme faaliyetlerinde, 6698 sayılı Kanun'un usul ve esaslarına uyma zorunluluğu bulunacak.

- Önceki düzenlemede sağlık verilerinin yalnızca sigortalının yazılı onayıyla alınabileceği belirtiliyordu. Yeni madde bu ifadeyi kaldırdı; artık veri işleme süreçlerinde KVKK'daki işleme şartları esas alınacak.

- Önceki düzenlemede sağlık bilgileri yalnızca Sigorta Bilgi ve Gözetim Merkezi ve yetkili mercilerle paylaşılabiliyordu. Artık bu sınır yerine KVKK'daki genel veri işleme esasları geçerli olacak.

- Saklama süreleri 10 yıl olarak belirlendi. Yeni düzenlemeye göre Merkez, sigortalılık sona erdikten sonra kişisel verileri 10 yıl boyunca saklayacak. Bu süre sonunda veriler resen silinecek, yok edilecek veya anonimleştirilecek.

- Sır saklama yükümlülüğü genişletildi. Yeni madde, 5684 sayılı Sigortacılık Kanunu'na atıf yaparak, sır saklama yükümlülüğünün görev veya sıfat sona erdikten sonra da devam edeceğini açıkça belirtti.

İlgili Resmi Gazete ilanına buradan ulaşabilirsiniz.

GÜNCEL HABERLER

KİŞİSEL VERİLERİ KORUMA KURUMU EKİM AYINI "SİBER GÜVENLİK FARKINDALIK AYI" İLAN ETTİ

Ekim ayı, dünya genelinde "Siber Güvenlik Farkındalık Ayı" olarak kutlanıyor. KVKK da bu kapsamda yayımladığı çeşitli kataloglar , duyuru ve bilgilendirmelerle Ekim ayının Siber Güvenlik farkındalık ayı olduğunu duyurdu.

KVKK'nın Ekim ayı vesilesi ile yayımladığı bilgi notları ile kişisel verilerin korunması ve bilgi güvenliğinin önemi ve siber güvenliliğin gerekliliği tekrar hatırlandı.

KVKK'nın yayımladığı katalog ve bilgilendirmelere göre siber güvenlik için alınacak bazı tedbirler:

- Güçlü parolalar & çok faktörlü doğrulama (MFA): Parola seçiminde uzunluk, karakter çeşitliliği ve benzersizlik önemlidir. Mümkünse hesaplarınız için çok faktörlü kimlik doğrulama aktif hale getirilmeli.
- Toplu e-postada gizlilik: Aynı anda gönderim yapılan mesajlarda alıcıların gizliliğini koruyun; güvenli toplu gönderim araçlarını tercih edin.
- Şüpheli iletilere dikkat: Phishing (oltalama) saldırılarına karşı tetikte olun; çalışanları bilinçlendirmek ve simülasyonlarla farkındalık oluşturmak etkili bir savunmadır.
- Antivirüs & güvenlik yazılımları: Tüm cihazlarda güncel antivirüs ve kötü amaçlı yazılım tarayıcıları bulundurulmalı, düzenli güncellenmelidir.
- Kısa süreli uzaklaşmalarda ekran kilitleme: Cihaz başından ayrıldığınızda ekran kilidi aktif olmalı; böylece izinsiz erişim önlenir.
- Erişim kontrolü: Çalışanların yalnızca görevleri kapsamında izinli erişim hakları olmalı; "herkese her şeye erişim" yaklaşımından kaçınılmalı.
- Gizlilik bilinci: Kalabalık ortamlarda ekranınızdaki belgeleri dikkatle yönetin; ortak alanlarda kişisel veriler görünür durumda kalmamalı.
- Çevrim içi toplantılarda özen: Ekran paylaşımı yapmadan önce açık belgeleri kapatın; bildirimlerin görünürlüğünü sınırlandırın.
- Veri saklama süresi: Kişisel veriler yalnızca yasal zorunluluklar gerektirdiği süre boyunca saklanmalı; ihtiyaç kalmadığında güvenli biçimde imha edilmeli.

GÜNCEL HABERLER

MİLLİ EĞİTİM BAKANLIĞI, "YAPAY ZEKA ETİĞİ TAVSİYELERİ" KİTAPÇIĞINI YAYIMLADI

Yapay zeka teknolojilerinin eğitim sistemine güvenli, etik ve sorumlu biçimde entegrasyonuna rehberlik etmek amacıyla hazırlanan bu e-kitap, eğitim paydaşlarına yönelik tavsiyeler sunuyor.

farkındalık artırmayı, eğitimde siber güvenlik tedbirlerini almayı ve yapay zekanın etik kullanımını sağlamayı hedefliyor.

Genel tavsiyelerin yanı sıra özellikle geliştiriciler, üreticiler ve servis sağlayıcılar için aşağıdaki başlıklar altında öneriler yer alıyor.

- Veri Koruma ve Gizlilik
- Şeffaflık ve Açıklanabilirlik
- İnsan Onayı ve Denetim
- Çocuklara Yönelik Güvenlik
- Etik ve Pedagojik Uyum
- Erişilebilirlik ve Kapsayıcılık
- Üçüncü Taraflarla İş birliği
- Etik Zorunluluk

Milli Eğitim Bakanlığı tarafından yayımlanan işbu kitapçıkta ayrıca öğrenciler, öğretmenler, idareciler ve veliler için de tavsiyeler bulunuyor.

Ayrıca bu kitapçıkta, Kitapçığın Cumhurbaşkanlığının vizyonu ve 12. Kalkınma Planı kapsamındaki Ulusal Yapay Zeka Stratejisi çerçevesinde yürürlüğe konulan "Eğitimde Yapay Zeka Politika Belgesi ve Eylem Planı (2025-2029)" doğrultusunda hazırlandığı belirtilmiştir.

Bu e-kitapçıktan alınan bir alıntı aşağıdaki gibidir:

"Yapay zekâ sistemleri; veri yanlılığı, şeffaflık eksikliği ve özellikle çocuklara ait hassas verilerin korunması gibi önemli riskler de barındırmaktadır. Yapay zekânın sorumlu ve etik kullanımı, yalnızca doğru algoritmaların kullanılmasından daha fazlasıdır. Bu, eğitim sisteminin tüm paydaşlarının (öğrenciler, eğitimciler, tasarımcılar, politika yapıcılar vb.) iş birliği içinde çalışmasını ve aktif bir sorumluluk taşımasını gerektirir. Bunun bilinciyle Yapay Zekâ Etiği Tavsiyeleri kitapçığı, şeffaflık, hesap verebilirlik, veri güvenliği, mahremiyet, adalet, eşitlik, insan merkezlilik gibi ilkeleri esas alarak, yapay zekânın eğitim sistemine güvenli ve etik biçimde entegrasyonuna rehberlik etmeyi amaçlamaktadır."

İlgili kitapçığa buradan ulaşabilirsiniz.

GÜNCEL HABERLER

QR KODLARLA GELEN RİSK: QUISHING

KVKK'nın Siber Güvenlik Farkındalık ayında siber güvenliğe dikkat çekmek için yaptığı paylaşımlardan biri de "Quishing"e ilişkin oldu. KVKK QR kodlar ile gelen bu riske dikkat çekerken aşağıdaki ifadelere yer verdi:

QR kodlar son yıllarda günlük yaşamın birçok alanında kullanılmaktadır. QR kodlar, hızlı ve pratik bir kullanım imkânı sağlamakla birlikte, artan kullanımları kişisel veri güvenliği ve gizliliğine yönelik birtakım riskleri de beraberinde getirmektedir.

QR (Quick Response) ve oltalama (phishing) kelimelerinin birleşiminden oluşan "Quishing"; siber tehdit aktörlerinin sahte veya değiştirilmiş QR kodlarını kullanarak, kullanıcıları kötü amaçlı web sitelerine yönlendirmesi, kişisel verilerini paylaşmaya ikna etmesi ya da cihazlarına zararlı yazılımlar yüklemesi biçiminde ortaya çıkan bir oltalama yöntemidir.

Bu tür tehditlere karşı korunmak ve QR kodları güvenle kullanmak için şu hususlara dikkat edilmesi önem taşımaktadır:

- QR kodun kaynağını doğrulayınız. Kodları yalnızca güvenli kaynaklardan tarayınız. Tanımadığınız kişilerden veya beklenmedik e-posta/mesajlardan gelen QR kodları taramaktan kaçınınız. Özellikle aciliyet veya panik hissi yaratacak şekilde kurgulanmış mesajlara karşı temkinli olunuz.

- Güvenilir QR kod okuyucuları tercih ediniz. Çoğu akıllı telefonun kamera uygulaması QR kodları doğrudan tanımakla birlikte, üçüncü taraf bir uygulama kullanmanız gerekmesi durumunda bu uygulamanın güvenilir olduğundan emin olunuz.

- Yönlendirildiğiniz bağlantıyı inceleyiniz. Tarama sonrası ulaştığınız bağlantının gerçekten doğru siteye veya mobil uygulamaya ait olup olmadığını kontrol ediniz. Bu kapsamda yazım hataları, farklı karakterler veya alışılmadık uzantılar bulunup bulunmadığına dikkat ediniz.

- Kişisel bilgi taleplerine karşı dikkatli olunuz. İlgili kodu taramanızın ardından kişisel bilgilerinizi talep eden bir bağlantıya yönlendirilmeniz durumunda, bilgilerinizi paylaşmadan önce internet sitesinin doğruluğundan emin olunuz. Mümkünse ilgili adresi tarayıcınıza manuel olarak giriniz.

- Kamuya açık alanlardaki QR kodlara karşı dikkatli olunuz. Sonradan yapıştırılma, hizasızlık veya pikselleşme gibi fiziksel değişiklikler olup olmadığını kontrol ediniz. Şüpheli görünen kodları taramayınız.

- Cihaz ve hesap güvenliğinizi güçlendiriniz. İşletim sisteminizi güncel tutmaya, güçlü parolalar belirlemeye ve mümkünse çok faktörlü kimlik doğrulama kullanmaya özen gösteriniz.

Unutmayın: QR kodlar pratik bir araç olsa da kötüye kullanıldıklarında kişisel verileriniz için risk oluşturabilir. Farkındalıkla hareket etmek, olası risklere karşı en güçlü korumadır.

İlgili bilgilendirmeye buradan ulaşabilirsiniz.

GÜNCEL HABERLER

EKİM AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Cleverbrige GmbH

Veri sorumlusu sıfatını haiz Cleverbridge GmbH (Tunisstraße 19-23 50667 Cologne, Germany) tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 10.09.2025 tarihinde gerçekleştiği ve 15.09.2025 tarihinde tespit edildiği,
- Veri sorumlusunun müşteri veri tabanına yetkisiz erişim sonucu ihlalin gerçekleştiği,
- Bilinmeyen bir IP Adresi tarafından API'nin alışılmadık bir şekilde kullanıldığının fark edilmesi üzerine API'nin bilgi güvenliği ekibi tarafından engellendiği,
- İhlalden etkilenen kişisel verilerin isim, şirket, e-posta, ödeme yöntemi, kartın son 4 hanesi, kartın son kullanma tarihi, satın alınan ürünlerin fiyatlandırma ayrıntıları, tekrarlayan faturalandırma ayrıntıları olduğu,
- İhlalden etkilenen ilgili kişi grubunun müşteriler ve potansiyel müşteriler olduğu
- İhlalden etkilenen ilgili kişi sayısının 1235 olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 09.10.2025 tarih ve 2025/1911 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili ihlal duyurusuna buradan ulaşabilirsiniz.

Haydigiy E-Ticaret Tekstil San. ve Tic. Ltd. Şti.

Veri sorumlusu sıfatını haiz Haydigiy E-Ticaret Tekstil Sanayi ve Ticaret Limited Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- 15.10.2025 tarihinde tespit edilen ihlalin başlama tarihinin tam olarak bilinmediği,
- Veri sorumlusunun bazı müşterileri tarafından iletilen şüpheli işlem bildirimleri üzerine başlatılan inceleme sonucunda bir yönetici hesabına yetkisiz erişim sağlandığı ve bu hesap üzerinden siteye bir kod eklendiğinin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının abone/üyeler ile müşteri ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin iletişim, lokasyon ve finans bilgileri olduğu,
- İhlalden etkilenen ilgili kişi sayısının belirlenmesi için çalışmaların devam ettiği
- İlgili kişilerin veri ihlali ile ilgili olarak; www.haydigiy.com internet adresi, haydigiy başlıklı sms, info@haydigiy.com iletişim araçlarıyla bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.10.2025 tarih ve 2025/1976 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili ihlal duyurusuna buradan ulaşabilirsiniz.

GÜNCEL HABERLER

EKİM AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

İstanbul Golf İhtisas Spor Kulübü

Veri sorumlusu sıfatını haiz İstanbul Golf İhtisas Spor Kulübü tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin, 15.10.2025 tarihinde veri sorumlusu bilgisayarında fidye talebi içeren mesajın görülmesiyle tespit edildiği,
- Bilgisayar üzerinde bulunan dosyalarda şifreleme işleminin başarılı bir şekilde gerçekleşmediği,
- İhlalden etkilenen ilgili kişi grubunun; aboneler/üyeler olduğu,
- İhlalden etkilenen kişisel verilerin; kimlik (T.C. No), iletişim (e-posta, cep telefonu veya ofis telefonu), lokasyon (adres), özlük (medeni durumu, adli sicil kaydı) ve mesleki deneyim bilgileri olduğu,
- İhlalden etkilenen kişi sayısının henüz tespit edilemediği incelemelerin devam ettiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.10.2025 tarih ve 2025/1977 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili ihlal duyurusuna buradan ulaşabilirsiniz.

Mango T.R. Tekstil Tic. Ltd. Şti.

Veri sorumlusu sıfatını haiz Mango T.R. Tekstil Tic. Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin 06.10.2025-10.10.2025 tarihleri arasında gerçekleştiği, 10.10.2025 tarihinde tespit edildiği,
- İhlalin, veri sorumlusunun kullandığı dijital pazarlama e-posta sistemi platformunun API'sine erişim için kullanılan bir yönetici kimlik bilgisinin sızdırılması sonucu, müşteri verilerine yetkisiz erişim sağlanmasıyla gerçekleştiği,
- Siber saldırının Mango'nun İspanya merkezine gerçekleştirildiği ve Türk vatandaşları da dahil olmak üzere global olarak tüm müşterilerin kişisel verilerine yetkisiz olarak erişilmiş olduğu,
- İhlalden müşterilere ait ad (soyad verisi için ihlal olmadığı), ülke, posta kodu, telefon numarası ve e-posta adresi bilgilerinin etkilendiği,
- İhlalden, Mango Türkiye için 4.349.620 ilgili kişinin etkilendiği,
- İlgili kişilerin veri ihlali ile ilgili olarak e-posta, çağrı merkezi ve sohbet robotu iletişim araçlarıyla bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.10.2025 tarih ve 2025/1973 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

İlgili ihlal duyurusuna buradan ulaşabilirsiniz.

GLOBAL GELİŞMELER

AVRUPA VERI KORUMA DENETÇİSİ'NDEN YAPAY ZEKA VE KIŞISEL VERİLERE İLİŞKİN REHBER

Avrupa Veri Koruma Denetçisi (EDPS), AB kurumlarının üretken yapay zeka kullanımı ve kişisel veri işleme süreçlerine dair yeni bir rehber yayımladı.

Daha önce yayımlanan rehber, AB kurumlarından alınan geri bildirimlere dayanılarak revize edilmiştir. Yeni rehber, üretken yapay zeka araçlarının sorumlu bir şekilde geliştirilmesi ve kullanımı için uygulanabilir, daha net ve daha pratik bir dizi açıklamalar ve tavsiyeler sunuyor.

Kılavuz, aşağıdakiler de dahil olmak üzere bir dizi önemli güncelleme sunmaktadır:

- Netlik ve tutarlılık adına, üretken yapay zeka için daha net bir tanım getirilmiştir.
- AB kurumlarının veri işleme faaliyetlerinin yasallığını değerlendirmelerini kolaylaştıracak eylem odaklı bir uyum kontrol listesi belirlenmiştir.
- Kurumların veri sorumlusu, müşterek veri sorumlusu veya veri işleyen olup olmadıklarını belirlemede kolaylıklar getirilmiştir.
- Üretken yapay zeka kapsamında yasal dayanaklar, amaç sınırlamaları ve veri sahiplerinin haklarının nasıl korunacağına ilişkin ayrıntılı tavsiyeler ve açıklamalr verilmiştir.

Avrupa Veri Koruma Denetçisi (EDPS), bu rehberi AB kurumlarının bağımsız veri koruma denetim otoritesi olarak görevini yerine getirirken yayımladığını, bu rehberin AB Yapay Zeka Yasası kapsamında bir piyasa denetim otoritesi görevi çerçevesinde hazırlanmadığını vurguladı.

Avrupa Veri Koruma Sorumlusu Wojciech Wiewiórowski şunları söyledi:

"Yapay zeka, insan yaratıcılığının bir uzantısıdır ve onu yöneten kurallar da aynı dinamiklikle gelişmelidir. Yönergelerimizin bu ilk revizyonu, bir güncellemeden çok daha fazlasıdır; AB içinde insan merkezli inovasyonu mümkün kılarken bireylerin kişisel verilerini titizlikle korumak gibi ikili misyonumuzun bir yeniden teyididir. Bu yeni sürümle, AB kurumları tarafından kullanılan tüm üretken yapay zekaların, Avrupa'nın veri koruma standartlarından ödün vermeden kamu yararına hizmet etmesini sağlamak için uygulamalı rehberlik sağlıyoruz."

İlgili rehbere buradan ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

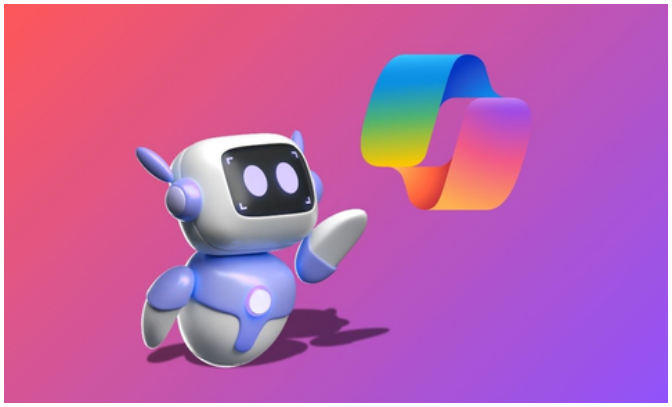
MICROSOFT 365 COPILOT İLE HUKUK ENDÜSTRİSİ

Microsoft, yapay zekanın hukuk sektöründeki kullanımına yönelik yeni bir kaynak yayınladı: Microsoft 365 Copilot ile Hukuk Endüstrisi.

Hukuk profesyonellerinin iş süreçlerini dönüştürmek için tasarlanmış e-kitap, karmaşık sözleşme analizlerinden yasal dava özetlemelerine, maliyet optimizasyonundan uyum eğitim videolarına kadar altı pratik senaryoyu ve ipuçlarını adım adım ele alıyor. Örneğin, bir senaryo sözleşmeleri nasıl otomatikleştireceğinizi ve hassas bir şekilde inceleyeceğinizi gösteriyor. Microsoft, kişisel hukuk asistanınız 365 Copilot ile zaman alıcı süreçlere ve hataya açık manuel görevlere yer olmayacağını belirtiyor.

Microsoft E-Kitaptan neler beklenebileceğini şöyle açıklıyor:

- Saf Uygulama: Microsoft 365 Copilot ile günlük hukuki görevleriniz için heyecan verici pratik senaryolar – sözleşme yönetiminden hukuki danışmanlığa kadar.
- Yapay Zeka Destekli Hukuk Stratejisi: Pazarın zorluklarının üstesinden gelin.
- Verileriniz, Sözümüz: Microsoft 365 Copilot en yüksek güvenlik standartlarını nasıl karşılıyor?



- **Prompt Magic: Microsoft 365 Copilot'un tüm potansiyelinden yararlanmanızı sağlayan etkili istemler.**

E-kitaptan bazı dikkat çekici başlıklar:

- **Veri Koruma Garantisi: Microsoft 365 Copilot, kurumsal verileri (EDP ile) korurken, verilerin temel modelleri eğitmek için kullanılmadığını taahhüt ediyor.**
- **Pratik Senaryolar: Otomatik sözleşme incelemesi, maliyet optimizasyonu, dış iletişim düzenlemesi gibi örneklerle uygulanabilir promptlar ve indirilebilir araçlar sunuluyor.**
- **Geleceğe Hazırlık: "AI'sız ve AI'li Dünya" karşılaştırması, yapay zekanın hukuk iş akışlarında nasıl fark yarattığına odaklanıyor.**

Microsoft, Copilot ve e-kitapçık ile hukuk departmanınızın inovasyonun öncüsü haline geleceğini söylüyor.

Ayrıca, Microsoft bu e-kitabı, "Herkes İçin Yapay Zeka" adlı ücretsiz e-kitap serisinin bir parçası olarak ücretsiz sunuyor.

E-kitaba ulaşmak için buradan form doldurabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership