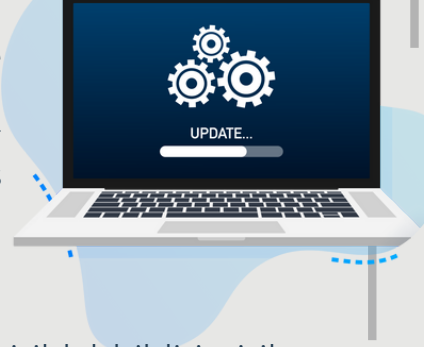


EKİM 2023

KVKK BÜLTEN

Kişisel Verilerin Korunması Kanunu ve ikincil mevzuatı yürürlük tarihinden bugüne güncellemesi sık yaşanan ve yaşanan bir hukuktur. Yalnızca Kanun, Yönetmelik ve Tebliğ ile değil, Kurul Kararları, İlke Kararları ve Kurul Karar Özetleri ile de veri koruma alanıyla ilgili birçok usul ve esas belirlenmektedir. Dolayısıyla aylık bültenlerimiz, Kişisel Verileri Koruma Kurulu uygulamalarından ilgililerini haberdar etmeyi ve güncelliği sağlamayı amaçlamaktadır.



2023 Ekim ayında Kurul tarafından **üç adet** veri ihlal bildirimini ile birlikte genetik verilerin işlenmesi ve ilkeleri ve genetik veri güvenliği başlıklarının yanı sıra Avrupa Birliği Genel Veri Koruma Tüzüğü'nde belirtilen Mahremiyet Temelli Tasarım ve Veri Koruma Etki Değerlendirmesi kavramlarına değinerek uluslararası kişisel verilerin korunması mevzuatını göz önünde bulunduran **“Genetik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber”** yayımlanmıştır. *İlgili rehberle ilişkin değerlendirmelerimizi içeren özet çalışmamıza [LinkedIn](#) hesabımız üzerinden ulaşabilirsiniz.*



VERİ İHLAL BİLDİRİMLERİ

“Veri güvenliğine ilişkin yükümlülükler” başlıklı KVKK m. 12/5. “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

2023 Ekim ayında Kişisel Verileri Koruma Kurumu internet sitesi olan www.kvkk.gov.tr alan adlı sitede üç adet veri ihlal bildirimini yayınlanmıştır.

Havaist Taşımacılık Sanayi ve Ticaret A.Ş.

Veri sorumlusu sıfatını haiz olan Havaist Taşımacılık Sanayi ve Ticaret A.Ş. tarafından Kurula iletilen kişisel veri ihlali bildiriminde özetle; veri sorumlusu tarafından, kısa mesaj gönderimleri için hizmet alınan veri işleyen sistemlerine saldırıda bulunulduğu ve ilgili kişilerin bilgilerine yetkisiz erişim sağlanması ile ihlalin gerçekleştiği, ilgili kişilere **oltalama saldırısı** gerçekleştirilmesi amacıyla kısa mesaj gönderildiği, ihlalden **77.000** kişiye ilişkin cep telefonu verisinin etkilendiği, ihlalden etkilenen kişi grubunun henüz bilinmediği bilgilerine yer verilmiştir.



Tokat Gaziosmanpaşa Üniversitesi



Veri sorumlusu sıfatını haiz Tokat Gaziosmanpaşa Üniversitesi tarafından Kurula iletilen kişisel veri ihlali bildiriminde özetle; Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından yürütülen tehdit istihbaratı faaliyetleri kapsamında Reşadiye Meslek Yüksekokuluna ait olduğu değerlendirilen öğrenci bilgilerinin **saldırganlar** tarafından internette çeşitli forum sitelerinde satıldığı veya satılmaya çalışıldığı bilgisinin 03.10.2023 tarihinde veri sorumlusuna bildirildiği ifade edilmiştir.

Yapılan incelemelerde yurtdışı IP adreslerinden veri sorumlusu sistemlerine yetkili kullanıcı olarak giriş yapıldığının tespit edildiği, ihlalden etkilenen ilgili kişi grubunun **öğrenciler** olduğu, ihlalden etkilenen verilerin; **kimlik, iletişim, görsel ve işitsel kayıt verileri** olduğu, ihlalden etkilenen kişi sayısının **tahmini 741** olduğu bilgilerine yer verilmiştir.

Johnson Controls Klima ve Servis Soğutma San. ve Tic. Ltd. Şti.

Veri sorumlusu sıfatını haiz olan Johnson Controls Klima ve Servis Soğutma San. ve Tic. Ltd. Şti. tarafından Kurula iletilen veri ihlal bildiriminde özetle; veri sorumlusunun 24.09.2023 tarihinde **fidye yazılımı saldırısına** maruz kalması sonucunda ihlalin gerçekleştiği, kişisel verileri içeriyor olabilecek bazı bilgi teknolojileri varlıklarının da bu saldırıdan etkilendiği ve kullanılamamakta olduğu, ihlalden etkilenen kişisel veri kategorilerinin bu aşamada bilinmediği, ihlalden etkilenen ilgili kişi sayısının ve gruplarının henüz bilinmediği bilgilerine yer verilmiştir.



Ekim ayında yayımlanan veri ihlal bildirimleri incelendiğinde, ilgili ihlallerin ortalama ve fidye yazılımı saldırıları neticesinde gerçekleştiği gözlemlenmektedir. Söz konusu veri sorumlularının KVKK uyarınca kendilerine getirilen, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülükleri kapsamında aldıkları önlemlerin yetersizliği veya hiç alınmamış olması sonucu veri ihlali ile karşı karşıya kaldıkları söylenebilecektir.

GRC LEGAL Yorumu

Bu kapsamda, Kurul tarafından yayımlanan **Kişisel Veri Güvenliği Rehberi** ile örneklendirilen idari ve teknik tedbirlerin Şirket iş ve süreçlerine entegre edilmesi ve kişisel veri ve gizlilik nosyonu kapsamında bir kurum kültürü oluşturulması büyük önem arz etmektedir. Özellikle, çalışanlara yönelik periyodik farkındalık eğitimlerinin gerçekleştirilmesi, teknolojik alt yapıların güçlendirilerek şirketlerin bilgi varlıklarına dış erişimin zorlaştırılması gibi birtakım önlemler, bugün pek çok veri ihlalinin önüne geçebilecektir.

EKİM 2023

KİŞİSEL VERİLERİ KORUMA KURUMU İLE REKABET KURUMU ARASINDA İŞ BİRLİĞİ PROTOKOLÜ İMZALANDI!



Veriye dayalı teknolojiler ile dijital ekonomiyi destekleyen çok sayıda ve çeşitte ürün ve hizmetin gelişmesi ile birlikte rekabetin ve kişisel verilerin korunması alanlarının birbirine sıkı sıkıya temas eder hale gelmesi üzerine **Kişisel Verileri Koruma Kurumu** ile **Rekabet Kurumu** arasında iş birliği protokolü imzalanmıştır.

Bu kapsamda, iki otorite tarafından somut olarak;

- İki otoritenin de görev alanına giren gelişmekte olan ve hızlı ve etkin müdahale edilmemesi halinde telafi edilemez zararlara yol açabilecek nitelikteki alanlarda ortak çalışmalar yürütmek,
- Özellikle dijital pazarlarda kişisel verilerin ve rekabetin korunması bakımından kullanıcılar nezdinde farkındalığı artırmak ve her iki hukuk alanını da ilgilendiren uygulamalar bakımından teşebbüslere ortak mesaj iletmek amacıyla her iki kurumun iş birliğiyle raporlar yayımlamak,
- Kişisel Verileri Koruma Kurumunun gelenekselleşmiş “Çarşamba Seminerleri” ve/veya Rekabet Kurumunun “Perşembe Konferansları” kapsamında ortak sunum ve tartışma programları düzenlemek,
- İlgili otoritelerin görev alanlarına ilişkin uzmanlık bilgisini ve tecrübelerini birbirleriyle paylaştığı eğitimler düzenlemek,
- İlgili otoritelerin düzenlediği ve/veya katıldığı ulusal ve/veya uluslararası etkinliklerde ortak konuları istişare etmek, otoritelerin kendi alanlarına giren konularda bu etkinliklere destek vermek,

gibi aktif iş birliğine yönelik çalışmalara başvurulması hususunda anlaşılmıştır.