SAYI: 29

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

KVK & SİBER GÜVENLİK BÜLTENİ

HAZİRAN 2023

GÜNCEL HABERLER

- Haziran Ayında Yayımlanan Veri İhlal Bildirimleri Yayımlandı
- Kişisel Verileri Koruma Kurulu Tarafından Kamuoyu Duyurusu Yayımlandı
- KVKK Akademi Derleme Çalışması Yayımlandı
- Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Tarafından Chatbot Uygulaması ve ChatGPT Örneği Değerlendirme Raporu Yayımlandı

GLOBAL GELİŞMELER

- Avrupa Veri Koruma Kurulu İdari Para Cezalarının Hesaplanmasına İlişkin Kılavuz İlkeleri Kabul Etti
- Birleşik Krallık Veri Koruma Otoritesi Gizliliği Artıran Teknolojilere İlişkin Bir Rehber Yayımladı
- Japonya Kişisel Verileri Koruma Komisyonu OpenAI'yi Kişisel Veriler Konusunda Uyardı
- Amerika Birleşik Devletleri'nde Önde Gelen Bir Hukuk Bürosu OPENAI'ya Dava Açtı
- ABD'de 769 bin emeklinin kişisel verileri ele geçirildi
- Danimarka hükümeti, Google, Snapchat ve Meta gibi teknoloji şirketlerinin kişisel verileri toplamasında yaş sınırını yükseltmeyi planladığını açıkladı
- İrlanda Veri Koruma Komisyonu, Bard Chatbot'unun AB Lansmanını Gizlilik Endişeleri Nedeniyle Ertelemek Zorunda Kaldı

İŞE ALIM FAALİYETLERİNDE DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Kişisel Verilerin Korunmasına ilişkin mevzuat düzenlemeleri ve Kişisel Verileri Koruma Kurulu'nun yerleşik kararları uyarınca , yetkililerin işe alım süreçlerini yürütürken veri minimizasyonu ilkesi de gözetilerek ihtiyaç doğrultusunda ve makul bir süre ile kişisel veri işlenmelidir. Buradaki ihtiyaç kriteri, yetkililerin kanaati doğrultusunda değil, hukuk kurallarına uygunluk kapsamında ölçülülük ve gereklilik ilkesine göre tespit edilmelidir. Bu sebeple adaylardan alınması elzem olmayan bilgilerin alınmaması ve ayrıca eşitsizlik ya da ayrımcılık iddialarına sebebiyet verecek kişisel verilerinin elde edilmemesi gerekmektedir (örneğin, kişinin T.C. Kimlik Numarası, araç tahsis edilme ihtimali bulunmayan kişilerin ehliyet bilgisinin,kan grubu, eşinin çalışma bilgilerinin alınması vb.)

Kanunda öngörülen işleme şartlarının bulunmaması halinde açık rıza ile her türlü kişisel verilerin işlenebileceği fikri hatalı ve hukuka aykırı sonuçlara sebebiyet vermektedir.
Açık rızanın geçerliliği hususunda Kurum, almış olduğu bir kararda işçi-işveren ilişkisinde, işçiye rıza göstermeme imkanının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda işçinin özgür iradesinin zedeleneceğinden bahisle veri işlemenin açık rızaya dayandırılamayacağına karar vermiştir.

İşe alımda kişisel veri elde edilecek hususlara aşağıdaki yanıtlara göre belirlenmelidir:
Söz konusu kişisel veri;
➢ Süreç için elde edilmesi zorunlu mudur? ➢ işe alım amacıyla bağlantılı mı?
➢ ilgili kişinin almak istediğimiz pozisyondaki görev tanımına uygunlukla alakalı mı?
➢ kişinin özel hayatıyla ilgili mi? ➢ kişinin kendisinden başka kişilere ilişkin mi?
➢ İş görüşmeleri aşaması yerine işe alım yapıldıktan sonra elde edilmesi halinde aynı amaca ulaşabilir miyiz?
Özetle, çalışan/stajyer adaylarından iş başvurusu ve/veya görüşme esnasında mümkün olduğunca minimum düzeyde kişisel veri elde edilmeli; özel nitelikli kişisel veriler elde edilmemeli, yalnızca kişinin alınacağı pozisyona uygunluk denetimi içeren, amacı aşmayan makul sorular sorulmalıdır.

HAZİRAN AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

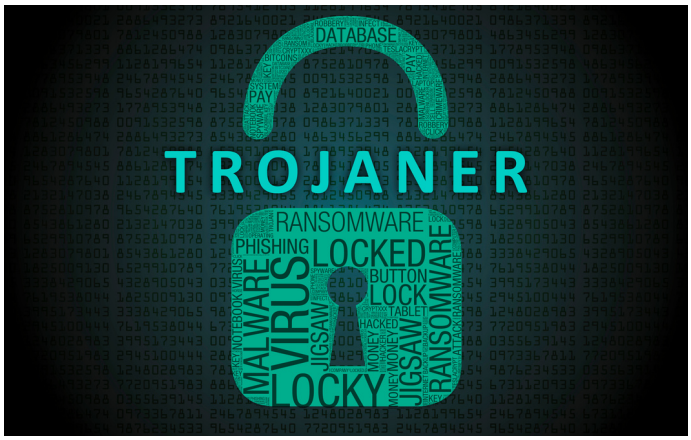
OSDS Su Arıtma Sistemleri San. Tic. Ltd. Şti

Veri sorumlusu sıfatını haiz OSDS Su Arıtma Sistemleri San. Tic. Ltd. Şti tarafından Kurula iletilen veri ihlal bildiriminde özetle:

- Veri sorumlusunun müşterilerine, dolandırıcılık amaçlı olduğu düşünülen ve bir link içeren SMS gönderildiği; söz konusu SMS'lerin gönderim tarihlerinin 26-27 Mayıs 2023 olduğu,
- MAS GSM Haberleşme A.Ş.'nin veri sorumlusunun veri işleyeni pozisyonunda olduğu,
- Yetkisiz kişiler tarafından 45.228 adet SMS gönderildiği ve SMS gönderilen numaraların birçoğunun veri sorumlusu müşterisi olduğu,
- İhlalden etkilenen kişisel verilerin iletişim, lokasyon, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, pazarlama ve ceza mahkumiyeti ve güvenlik tedbirleri olduğu,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler ve potansiyel müşteriler olduğu

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.06.2023 tarih ve 2023/973 sayılı Kararı ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.



Bilge Adam Yazılım ve Teknoloji A.Ş.

Veri sorumlusu sıfatını haiz Bilge Adam Yazılım ve Teknoloji A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

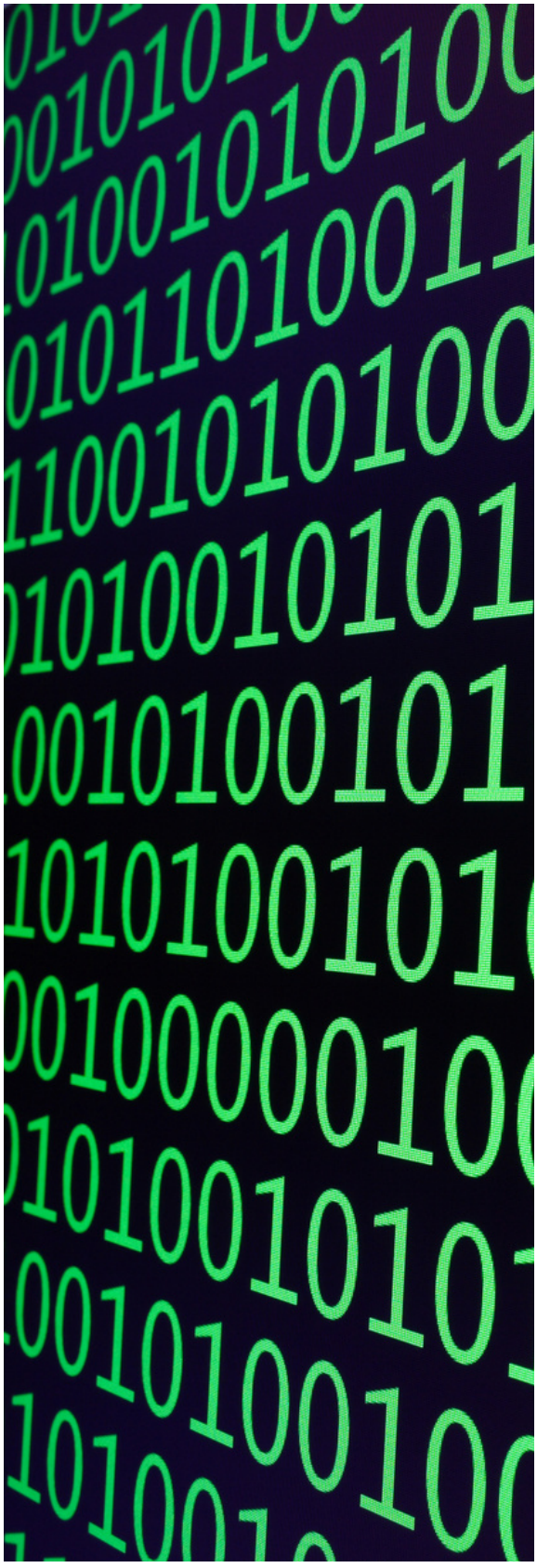
- Veri sorumlusuna karşı gerçekleştirilen oltalama saldırısı neticesinde veri sorumlusunun 3 personelinin bilgisayarına erişildiği ve bu bilgisayarların fidye yazılımı ile şifrelendiği,
- Yetkisiz erişim sağlanan bilgisayarlarda çalışan ve çalışan adaylarına ait verilerin tutulduğu,
- İhlalden etkilenen kişisel verilerin ad, soyad, TC kimlik numarası ve işyeri sicil numarası olduğu,
- İhlalden etkilenen kişi ve kayıt sayısının henüz tespit edilemediği,
- İlgili kişilerin çağrı merkezi ve e-posta aracılığıyla veri ihlali hakkında bilgi alabileceği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.06.2023 tarih ve 2023/975 sayılı Kararları ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

HAZİRAN AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Arçelik A.Ş.



Veri sorumlusu sıfatını haiz Arçelik A.Ş. tarafından Kurula iletilen veri ihlal bildiriminde özetle;

- Veri sorumlusunun anlaşmalı olduğu bayi ve yetkili servis çalışanlarının satış hedefleri kapsamında ek menfaat niteliğinde ödül kazandıkları, Arçelik Bizbize mobil uygulama ve internet sitesinin barındırıldığı tedarikçi sistemlerinde tespit edilen bir güvenlik zafiyeti dolayısıyla kişisel verilere yetkisiz erişim sağlandığı,
- İlgili sistemlerin kod ve mülkiyet sahipliğinin veri işleyende bulunduğu, veri sorumlusunun yalnızca kullanım imkanına sahip olduğu bir modelle hizmet aldığı,
- Yetkisiz kişiler tarafından admin paneline erişim sağlandığı ve Almanya'da görünen bir IP adresine kişisel verilerin alındığının tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının bayi ve yetkili servis çalışanları olduğu,
- İhlalden etkilenen kişisel verilerin Kimlik (ad, soyadı, TCKN, unvan, doğum tarihi, cinsiyet), İletişim (elektronik posta adresi, GSM numarası), İşlem Güvenliği (LDAP (Lightweight directory access protocol) kodu (verinin tutulması ve erişim doğrulaması için kullanılan koddur) ve kullanıcı şifresi, kayıt ve güncelleme tarihi, son giriş tarihi, hesabının aktiflik durumu, cihaz modeli, versiyonu ve işletim sistemi bilgisi, uygulama versiyon bilgisi, bildirim izin durumu), Diğer (sistem kapsamında, bayi ve yetkili servis çalışanlarının puan kazanım ve harcama bilgileri, uzmanlık, eğitim, işe başlama tarihi, ilgili kişinin şahsi bilgileri olmamakla beraber çalışmakta olduğu bayi ve mağazasının kodu, adı ve adresi) olduğu
- İhlalden etkilenen ilgili kişi sayısının tahmini 30.373 kişi olduğu,
- İlgili kişilerin veri sorumlusunun başvuru panelinden (https://privacyportal-eu.onetrust.com/webform/1ee6a6ce-9b09-49bd-b9e4-a3544706c63e/6361bf5f-8fd5-4af5-8c3a-6cd46cddca1b) bilgi alabilecekleri

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 01.06.2023 tarih ve 2023/978 sayılı Kararları ile söz konusu veri ihlal bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

HAZİRAN AYI İÇERİSİNDE BİLDİRİLEN KİŞİSEL VERİ İHLALLERİ

Tıp Evi Sağlık Hizmetleri Ticaret Limited Şirketi

Veri sorumlusu sıfatını haiz olan Tıp Evi Sağlık Hizmetleri Ticaret Limited Şirketi tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin 02.02.2023 tarihinde gerçekleştiği ve 17.04.2023 tarihinde tespit edildiği,
- İhlalin veri sorumlusunun anlaşmalı olduğu bir şirkete siber saldırı düzenlenmesi neticesinde gerçekleştiği,
- Söz konusu siber saldırı sonucu verilere ulaşılamadığı,
- İhlalden etkilenen kişi sayısının tam olarak bilinmediği,
- İhlalden etkilenen ilgili kişi gruplarının henüz bilinmediği,
- İhlalden özlük bilgileri ile özel nitelikli kişisel verilerden olan sağlık verilerinin etkilendiği

bilgilerine yer verilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 08.06.2023 tarih ve 2023/1023 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

KİŞİSEL VERİLERİ KORUMA KURULU TARAFINDAN KAMUOYU DUYURUSU YAYIMLANDI

İlgili duyuruda özetle aşağıdaki hususlardan bahsedilmiştir:

Kurulun görev ve yetkileri arasında; "…Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak", "Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak" ve "Bu Kanunda öngörülen idari yaptırımlara karar vermek…" bulunmaktadır.

Ayrıca, KV12. maddesi uyarınca "veri sorumlusunun;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu, (5) numaralı fıkrasında ise, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kuruluna (Kurul) bildireceği, Kurulun, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükme bağlanmıştır.

Veri sorumlularının, Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 Sayılı Kararı gereğince ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirme yükümlülüğü bulunmaktadır.

Veri ihlal bildirimlerinde, Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amaç, ilgili kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamaktır.

Veri sorumlusunun Kanunun 12 inci maddesinin (5) numaralı fıkrası gereğince bildirim yükümlülüğünü yerine getirmesinden sonra Kurul tarafından inceleme kararı alınabilmektedir.

Diğer taraftan Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda, görev alanına giren konularda Kanunun 15 inci maddesinin (1) numaralı fıkrası hükmü gereğince gerekli incelemeyi resen yapmaktadır.

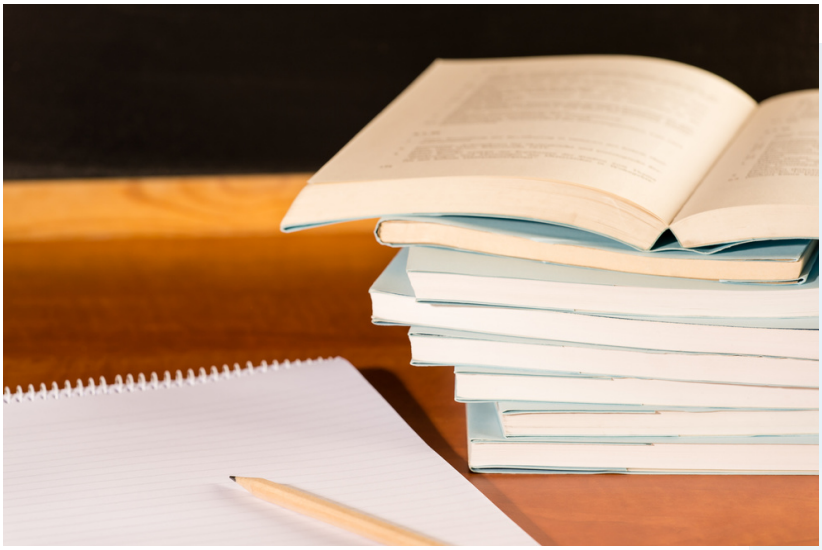
Dolayısıyla Kurul, bir kişisel veri ihlali durumunu inceleme konusu olarak ele alabilmesi için bu iki hususdan birinin gerçekleşmiş olmasını aramaktadır.

15 Haziran itibariyle Kurumumuza veri sorumlularından intikal eden 1001 adet veri ihlali bildiriminin yanında Kurul tarafından resen incelemeye alınan 107 adet veri ihlali ile birlikte toplam 1108 adet veri ihlali inceleme konusu bulunmaktadır. Bu inceleme konularının büyük çoğunluğu sonuçlandırılmıştır.

Muhtelif haber kanallarında ve sosyal medya platformlarında vatandaşların kişisel verilerinin kamu kurumlarından sızdırıldığına yönelik çeşitli haberler yer almış ancak Kurumumuza bugüne kadar konuya ilişkin olarak kamu kurumlarından intikal etmiş herhangi bir veri ihlali bildirimi bulunmamaktadır.

Konu hakkında medyada daha önce de benzer haberlerin yer alması sebebiyle Kişisel Verileri Koruma Kurulunun 09 Mart 2023 tarih ve 2023/341 sayılı kararı ile bu durum hakkında resen inceleme başlatılmış olup ilgili kamu kurumları ile koordineli bir şekilde çalışmalara devam edilmektedir.

KVKK AKADEMİ DERLEME ÇALIŞMASI YAYIMLANDI



Teknolojinin ve dijital hizmetlerin hızla gelişmesiyle, kişisel verilerin işlendiği sektörler ve faaliyet alanları artmış, bu yeni alanlarda kişisel verilerin korunmasına ilişkin yeni bakış açıları ortaya koyma gerekliliği ortaya çıkmıştır. Bu doğrultuda Kurum tarafından, kişisel verilerin korunması hukukunu çeşitli boyutlarıyla değerlendiren, alanlarında uzman akademisyenlerin eserlerinden oluşan "Kişisel Verilerin Korunmasına Akademik Bakış: KVKK Akademi Derleme Çalışması" isimli kitap yayımlanmıştır.

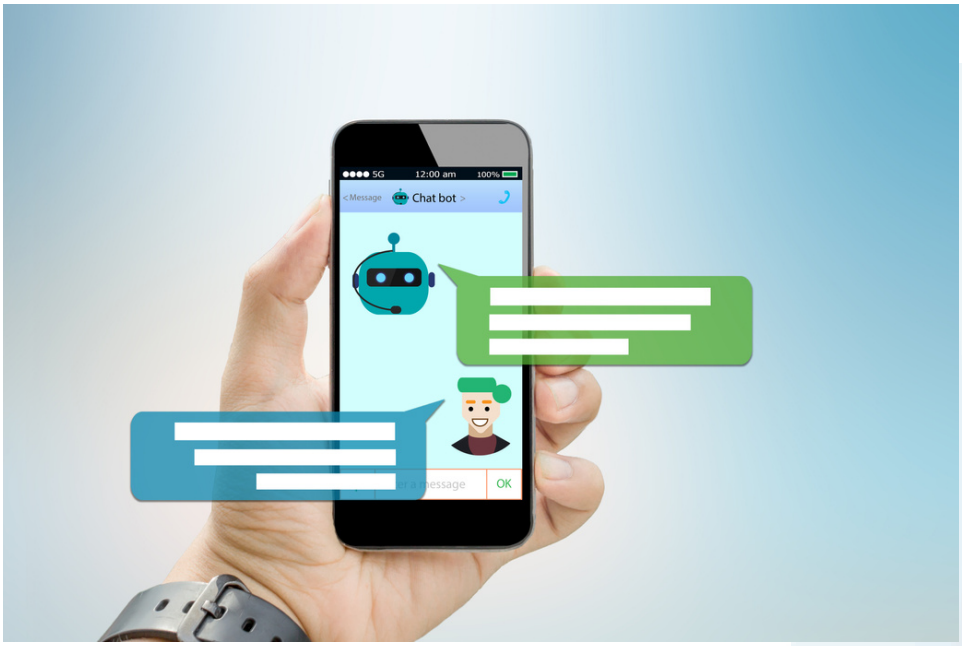
Kişisel verilerin korunması, mahremiyet, veri koruma hukuku ve kişisel verilerin güvenliği ile ilgili çalışmaların yer aldığı kitapta:

- Kişisel Verilerin Korunması Hakkı
- Kişisel Verilerin Korunması ve Etik
- Genel Kavramlar
- Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler
- Açık Rıza
- İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması Yükümlülüğü
- Başvuru ve Şikâyet Usulleri ile Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü
- Kişisel Verilere İlişkin Suçlar
- Güncel Teknoloji ve Kişisel Veri
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi
- Sürdürülebilir Kişisel Veri Güvenliği Yönetişimi
- Blokzinciri ve Kişisel Verilerin Korunması
- Yapay Zekâda Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler
- Medeni Hukuk İlişkilerinde Kişisel Verilerin Korunması
- Fikri Mülkiyet Alanında Kişisel Verilerin İşlenmesi
- Medenî Usul Hukuku Çerçevesinde Kişisel Verilerin Korunması
- İş Hukukunda Kişisel Verilerin İşlenmesi
- Sağlık Sektöründe Kişisel Verilerin İşlenmesi

başlıklı eserler, kişisel verilerin korunması alanına katkı sağlamak üzere ilgililerin kullanımına sunulmuştur.

İlgili çalışmaya buraya tıklayarak erişim sağlayabilirsiniz.

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI DİJİTAL DÖNÜŞÜM OFISI TARAFINDAN CHATBOT UYGULAMASI VE CHATGPT ÖRNEĞI DEĞERLENDİRME RAPORU YAYIMLANDI



Yayımlanan raporda, chatbot uygulamalarının türleri ve tarihçesi, chatbotların kullanım amaçları, chatbotların faydaları, güvenlik riskleri, chatbotlarda güvenlik, gizlilik ve veri koruma gibi önemli hususlara ilişkin açıklamalara yer verilmiştir.

Kişisel veriler bakımından yapılan değerlendirmede özetle şu hususlara değinilmiştir:

Güvenlik sorunları, güvenlik tehditleri ve güvenlik açıkları olmak üzere iki ana kategoriye ayrılmaktadır. Güvenlik tehdidi, bir kuruluşun ve sistemlerinin tehlikeye atılabileceği bir risktir. Bilgisayar güvenliği tehditleri ise “STRIDE” modeli; sahte e-posta , onaysız değişiklik , reddetme, bilgi ifşası, hizmet reddi, ayrıcalıkların kaldırılması ile tanımlanmaktadır. Güvenlik tehditleri; güvenilirlik, bütünlük, reddedilemezlik, gizlilik, kullanılabilirlik, yetkilendirme gibi aşağıda açıklanan özellikleri karşılayan koruyucu mekanizmalarla azaltılabilmektedir. Sistem açıkları, saldırganlar tarafından bir bilgisayar sistemi içinde yetkisiz eylemler gerçekleştirmek için kullanılabilecek zayıflıklardır.

Birçok chatbot, verileri depolamak amacıyla tehditlerin ve güvenlik açıklarının iyi derecede ele alındığı bulut bilişim hizmetlerini kullanarak metin iletişim konusuna ve veri manipülasyonunun farklı yönlerine odaklanmaktadır. Güvenli mesajlaşma iki alana ayrılmaktadır. İlk alan; veri aktarımlarındaki güvenlikle yani mesajların, seslerin ve görüntülerin chatbot’un barındırıldığı bir sunucuya güvenli bir şekilde aktarılmasıyla ilgilidir. İkinci alan ise; sunucudaki (arka uç) verilerin işlenme, depolanma ve paylaşılma teknikleri ile ilgilenmektedir. Herhangi bir şirket bir kullanıcının verilerini işliyorsa, aşağıda açıklanan yöntemlerin çoğunun uygulanması gerekmektedir. Belirtilen yöntemler, bir internet tarayıcısında veya mobil uygulamada açılır sohbet penceresi gibi chatbot ile yapılan her türlü iletişimi kapsamaktadır:

1) Kimlik Doğrulama ve Yetkilendirme
2)Uçtan Uca Şifreleme
3)Kendi kendini imha eden mesajlar
4)Kullanıcı İletişim Verileri, Arka Uç Tarafı

GLOBAL GELİŞMELER

AVRUPA VERİ KORUMA KURULU İDARİ PARA CEZALARININ HESAPLANMASINA İLİŞKİN KILAVUZ İLKELERİ KABUL ETTİ

Avrupa Veri Koruma Kurulu (“ EDPB ”), 7 Haziran 2023 tarihinde, halkla gerçekleştirilen istişarenin ardından, veri koruma yetkililerinin kullandığı metodolojiyi uyumlu hale getirmeyi amaçlayan GDPR kapsamındaki idari para cezalarının hesaplanmasına ilişkin Kılavuz İlkeleri’nin son halini kabul etmiştir. EDPB özellikle, para cezalarının hesaplanması için üç unsuru dikkate almaktadır; ihlallerin doğasına göre sınıflandırılması, ihlalin ciddiyeti ve ihlali gerçekleştiren işletmenin cirosu. Kılavuz İlkeler’e idari para cezalarının hesaplanmasına ilişkin beş aşamalı metodolojiyi özetleyen bir referans tablosu ve iki pratik uygulama örneğini içeren bir ek eklenmiştir. Kılavuz İlkeler, EDPB için stratejik bir öncelik olan sınır ötesi davalarda yerel veri koruma yetkililer ile daha verimli iş birliğinin kurulmasına önemli bir katkı sağlamayı hedeflemektedir.

JAPONYA KİŞİSEL VERİLERİ KORUMA KOMİSYONU OPENAI’Yİ KİŞİSEL VERİLER KONUSUNDA UYARDI

Japonya Kişisel Verileri Koruma Komisyonu (Personal Information Protection Comission Japan, “PPC”), ChatGPT sohbet robotunun arkasındaki girişim OpenAI’yi kullanıcıların izni olmaksızın hassas verileri topladığı gerekçesi ile uyardı. Yapılan açıklamada, yapay zekanın öğrenimi ve gelişimi için toplanan hassas verileri minimize etmesi gerektiğini ve önlemleri artırabileceğini söyledi. Komisyon, OpenAI’ya, kullanıcılara ilişkin hassas verileri onların açık rızası olmaksızın toplamaktan kaçınması gerektiğini belirtti.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership

AMERİKA BİRLEŞİK DEVLETLERİ’NDE ÖNDE GELEN BİR HUKUK BÜROSU OPENAI’YA DAVA AÇTI

Amerika Birleşik Devletleri’nin California eyaletindeki önde gelen bir hukuk bürosu, ChatPT’nin ana şirketi OpenAI’ya yapay zekâ teknolojisini eğitmek için bireylerin internet ortamında yer alan verilerinin seçilerek sayısız kişinin kişisel verilerini, fikri ve sınai haklarını ve mahremiyetini büyük ölçüde ihlal ettiğini iddia ederek federal mahkemede toplu bir dava açtı. Hukuk bürosunun yönetici ortağı OpenAI’nin “bu çok güçlü teknolojiyi yaratmak için bilgileri çalınan ve ticari olarak kötüye kullanılan gerçek kişileri” temsil etmek istediğini söyledi. Bu dava ile, şirketin yapay zeka algoritmalarının eğitim yöntemleri için yasal önlemler oluşturmayı ve verileri kullanılan kişiler için uygun tazminat sağlamayı amaçlanıyor.

BİRLEŞİK KRALLIK VERİ KORUMA OTORİTESİ GİZLİLİĞİ ARTIRAN TEKNOLOJİLERE İLİŞKİN BİR REHBER YAYIMLADI

Birleşik Krallık Veri Koruma Otoritesi (Information Commissioner’s Office, “ICO”), gizliliği artıran teknolojileri ve bu teknolojilerin pratikte uygulanmasına yönelik ayrıntılı bir kılavuz yayımladı. Kılavuz iki ana bölümden oluşturuldu. İlk bölümde gizliliği artıran teknolojilerin neler olduğu ve veri koruma yasasıyla nasıl ilişkilendirildikleri, faydaları, kullanmanın riskleri, türleri, anonimleştirme teknikleri gibi hususlara yer verildi. İkinci bölüm ise daha teknik bir kitleye ve şu anda mevcut olan gizliliği artıran teknoloji türleri hakkında daha fazla ayrıntıyı anlamak isteyen veri koruma yetkililerine yönelik hazırlandı ve diferansiyel gizlilik, sentetik veri, homomorfik şifreleme, sıfır bilgi kanıtları, güvenilir yürütme ortamları, güvenli çok taraflı hesaplama, özel küme kesişimi, federe öğrenme ve referans tablosu hususlarına yer verildi.

GLOBAL GELİŞMELER

ABD'DE 769 BİN EMEKLİNİN KİŞİSEL VERİLERİ ELE GEÇİRİLDİ

Kaliforniya Kamu Çalışanları Emeklilik Sistemi'nden yapılan açıklamaya göre, haziranda dosya aktarım aracı olan MOVEit Transfer'deki bir açıktan faydalanılarak yapılan siber saldırıdan birçok kişi ve kurumun etkilendiği anımsatıldı.

Söz konusu siber saldırıda, sistemin 769 bin üyesinin kişisel verileri ele geçirildi. Bunların arasında, ad-soyad, doğum tarihi, sosyal güvenlik numaraları ve aile üyelerinin adları gibi bilgiler yer alıyor.

Bu arada, kişisel verileri çalınan kişiler konuyla ilgili bilgilendirildi.

DANİMARKA HÜKÜMETİ, GOOGLE, SNAPCHAT VE META GİBİ TEKNOLOJİ ŞİRKETLERİNİN KİŞİSEL VERİLERİ TOPLAMASINDA YAŞ SINIRINI YÜKSELTMEYİ PLANLADIĞINI AÇIKLADI

Büyük teknoloji şirketlerinin konuyla ilgili daha fazla sorumluluk alması gerektiğini belirtilirken, "Şirketlerin çocukları ve yetişkinleri ekranın önünde tutmak ve akıl almaz miktarda kişisel veri toplamak için çılgınca yöntemler kullanan üstü kapalı algoritmalarına bir son vermeliyiz" ifadelerine yer verildi.

Bodskov, çocukların verilerinin Google, Snapchat ve Meta gibi teknoloji şirketleriyle paylaşılması için 13 olan yaş sınırını 15 veya 16'ya çıkarmayı planladıklarını belirtti.

Bakan Bodskov, hükümetin ayrıca reşit olmayan kullanıcıların pornografik içerik ve savaş videolarının izlenmesini en aza indirmek için yaş doğrulama önlemlerini uygulamaya koymayı planladığını kaydetti

Yaş sınırına yönelik yapılacak düzenleme kapsamında, teknoloji şirketlerinin çocukların verilerine ulaşabilmesi için ebeveynlerinden izin alması gerekecek.

İRLANDA VERİ KORUMA KOMİSYONU, BARD CHATBOT'UNUN AB LANSMANINI GİZLİLİK ENDİŞELERİ NEDENİYLE ERTELEMEK ZORUNDA KALDI

İrlanda Veri Koruma Komisyonu (Data Protection Commission Ireland, "DPC"), arkasında Google'ın olduğu Bard isimli sohbet robotunun Avrupa Birliği lansmanını gizlilik endişeleri nedeniyle ertelediğini bildirdi. Komisyon, Google tarafından Bard için herhangi bir ayrıntılı brifing veya bir veri koruma etki değerlendirmesi veya herhangi bir destekleyici belge ortaya koymadığını ifade etti. Komisyon, Bard'ın acil olarak AB'nin veri koruma kurallarına uyup uymadığına ilişkin ayrıntılı bir değerlendirme ve bu yöndeki diğer endişeleri yanıtlamasını istediğini ve beklediğini söyledi.

MCLEGAL
Metin-Çiçek Avukatlık Ortaklığı
Attorney Partnership