SAYI: 32

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

KVK & SİBER GÜVENLİK BÜLTENİ

EYLÜL 2023

GÜNCEL HABERLER

- Kişi Kurulu'nun Yeni Yayımlanan Karar Özetleri
- Eylül Ayında Gerçekleştirilen Veri İhlal Bildirimleri

GLOBAL GELİŞMELER

- Suudi Arabistanda Kvk Hakkında Yeni Kanun Yürürlüğe Girdi
- Kalifornia Milletvekilleri Çevrimiçi Kişisel Verilerin Silinmesini Kolaylaştıracak Yasa Tasarısını Kabul Etti
- Yeni Zelanda Mahremiyet Komisyonerliği Ofisi Rehber Yayımladı
- İrlanda Veri Koruma Otoritesi (DPC), GDPR'ın Uygulanmasının İlk Beş Yılını İçerecek Şekilde 2018-2023 Yıllarına Tekabül Eden Dönemde Alınan Kararlara İlişkin Özetleri İçeren Bir Çalışma Yayımlandı
- Avrupa Veri Yönetişimi Yasası (European Data Governance Act) Uygulanmaya Başladı
- Vd.

KİŞİSEL VERİSİ İŞLENEN KİŞİNİN HAKLARI NELERDİR NASIL KULLANILIR?

Anayasamızın 20. maddesine göre; Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

Kişisel Verilerin Korunması Kanunu uyarınca ise ilgili kişi her zaman veri sorumlusuna başvurarak kendisi ile ilgili;

- Kişisel verilerinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kişisel verilerin silinmesini veya yok edilmesini isteme,
- Kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

Bu başvuruya yetersiz cevap verilmesi yahut verilen cevabın yeterli ya da hukuka uygun bulunmaması halinde 30 gün içerisinde ilgili kişilerin Kişisel Verileri Koruma Kurulu'na şikâyet hakkı bulunmaktadır.

GÜNCEL HABERLER

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Elca Kozmetik Limited Şirketi

Veri sorumlusu sıfatını haiz Elca Kozmetik Limited Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin; veri sorumlusunun dahil olduğu Estee Lauder grup şirketlerinin global düzeyde kullandığı MOVEit isimli yazılımda 30/05/2023 tarihinde yaşanan bir veri sızıntısı sonucunda gerçekleştiği ve 20/09/2023 tarihinde tespit edildiği,
- İhlalden etkilenen kişisel verilerin isim, soyisim, e-mail adresi, cep telefonu numarası veya sabit hat ve doğum tarihi olduğu,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen ilgili kişi sayısının yaklaşık 83.185 olduğu,
- İhlalin etkilerini tespit etmek için yapılan çalışmaların devam ettiği bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 28.09.2023 tarih ve 2023/1682 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

Defacto Perakende Tic. A.Ş.

Veri sorumlusu sıfatını haiz olan Defacto Perakende Tic. AŞ tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Müşterilerinin profil sayfalarında kendilerine ait olmayan kişisel bilgileri gördüğüne ilişkin bilgilendirme ile 14.09.2023 tarihinde ihlalin tespit edildiği,
- Veri sorumlusunun, müşteri içeriklerinin son kullanıcıya eriştirilebilmesi için CDN tüketim trafiği sağlanması adına veri işleyenden hizmet aldığı,
- Veri işleyenin sunduğu hizmetlerin iyileştirilmesi adına yapılan bir dizi geliştirmeleri kapsayan yazılım versiyonunun devreye alınması sonrasında veri ihlalinin yaşandığı,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim ve müşteri işlem verileri olduğu,
- Hesabım sayfasındaki Hesap Bilgileri ekranını ziyaret eden toplamda 1337 müşteriden bir kısmı sadece kendi hesap bilgileri ekranını görüntülerken bir kısım müşterinin ise hesap bilgileri ekranının ara yüzünde başka müşterilerin bilgisini görebildiği, ihlalden etkilenen kişi sayısının 2686 olduğunun tahmin edildiği,
- İlgili kişilerin veri ihlali ile ilgili olarak 0850 333 22 86 numaralı çağrı merkezinden, DeFacto Müşteri Hizmetlerine ait destek@defacto.com.tr e-posta adresinden ve kvkk@defacto.com.tr e-posta adresinden bilgi alabilecekleri bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 21.09.2023 tarih ve 2023/1636 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

GÜNCEL HABERLER

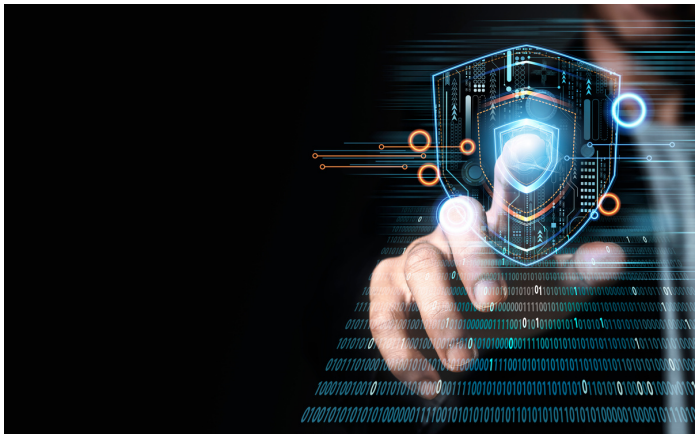
EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Suzuki Motorlu Araçlar Pazarlama A.Ş.

Veri sorumlusu sıfatını haiz Suzuki Motorlu Araçlar Pazarlama A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin Vodatech Bilişim Proje Danışmanlık Sanayi ve Dış Ticaret AŞ (Vodatech) sunucularına yapılan siber saldırı sonucu depolama aygıtlarında bulunan verilerin şifrelenmek suretiyle erişilemez duruma gelmesiyle gerçekleştiği,
- İhlalin 25.07.2023 tarihinde meydana geldiği ve 31.07.2023 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun henüz bilinmediği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin henüz tespit edilemediği bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.09.2023 tarih ve 2023/1599 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.



Trend Otomotiv Ticaret Hizmet ve Teknoloji Anonim Şirketi

Trend Otomotiv Ticaret Hizmet ve Teknoloji Anonim Şirketi tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- İhlalin Vodatech Bilişim Proje Danışmanlık Sanayi ve Dış Ticaret AŞ (Vodatech) sunucularına yapılan siber saldırı sonucu depolama aygıtlarında bulunan verilerin şifrelenmek suretiyle erişilemez duruma gelmesiyle gerçekleştiği,
- İhlalin 25.07.2023 tarihinde meydana geldiği ve 31.07.2023 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi grubunun henüz bilinmediği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İhlalden etkilenen kişisel veri kategorilerinin henüz tespit edilemediği bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 14.09.2023 tarih ve 2023/1600 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sitesinde ilan edilmesine karar verilmiştir.

GÜNCEL HABERLER

EYLÜL AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Hotiç Ayakkabı San. ve Tic. A.Ş.

Veri sorumlusu sıfatını haiz olan Hotiç Ayakkabı San. ve Tic. A.Ş. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusu tarafından SMS ile e-posta gönderimleri için oluşturulan izin yönetimi platformu ile ilgili olarak veri işleyenden hizmet alındığı,
- Bu platform üzerinde veri sorumlusuna tanımlı hesaba 23.06.2023 tarihinde yetkisiz kişiler tarafında giriş yapılmaya çalışıldığı ve müşterilerin cep telefonu bilgilerine erişildiği,
- İlgili kişilere oltalama saldırısını hedefleyen içeriğin yer aldığı kısa mesaj gönderimlerinin gerçekleştirildiği,
- Veri sorumlusu çalışanlarının da bahse konu kısa mesaj gönderim gruplarında bulunması sebebiyle oltalama saldırısına yönelik kısa mesaj gönderiminin başlatılması ile olay anında durumdan haberdar olunduğu,
- İhlalden etkilenen kişi ve kayıt sayısının 1.926.889 olduğu,
- İhlalden etkilenen kişisel verilerin müşterilere ait cep telefonu bilgisi olduğu,
- İlgili kişilerin veri ihlali ile ilgili crm@hotic.com.tr e-posta adresinden veya 0850 288 44 82 numaralı çağrı merkezinden bilgi alabilecekleri ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 07.09.2023 tarih ve 2023/1575 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

GLOBAL GELİŞMELER

SUUDİ ARABİSTANDA KVK HAKKINDA YENİ KANUN YÜRÜRLÜĞE GİRDİ

Krallık, yasayı 16 Eylül 2021'de kraliyet kararnamesi ile çıkarmış ve orijinal yasanın Resmi Gazetede yayınlanmasının ardından uygulanması için 720 günlük ek süre tanımıştı. 27 Mart 2023'te yayınlanan başka bir kraliyet kararnamesi ile yasada beş değişiklik yapılmıştı. Tüm bunların ardından Suudi Arabistan'da KVKK yasası 14 Eylül itibariyle yürürlüğe girdi.

Bu kanunla beraber Suudi Arabistan'da veri toplama, işleme, ifşa etme ve koruma alanları düzenlenmiş, bireysel gizliliği korumayı amaçlayan ilk kapsamlı veri koruma düzenlemesi elde edilmiştir.

Yasanın işleme standartları, veri sahiplerinin hakları, ilgili kurumların işleme sırasındaki yükümlülükleri, veri egemenliği ve yasa hükümlerinin ihlal edilmesi durumunda verilecek cezalar hakkında ayrıntılı bir düzenleme getirilmiştir.

Kanun'un 10. maddesinde kontrol otoritesinin kişisel verileri yalnızca doğrudan sahibinden toplayabileceği ve verilerin ancak toplanma amacını gerçekleştirmek için işlenebileceği düzenlenmiş ayrıca kanunun 36. Maddesi ile yetkili makam başkanının kararıyla oluşturulan bir komisyona başvurarak, kanun hükümlerine ve idari düzenlemelere aykırılık halinde kanunda öngörülen ihlalleri inceleme ve ceza verme yetkisi verilmiştir.

KALİFORNİA MİLLETVEKİLLERİ ÇEVRİMİÇİ KİŞİSEL VERİLERİN SİLİNMESİNİ KOLAYLAŞTIRACAK YASA TASARISINI KABUL ETTİ

Kaliforniya milletvekilleri Eylül ayında, tüketicilerin tek bir taleple her veri işleyenden kişisel bilgilerini silmesini sağlayacak olan ve Silme Yasası olarak bilinen bir yasa tasarısını kabul etti. Bu yasa ile beraber Kaliforniya Gizliliği Koruma Ajansı Ocak 2026'ya kadar tüketicilerin tek bir taleple kayıtlarının silinmesini talep edebilmelerini sağlayacak alt yapıyı oluşturacak.

Bu yasa 2018'de Kaliforniya Tüketici Gizliliği Yasası ile kabul edilen ve tüketicilere işletmelerden kişisel verilerini silmelerini isteme hakkını ancak zorlu bir süreçle isteme hakkı veren kapsamlı bir veri gizliliği yasa tasarısını temel alarak geliştirildi.

Yasa tasarısına karşı hem işletmelerden hem reklamcılardan Kaliforniya'nın veriye dayalı ekonomisini yok edeceğini" dair yasaya karşı agresif bir şekilde lobi faaliyeti de yürütülmüştü.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

YENİ ZELANDA MAHREMIYET KOMİSYONERLİĞİ OFİSİ REHBER YAYIMLADI

Yeni Zelanda Mahremiyet Komisyonerliği Ofisi, ülkenin veri koruma yasasında düzenlenen Bilgi Gizliliği İlkeleri ile yapay zekânın ilişkilendirilmesine yönelik açıklamaların yer aldığı ve bu ilkelerin yapay zekâ teknolojisinden nasıl etkilendiğine yönelik pratik örneklerin sunulduğu bir rehber yayımladı.

Rehberde Yapay zeka, kalıp bulma veya sınıflandırma gibi akıllı davranışlar gibi görünen görevleri yerine getiren bilgisayar sistemlerini ifade eder şeklinde tanımlanırken, ileride meydana gelebilecek veri gizliliği ihlalleri hakkında beklentilerini açıkladılar.

Gizlilik Yasasının Yeni Zelanda'da yapay zeka araçlarını kullanan herkes için geçerli olmasının temel amaçları olduğu ifade edildi.

Bilgi Gizliliği İlkelerinin (IPP'ler), kişisel bilgileri nasıl topladığını, kullandığını ve paylaştığına ilişkin yasal gereklilikleri belirten rehberde, bu araçları kullanmadan önce, IPP'lerin nasıl çalıştıklarını yeterince anlaşılması gerektiği ortaya konuldu.

Yayımlanan bu rehberle beraber bu anlamanın kolaylaşacağına değinildi. Rehbere **buradan** ulaşabilirsiniz.

İRLANDA VERI KORUMA OTORITESI (DPC), GDPR'IN UYGULANMASININ İLK BEŞ YILINI İÇERECEK ŞEKİLDE 2018-2023 YILLARINA TEKABÜL EDEN DÖNEMDE ALINAN KARARLARA İLIŞKİN ÖZETLERİ İÇEREN BİR ÇALIŞMA YAYIMLANDI

İrlanda Veri Koruma Otoritesi (DPC), GDPR'ın uygulanmasının ilk beş yılını içerecek şekilde 2018-2023 yıllarına tekabül eden dönemde alınan kararlara ilişkin özetleri içeren bir çalışma yayımlandı. Kitapçıkta çok çeşitli konularda incelemeler yapılırken.

Bunlardan bazıları Erişim talebi şikayetleri, sınır ötesi şikayetler, veri ihlal bildirimleri, açıklama/yetkisiz açıklama, elektronik doğrudan pazarlama, veri silinmesi, kolluk kuvvetleri direktifleri (LED), veri işlemeye itiraz, amaç sınırlaması ve şeffaflık konularıdır. Çalışma da 126 adet vaka incelemesi bulunmaktadır.

Rapor da Veri Koruma Komisyonu'nun (DPC) misyonunu verilerin tutarlı bir şekilde işlenmesinin sağlanması olduğunu belirten rapor. Veri korumasının nasıl sağlandığını, yasanın nasıl uygulandığını, uygunsuzlukların nasıl tespit edildiğini ve düzeltici tedbirlerin nasıl uygulanacağı hakkında bilgiler vermektedir.

Rapor da İşlemenin yasal dayanağı ve işlemenin güvenliği, Sınır ötesi şikayetlerde dostane çözüm yolları (Google YouTube) ve Grup postası yoluyla ifşa edilen e-posta adresleri hakkında verilen kararlar dikkat çeken bazı kararlar olarak öne çıkmaktadır.

İlgili çalışmaya **buradan** ulaşabilirsiniz.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

AVRUPA VERİ YÖNETİŞİMİ YASASI (EUROPEAN DATA GOVERNANCE ACT) UYGULANMAYA BAŞLADI

03.06.2022 tarihli Avrupa Birliği Resmî Gazetesi'nde yayımlanan Avrupa Veri Yönetişim Yasası "Yasa" Avrupa veri stratejisinin önemli bir dayanağı olan Veri Yönetişim Yasası, veri paylaşımına olan güveni artırmayı, veri kullanılabilirliğini artırmaya yönelik mekanizmaları güçlendirmeyi ve verilerin yeniden kullanılmasının önündeki teknik engellerin üstesinden gelmeyi amaçlıyor.

Yasasa aynı zamanda sağlık, çevre, enerji, tarım, mobilite, finans, imalat, kamu yönetimi ve benzeri sektörlerde hem özel hem de kamu aktörlerini içeren stratejik alanlarda ortak Avrupa veri alanlarının kurulmasını ve geliştirilmesini destekleyecektir.

Yasa geniş kapsamlı önlem aracılığıyla güvenilir veri paylaşım sistemlerinin geliştirilmesini destekleyecektir. Şöyle ki;

1. Açık veri olarak kullanıma sunulamayan belirli kamu sektörü verilerinin yeniden kullanımını kolaylaştıracak mekanizmalar. Örneğin, sağlık verilerinin yeniden kullanılması, nadir veya kronik hastalıklara tedavi bulma amaçlı araştırmaları ilerletebilir.
2. Veri aracılarının, ortak Avrupa veri alanları içerisinde veri paylaşımı veya havuzlama konusunda güvenilir düzenleyiciler olarak işlev görmesini sağlayacak önlemler.
3. Vatandaşların ve işletmelerin verilerini toplumun yararına sunmalarını kolaylaştıracak önlemler.
4. Veri paylaşımını kolaylaştıracak, özellikle verilerin sektörler ve sınırlar arasında kullanılmasını ve doğru verinin doğru amaç için bulunmasını sağlayacak önlemler.

Yasa kapsamı dahilindeki kuruluşlar açısından 24/09/2023 tarihinde uygulanmaya başlandı. Yasaya **buradan** ulaşabilirsiniz.

GDPR ŞİKAYETİ SONUCU POLONYA CHATGPTYE KARŞI GİZLİLİK SORUŞTURMASI BAŞLATTI

Geçtiğimiz ay Polonya'da ChatGPT ve OpenAI'ye karşı, şirketi AB'nin Genel Veri Koruma Yönetmeliğini (GDPR) bir dizi ihlal etmekle suçlayan bir şikâyette bulunulmuştu. Bunun üzerine Polonyalı yetkililer 20/09/2023 tarihinde bir adım atarak soruşturma başlattığını doğrulayan bir kamuoyu duyurusu yaptı.

Kişisel Verileri Koruma Kurumu'na iletilen şikayette ayrıca şirketin şikayetçiye yönelik bilgilendirme yükümlülüğünü yerine getirmediği belirtiliyor. Bu kişinin verileri 2021 yılında elde edildi. Şikayetçiye göre, elde edilen verilerin yapay zeka dil modellerinin eğitim amaçlı işlenmesi aşamasında bilgilendirme yükümlülüğünün yerine getirilmesi gerekmektedir. Şirket, şikayetçiye kendisiyle ilgili verilerin kaynağı veya bu verilerin alıcıları veya alıcı kategorileri hakkında bilgi vermedi.

Kişisel Verileri Koruma Dairesi Başkan Yardımcısı Jakub Groszkowski, vrupa kişisel veri koruma makamlarının görevinin Avrupa Birliği vatandaşlarını bilgi işleme teknolojilerinin olumsuz etkilerine karşı korumak olduğunu vurguluyor.

Şikayette dile getirilen iddiaların, OpenAI'nin Avrupa kişisel veri koruma kurallarına sistemik yaklaşımı hakkında şüpheler uyandırdığını ekliyor. Bu nedenle Ofis, bu şüpheleri, özellikle GDPR'de yer alan tasarım gereği gizlilik temel ilkesinin arka planına karşı açıklığa kavuşturacaktır.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

DANİMARKA VERI KORUMA OTORİTESİ, ÇALIŞANLARIN KİŞİSEL VERİLERE YETKİSİZ ERİŞİMLERİNİN ÖNLENMESİNE YÖNELIK BİR REHBER YAYIMLADI

Danimarka Veri Koruma Otoritesi, çalışanların kişisel verilere yetkisiz erişimlerinin önüne geçilmesine yönelik bir rehber yayımladı.

Rehberde, düzenlemelere uyum sağlandığından emin olmak için şirketlerin bir risk değerlendirmesi gerçekleştirmeleri, yalnızca iş ile ilgili bir ihtiyaç olduğunda çalışanların bu verilere erişim sağlayabilmeleri, çalışanların kişisel veri kullanımlarının kaydedilmesi ve çalışanların kişisel veri içeren sistemleri kullanımının sürekli şekilde izlenmesi gibi kontrol önlemlerinin uygulanması yönünde tavsiyelerde bulunulmaktadır.

Rehber de birçok kamu kurumunun elinde Bilgi Sistemlerinin bulunduğu ve bu sistemler aracılığıyla birçok verinin işlendiğini belirtildi, veri güvenliği için çalışanların düzensiz aralıklarla ve kamu yetkililerince sık sık denetlenmesi gerektiğini tavsiye etmektedir.

Bu kişisel verilere erişimi olan çalışanların sık sık işten ayrılması yahut departman değişmesi gibi durumların yaşandığını belirten rehber, çeşitli öneriler ile bu çalışanların bu verilere erişiminin departmanları ile sınırlı kalmasının yollarını göstermiştir. Birden fazla kişinin erişimi olan verilerin sınırlandırılması yahut maaş bordro sistemi tarzı öneriler rehberde yer almaktadır.

Rehber de Bilgi Teknolojileri sistemlerinde çalışanların hareketlerini denetlenmesinin önemi vurgularken bunun yolları hakkında bilgi verilmektedir.

Sistemlerde çalışanların hareketlerinin günlük olarak kaydedilmesi ve yeterli süre boyunca saklanması tavsiye edilmektedir.

Son olarak yaptırım konusunda rehber de Çalışanların haksız paylaşımlarda bulunmamasını sağlama sorumluluğu hem kuruma hem de bireysel çalışana aittir ifadesine yer verilerek hem bireysel hem kurumsal bir sorumluluk benimsendi. Tüm bu önlemlere rağmen çalışanlarca gizlice öğrenilen veriler için para cezaları da öngörülmektedir.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

GLOBAL GELİŞMELER

BİRLEŞİK KRALLIK VERİ KORUMA OTORİTESİ TARAFINDAN YAYIMLANAN ÇOCUK GÜVENLİĞİ BİLGİ PAYLAŞIM KLAVUZU

Birleşik Krallık Veri Koruma Otoritesi (ICO) tarafından çocukları ve gençleri fiziksel, duygusal veya zihinsel zararlardan korumak üzere bilgi paylaşımına yönelik on adımlı bir kılavuz yayımlandı.

Kılavuz çocukların korunması amacıyla kişisel bilgilerin paylaşılması sırasında veri korumayla ilgili hususlara ilişkin 10 adımdan oluşmaktadır. Adımlar sırasıyla şöyle düzenlenmiştir;

Adım 1: Veri korumanın, bir çocuğu korumak için bilgi paylaşmanıza nasıl yardımcı olabileceği konusunda net olun.

Bir çocuğu veya genci korumak için gerekli olan bilgilerin paylaşılmaması daha zararlı olabilir. Bir çocuğu korumak için ihtiyaç dahilindeki olan tüm bilgileri uygun bir kişi veya makamla paylaşmak hiçbir zaman Birleşik Krallık veri koruma yasasını ihlal etmeyecektir.

Adım 2: Bilgi paylaşma hedefinizi belirleyin ve bir çocuğu korumak için ihtiyaç duyduğunuz bilgileri paylaşın.

Bir çocuğun korunması için bilgi paylaşımı zorlayıcı bir neden olarak kabul edilmiştir. Bu kapsamda çocuğun korunmasında ihtiyaç olunan tüm bilgiler uygun kişi veya makamla paylaşılmalıdır.

Adım 3: Bilgi paylaşımına yönelik açık ve güvenli politikalar ve sistemler geliştirin.

Bilgilerin işlenmesi ve paylaşılması konusunda 'tasarım gereği ve varsayılan olarak veri koruma' yaklaşımını izlenmelidir.

Bilgilerin güvenli bir şekilde paylaşılması için kuruluşların bir uyumluluk kültürü ve iyi uygulama oluşturması gerekmektedir.

Adım 4: Şeffaflık ve bireysel haklar konusunda net olun.

İnsanlara bilgilerinin nasıl ve neden kullanıldığını anlatılması ve onlara gizlilik bilgilerinin verilmesi gerekmektedir.

Herhangi bir paylaşım düzenlemesinde, kişilerin veri koruma kanunu kapsamında bireysel haklarını kullanmalarına olanak tanıyan politika ve prosedürlere sahip olunmalıdır.

Adım 5: Riskleri değerlendirin ve gerektiğinde paylaşın.

Bir çocuk hakkında bilgi paylaşmaya karar verirken riskleri değerlendirmek çok önemlidir. Düzenli olarak veri paylaşan kuruluşların Veri Koruma Etki Değerlendirmesi aracılığıyla bilgi paylaşımını planlamada ve çocukların haklarına ve özgürlüklerine yönelik riskleri değerlendirmede ve azaltmada önlemler alması gerekmektedir.

Adım 6: Bir veri paylaşım sözleşmesi yapın.

Zorunlu olmasa da veri paylaşım sözleşmesi yapılması tavsiye edilir.

Adım 7: Veri koruma ilkelerini takip edin.

Yedi veri koruma ilkesi, veri korumanın merkezinde yer alır; Kişisel bilgiler kullanılırken veya paylaşılırken veri koruma ilkelerine dikkat edilmelidir.

- Hukuka uygunluk, adalet ve şeffaflık
- Amaç sınırlaması
- Veri minimizasyonu
- Doğruluk
- Depolama sınırlaması
- Bütünlük ve gizlilik
- Sorumluluk

Adım 8: Bilgileri doğru yasal dayanağı kullanarak paylaşın.

Adım 9: Acil durumda bilgileri paylaşın.

Acil bir durumda, bir çocuğu korumak için bilgilerinin paylaşılması önem arz edebilir. Olağan süreçlerin tamamını takip edecek zaman olmayabilir. Bu durumlar için önceden planlamalar yapılması gerekmektedir.

Adım 10: Veri paylaşım mevzuatını okuyun.

GLOBAL GELİŞMELER

HONG KONG VERİ KORUMA OTORİTESİ VERİ İHLALLERİNE İLİŞKİN BİLGİ NOTU YAYIMLADI

Hong Kong Veri Koruma Otoritesi, kuruluşlar bünyesinde gerçekleşen veri ihlallerinin ele alınması ve veri ihlal bildirimlerine ilişkin yol gösterilmesi amacıyla rehber nitelikte bir bilgi notu yayımladı.

Hong Kong Veri Koruma Otoritesi tarafından 22/09/2023 tarihli medya açıklamasında son zamanlarda kuruluşların bilgi sistemlerine yönelik kişisel verilerin sızmasını içeren art arda hacker saldırılarına dikkat çekti.

PCPD, kişisel verileri elinde bulunduran kuruluşların düzenli olarak veri güvenliği risk değerlendirmeleri yapmalarını ve kontrolü veya mülkiyetindeki bilgi ve iletişim sistemlerini ve kişisel verileri korumak için, verilerin niteliğine, ölçeğine ve karmaşıklığına bağlı olarak yeterli ve etkili güvenlik önlemlerini uygulamaya koymasını tavsiye etmektedir. Kurum tarafından verilen tavsiyeler aşağıdaki gibidir;

- Bilgisayar ağlarını korumak için güvenlik duvarları ve/veya kötü amaçlı yazılım önleme uygulamaları gibi güvenlik cihazlarının veya yazılımlarının kullanılması. Yazılımlar (mobil uygulamalar ve kötü amaçlı yazılımdan koruma uygulamaları dahil) yeni virüsleri ve ortaya çıkan tehditleri tespit edecek şekilde düzenli olarak güncellenmelidir;
- Özellikle internete bağlanan sistemler için düzenli olarak güvenlik açığı değerlendirmeleri ve sızma testleri gerçekleştirilmelidir;
- Güvenlik açıklarını zamanında düzeltmek için yama yönetimi uygulanmalıdır;
- Aktarılan ve depolanan verilerin şifrelenmesi ve şifreleme anahtarlarının etkin yönetimi ve korunması;
- Veritabanı yönetimi: Web sunucularının ele geçirilmesi durumunda dahili sunucuları korumak için veritabanı sunucularını web sunucularından güvenlik duvarlarıyla ayırmak;
- Bir görevi tamamlamak ve kullanıcılara uygun roller atamak için mümkün olduğunca az erişim hakkı vermek üzere "en az ayrıcalık" ilkesini benimsenmelidir (erişilecek veri hacminin ve erişim süresinin kısıtlanması dahil);
- Gereksiz veya süresi dolmuş kişisel verilerin zamanında imha edilmelidir.

Bununla beraber Veri güvenliği sistemini güçlendirmek amacıyla PCPD, veri kullanıcılarına önerilen veri güvenliği önlemlerini sağlamak amacıyla Ağustos 2022'de "Bilgi ve İletişim Teknolojileri için Veri Güvenliği Önlemlerine İlişkin Kılavuz Notu"nu (**Kılavuz Notu**) yayınladığını hatırlatmıştır.

Son olarak bilgi notunda Kurum, kuruluşlara herhangi bir veri ihlali olayını mümkün olan en kısa sürede Kuruma bildirmelerini şiddetle tavsiye etmiştir. Bir veri ihlali olayının erken bildirilmesi, Kurumun kuruluşa ve etkilenen taraflara, olayın kuruluşa ve etkilenen taraflara verdiği zararı en aza indirmek için uygun ve zamanında önlemler almasına yardımcı olmasını sağlayacaktır.

Kuruluşların ayrıca herhangi bir veri ihlali vakasını etkilenen veri sahiplerine mümkün olan en kısa sürede bildirmeleri önemle tavsiye edilmiştir.

GLOBAL GELİŞMELER

YAPAY ZEKÂ YASASI'NDA YAPAY ZEKÂNIN SİBER GÜVENLİĞİ ÇALIŞMASI

Avrupa Komisyonunun Ortak Araştırma Merkezi (JRC) tarafından hazırlanan "Yapay Zekâ Yasası'nda Yapay Zekânın Siber Güvenliği" başlıklı çalışmada, yüksek riskli yapay zekâ sistemleri için siber güvenlik gereksinimlerinin karşılanmasına yönelik yol gösterici ilkeler ele alınmaktadır.

Önerilen Yapay Zekâ Yasası, yapay zekâ sistemlerine odaklanıyor. Yapay zekâ modelleri yapay zekâ sistemlerinin temel bileşenleri olmasına rağmen tek başına yapay zekâ sistemleri oluşturmazlar.

Yapay Zekâ Yasası siber güvenlik gereklilikleri, doğrudan iç bileşenleri için değil, bir bütün olarak yapay zekâ sistemi için geçerlidir.

Uyumluluğun sağlanması için sistemin tasarımı dikkate alınarak güvenlik riski değerlendirmesi yapılmalı, riskler belirlenmeli ve gerekli azaltıcı önlemler uygulanmalıdır.

Bu süreç, kanıtlanmış siber güvenlik uygulamaları ve prosedürlerini yapay zekaya özgü kontrollerle birleştiren bütünleşmiş ve sürekli bir yaklaşım gerektirir.

Bu bağlamda, YZ Yasası özel bir önem taşımakta ve YZ sistemlerinin aşağıdakileri sağlamada çok önemli bir unsur haline gelmektedir yüksek riskli senaryolarda güvenli bir şekilde kullanılmakta ve temel haklara saygı göstermektedir. Bu rapor şu konulara odaklanmaktadır Yönetmeliğin 15. Maddesinde belirtildiği üzere, yüksek riskli YZ sistemleri için siber güvenlik gerekliliği. Sonuç olarak bu gerekliliğin uygulanmasına ilişkin gerçekleştirilen üst düzey analiz aşağıdaki dört yol göstericidir ilkeler aşağıda özetlenmiştir:

- YZ Yasası'nın odak noktası YZ sistemleridir. YZ sistemlerinin yapısı, bir dizi dahili Bazıları YZ ile ilgili olan, bazıları ise olmayan bileşenler. YZ modelleri gerekli olmasına rağmen YZ sistemlerinin bileşenleri, kendi başlarına YZ sistemlerini oluşturmazlar. Siber güvenlik YZ Yasası tarafından belirlenen gereklilikler, doğrudan YZ sisteminin kendi iç işleyişine değil, bir bütün olarak YZ sistemine uygulanır.
- YZ Yasası ile uyumluluk mutlaka bir güvenlik riski değerlendirmesi gerektirir. Bunun için Bir YZ sisteminin YZ Yasası'nın siber güvenlik gerekliliklerine uymasını sağlamak, bir güvenlik riski değerlendirme, YZ sisteminin iç mimarisi ve aşağıdaki hususlar dikkate alınarak yapılmalıdır.
- Yapay zekâ sistemlerinin güvenliğini sağlamak, kanıtlanmış yöntemler kullanarak entegre ve sürekli bir yaklaşım gerektirir. Bu süreç, mevcut siber güvenlik uygulamalarından yararlanmalıdır
- YZ modellerinin güvenliğini sağlamak için son teknolojinin sınırları vardır.

Çalışmada, mevcut YZ ortamında farklı olgunluk derecelerine sahip teknolojiler bir arada bulunmaktadır. Tüm yapay zekâ teknolojilerinin yüksek riskli senaryolarda kullanılmak üzere tasarlanmış YZ sistemlerinde kullanıma hazır olabileceği düşünülmektedir.

Gelişmekte olan yapay zekâ teknolojileri için, yalnızca şu anda ele alınamayacak doğal sınırlamalar bulunduğu, bu durumlarda, YZ Yasasının siber güvenlik gerekliliklerine uyumu ancak daha önce açıklanan bütüncül yaklaşımların izlenerek hareket edilebileceğine değinilmiştir.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership