ASChukuk | 20 YIL .YEARS
AKSU ÇALIŞKAN BEYGO AVUKATLIK ORTAKLIĞI

11 Ağustos 2021

KİŞİSEL VERİLERİ KORUMA KURULU'NUN 9 AĞUSTOS 2021 TARİHİNDE YAYIMLAMIŞ OLDUĞU KARARLARA İLİŞKİN BİLGİLENDİRME NOTU

I. YÖNETİCİ ÖZETİ

1. Kişisel Verileri Koruma Kurulu ("KVKK") tarafından 9 Ağustos 2021 tarihinde 9 Adet yeni karar yayımlanmıştır.
2. Kararların, yoğunluklu olarak, Oyun, Bankacılık, Kişisel Bakım, İlaç, Yazılım, Sigortacılık, E-Ticaret, Enerji, Perakende sektöründe faaliyet gösteren şirketlere ilişkin olduğu görülmektedir.
3. Söz konusu Kararlar kapsamında şirketlere ortalama 160.000 Türk Lirası idari para cezası kesildiği görülmektedir.
4. Şirketlere idari para cezası kesilmesinin en büyük sebepleri, 6698 sayılı Kişisel Verilerin Korunması Kanununa ilişkin uyum çalışmasının eksik veya hiç yapılmamış olması; yapılmış olan uyum çalışmalarının gerektiğinde güncellenmemesi, veri güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınmamış olmasıdır.

II. KARARLARA İLİŞKİN ÖZET TABLO

Karar No	Sektör	İhlalin Sebebi	Alınması Gerekli İdari/Teknik Tedbir	İdari Para Cezası
2020/345	Oyun	Yapılan rutin güvenlik denetimi sırasında eski bir veri sorumlusu çalışanı (web geliştiricisi) tarafından içerisinde kaynak kod ile veri dosyaları içeren bir klasörün yetkisiz olarak github.com internet sitesine yüklenmesi.	• Çalışanlara, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim verilmesi • Çalışanlara yönelik farkındalık çalışmaları yapılması • Güvenlik risklerinin belirlenebildiği bir ortam oluşturulması • Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumluluklarının, görev tanımlarında belirlenmesi ve çalışanların bu konudaki rol ve sorumluluğunun farkında olmasının sağlanması • Kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesi • Güvenlik kontrollerinin düzenli olarak yapılması • Kurum içi politikaların etkin şekilde uygulanması	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL ve 19.04.2017'de gerçekleşen veri ihlalinin 09.01.2019 tarihinde tespit edildiği, Kuruma 28.02.2019 tarihinde bildirim yapıldığı hususları dikkate alındığında, veri sorumlusunun Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL toplamda 130.000 TL idari para cezası uygulanmasına karar verilmiştir.
2020/359	Bankacılık	Veri Sorumlusu Banka'nın eski çalışanına Banka dışından 3. Şahıs tarafından T.C. kimlik numaralarının iletilmesi ve eski Banka çalışanının KKB ekranından ilgili kişilerin kredi skorlarını öğrenmesi.	• Kişisel verilerin korunmasına ilişkin kişisel veri güvenliği takibinin uygun zaman aralıklarıyla yapılması • Kullanıcı bazında log kayıtlarında yetki sınırlaması yapılması • Ekranların gereksiz rollere kapatılması • Kişisel verilerin korunması ile ilgili uyarı metnine yer verilmesi • Sorgulanabilecek kişi sayısının sınırlandırılması • Veri sorumlusuna ait çalışanlar için veri güvenliği ve Kişisel Verilerin Korunması Kanunu konusunda belli aralıklarla eğitim ve farkındalık çalışmalarının yapılması	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 400.000 TL ve Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" (Kurul'a bildirim için 72 saat) bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL toplamda 450.000 TL idari para cezası uygulanmasına karar verilmiştir.
2020/421	Kişisel Bakım	Veri sorumlusu ile herhangi bir ilişkisi olmayan üçüncü kişilerin veri sorumlusunun kullanımındaki veri tabanlarından herhangi bir sızıntı olmaksızın dışı kaynaklardan elde ettikleri elektronik posta adresleri/şifreler ile veri sorumlusuna ait internet sitesine giriş yapması	• Hem içeriden hem de dışarıdan saldırılara karşı bilişim ağlarının izlenmesi ve olmaması gereken durumların fark edilmesi	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 210.000 TL idari para cezası uygulanmasına karar verilmiştir.

2020/463	İlaç	Zararlı yazılımlardan ve fidye yazılımlarından kaynaklı bir siber saldırı sonucu veri sorumlusunun yetkili kullanıcı şifresinin ele geçirilmesi ve sistemlerine erişimin engellenmesi ve veri sorumlusunun faaliyetlerini sürdürmesi için kritik öneme sahip tüm sunucu ve verilerinin ve bunlara ek olarak diğer sunucuların yedek dosyalarının depolandığı Data Domain Sunucusu verilerinin silinmesi	• Sızma testlerinin ve risk analizlerinin yapılıp; tehditlerim belirlemesi • Güvenlik açıklarının kapatılması • Log kaydı takibi ile veri güvenliğini sağlayacak önlemlerin alınması • Kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi • Yedeklenen kişisel verilerin sadece sistem yöneticisi tarafından erişilebilir olması • Veri seti yedeklerinin mutlaka ağ dışında tutulması	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 125.000 TL idari para cezası uygulanmasına karar verilmiştir.
2020/465	Yazılım	Saldırganların “parola püskürtme" saldırısı ile veri sorumlusunun bilgi sistemleri iç ağına erişmesi	• Gerekli güvenlik kontrol ve denetimlerinin zamanında yapılması • Veri sorumlusunun son kullanıcılarının parola güvenliği farkındalığının tam olarak oluşturulması • Saldırılara karşı veri kaybı riskini azaltmaya yönelik gerekli idari ve teknik tedbirlerin alınması	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 75.000 TL ve veri sorumlusunun ihlalden etkilenen ilgili kişilere ihlal tespit edildikten 55 gün sonra bildirim yaptığı dikkate alındığında, Kanunun 12’nci maddesinin (5) numaralı fıkrasında yer verilen “en kısa sürede” bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL toplamda 125.000 TL idari para cezası uygulanmasına karar verilmiştir.
2020/532	Sigortacılık	Veri sorumlusunun bilgi sistem destek hizmeti aldığı hizmet sağlayıcısında meydana gelen sistemsel bir hata sonucu akıbet dosyası seçen sorgunun hatalı çalışması nedeniyle Otomatik Katılım Sistemi (OKS) kapsamında kendisine bağlı 61 şirketin müşterisi olan 367 ilgili kişinin kişisel verilerini içeren akıbet dosyalarını söz konusu hata sebebiyle yanlış alıcılara gönderilmesi	• Yazılımdaki sistemsel hatanın veri güvenliğinin sağlanması amacıyla sürekli olarak takibinin yapılması • Veri sorumlusunun gerekli kontrol ve denetimleri zamanında yapması • Sigortacılık işlemi yürüten bir kuruluşun bilgi sistemleri güvenliğinde daha dikkatli olması gerektiğinden, veri ihlaline sebep olan sistemsel hatanın işlem yayına alınmadan evvel düzeltilmesi	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında ihlale sebep olan hatanın istisnai bir durum olması ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 30.000 TL idari para cezasının uygulanmasına karar verilmiştir.
2020/763	E-Ticaret	E-posta gönderimini yapan çalışan tarafından e-postanın konu kısmına yanlışlıkla 43 müşteriye ait e-posta adresinin eklendiği, bu nedenle, e-postanın konu kısmında e-posta adresi yer alan 43 alıcı bilgisinin, e-posta gönderimi yapılan 400 kişilik alıcı grubu ile paylaşılması	• Veri sorumlusunun “en kısa sürede” (24.01.2019 tarih ve 2019/10 sayılı Kurul kararında belirtilen 72 saatlik süre içerisinde) Kuruma veri ihlalini bildirme yükümlülüğünü yerine getirmesi • Hatalı e-posta gönderimi yapılan 400 müşteriden ihlale konu e-postanın imha edilmesinin talep edilmesi	İhlalden 43 kişinin etkilenmesi; ihlale konu kişisel verilerin ilgili kişi üzerinde olumsuz etki doğurma olasılığının düşük olması ve ihlale sebep olan konuda veri sorumlusunun alması gerekli teknik ve idari tedbirleri almış olması sebebiyle idari para cezasına hükmedilmemiştir
2020/934	Enerji	Veri sorumlusunun yetkili üst düzey kullanıcıları tarafından erişim sağlanabilen bir ortak klasörde kurum içi bir platformun kullanıcılarının şifrelerinin açık bir şekilde, kullanıcı adı, isim, profesyonel e-posta adresi gibi tanımlayıcılarla birlikte yer alması	• Etkilenme ihtimali olan mevcut tüm kullanıcıların e-posta mesajıyla bilgilendirilmesi ve aynı şifreyi kullanmış olabilecekleri diğer platformlar da dâhil şifrelerini değiştirmeleri konusunda uyarılması • İhlal gerçekleştikten sonra tespit edilen dosyanın veri sorumlusu tarafından ivedilikle ortadan kaldırılması • İhlalden sonra ilgili platformdaki şifrelerin maskelenmesinin sağlanması • İhlale ilişkin dosyanın erişimden kaldırılmadan önce yalnızca sekiz (8) kullanıcı tarafından erişilmiş olabileceğinin tespit edilmesi ve söz konusu sekiz (8) kullanıcı ile görüşülmesi; tamamının gizlilik yükümlüklerini anladığının ve kabul ettiğinin ve herhangi bir şifre bilgisini kullanmayacaklarının veya paylaşmayacaklarının teyit edilmesi	Kanunun 12 nci maddesinin (1) numaralı fıkrası kapsamında bu aşamada yapılacak bir işlem bulunmadığı ve Kanunun 12 nci maddesinin (5) numaralı fıkrası uyarınca işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde en kısa sürede ilgilisine ve Kurula, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararına uygun olarak bildirimde bulunması hususunda daha dikkatli olunması yönünde talimatlandırılmasına karar verilmiştir.
2020/50	Perakende	Bazı müşterilerin yeni bir hesap açarken kişisel verilerinin yanlışlıkla bir URL üzerinden veri sorumlusunun iç sistemlerine ve çalıştığı bazı üçüncü taraf satıcı/sağlayıcılara aktarılması	• Şirketin log kaydı/takip alarm sistemlerinin bulunması ve etkin bir şekilde kullanılması • URL üzerinden kişisel verilerin üçüncü taraf satıcı/sağlayıcılar tarafından görülmesinin web sayfası tasarım aşamasında yeterli testlerin yapılarak engellenmesi	Veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 50.000 TL idari para cezası uygulanmasına karar verilmiştir

Ayrıntılı bilgi için bizimle temasa geçebilirsiniz.

Kemal Tağa

Ortak Avukat

kemal.taga@aschukuk.com

Emirhan Öncü

Avukat

emirhan.öncü@aschukuk.com

İşbu bilgilendirme notu ve tablosu Kişisel Verileri Koruma Kurulu'nun 9 Ağustos 2021 tarihinde web sitesinde yayımlamış olduğu karar özetlerine ilişkin bilgilendirme amacıyla 11.08.2021 tarihi itibariyle hazırlanmıştır.

İşbu bilgilendirme notu ve tablosu içerisinde yer alan değerlendirmeler hukuki tavsiye ya da hukuki görüş niteliği teşkil etmemekte olup, bu değerlendirmelerden ötürü herhangi bir şekilde Aksu Çalışkan Beygo Avukatlık Ortaklığı'na sorumluluk tahmili mümkün değildir. Bu bilgi notu ve tablosunun kapsamındaki soru ve sorunlarınız bakımından hukuki danışman görüşü alınması tavsiye edilir.

ASChukuk
AKSU ÇALIŞKAN BEYGO AVUKATLIK ORTAKLIĞI
20 YIL .YEARS