

Haziran 2021

KVKK KURUL KARARLARI

 **BERKER**BERKER

Yayın Tarihi : 21/06/2021

Karar Tarihi : 27/04/2021

Karar No : 2021/426

Konu Özeti : Yardım masası paneli hizmeti veren bir veri sorumlusunda gerçekleşen veri ihlali hakkında yapılan resen inceleme



Bir e-ticaret sitesindeki partner firmaya, e-ticaret sitesinin hizmet aldığı yardım masası panelinde yapılan toplu yetkilendirme çalışması esnasında, yanlış yetki verilmesi sonucunda üçüncü taraf diğer firmaların yardım masasında açtıkları bildirimlere erişim sağlamasıyla gerçekleşen veri ihlalinin, partner firma tarafından Kurumumuza bildirilmesi neticesinde Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmıştır.

Yardım masası paneli hizmeti veren veri sorumlusu nezdinde yapılan yerinde inceleme ve konuya ilişkin ifadelerinin yer aldığı tutanakta;

- Veri ihlalinin, veri sorumlusunun kendi yardım masası üzerinde yapılan toplu yetkilendirme çalışması esnasında veri tabanı katmanında çalıştırılan **SQL Script kodundaki bir hata sonucu oluştuğu,**
- Yapılan hata sonucu partner firmanın yer aldığı gruba yanlış yetki verilmesiyle, partner firmanın kendi yardım masası bildirimleri haricinde grup içerisinde yer alan diğer firmaların da yardım masası bildirimlerine ulaşabildiği,
- Veri sorumlusu tarafından yapılan analiz çalışması sonucunda, sadece söz konusu partner firmanın kendisi haricindeki **diğer yardım masası bildirimlerine erişim sağladığının tespit edildiği,**
- Durum tespit edilir edilmez partner firmaya ait yardım masası yetkisi veri sorumlusu tarafından kaldırılarak erişiminin engellendiği,
- Partner firma tarafından veri sorumlusuna gönderilen e-postada, ilgili hata sonucu diğer firmalara ait bilgileri görebildikleri, kendileri ile iletişime geçilmemesi durumunda ihbarda bulunulacağı ve veri sorumlusunun çalışmakta olduğu firmalarla iletişime geçileceğinin paylaşıldığı, veri sorumlusu avukatınca partner firmaya gerekli yasal hatırlatma yapılarak, erişilen verilerin silinmesinin talep edildiği,
- Veri ihlalden 13 farklı veri sorumlusu niteliği taşıyan firmanın etkilenmiş olduğu, veri sorumlusu tarafından ihlalden etkilenen veri sorumlularına gerçekleşen olay ile ilgili e-posta yoluyla bilgilendirme yapıldığı,

- Yazılım üzerindeki özelliklerin tüm veri sorumluları için standart olduğu, bu standardın belirlenmesinde yardım masası paneli hizmeti veren veri sorumlusunun karar verici pozisyonda olduğu, ancak gelen geri bildirimler (kullanıcı deneyimleri) çerçevesinde değerlendirme yapılarak ürün özelliği olarak versiyon planı dahilinde eklendiği, kullanıcıların esnek form ve iş akışları tasarlayabildikleri, böylelikle kendilerine özel ekranlar oluşturabildikleri

ifade edilmiştir.

Yardım masası panelinin, veri sorumlusunun kendisi tarafından kurulan ve yönetilen bir platform olduğu, yazılım hizmetleri ile ilgili bakım ve destek hizmetlerini sağladığı, diğer veri sorumlularının sınırlı bir erişime sahip olduğu ve üzerinde doğrudan değişiklik yapmasının mümkün olmadığı değerlendirilmiştir.

İhlal ile ilgili 3 veri sorumlusu tarafından, Kurumumuza kişisel veri ihlal bildiriminde bulunulmuş, bildirimde bulunmayan 10 veri sorumlusu hakkında 22.04.2020 tarih ve 2020/311 sayılı Kurul Kararı ile resen inceleme başlatılmasına karar verilmiş olup, bunun üzerine söz konusu veri sorumlularından bilgi ve belge talep edilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun **27/04/2021 tarih ve 2021/426 sayılı Kararı ile,**

A) Teknik ve idari tedbirler ile ilgili olarak;

- **Yardım masası panelinin, yazılım firmasından hizmet alan veri sorumlularının kullanıcı adı ve şifreleriyle giriş yapıp yardım taleplerini ilettikleri bir platform olduğu,** söz konusu platform üzerinde verilen hizmetler açısından yazılım firmasının veri sorumlusu sıfatını haiz olduğu,
- Veri ihlalinin 13 farklı veri sorumlusunun, 950'den fazla sayıda çalışanına ve müşterisine ait kimlik, iletişim ve müşteri işlem verilerinin etkilendiği,
- Veri ihlalinin, hatalı bir şekilde yapılan yetki düzenlemesinden ve veri sorumlusunun ihmalkarlığı sebebiyle yeterli güvenlik önlemlerini almamasından kaynaklandığı,
- Bilişim hizmeti yürüten bir veri sorumlusunun bilgi sistemleri güvenliğinde daha dikkatli olmasının beklenildiği, yazılım geliştirme süreçlerinin test platformunda yapılması gerekirken, veri tabanında gerçekleştirilen güncelleme canlı ortamda yapılmış olması sebebiyle ihlalin gerçekleştiği,
- Veri sorumlusunun sistemlerinde kişisel veri içeren belgelerin bulunması halinde kişisel verileri maskeleyen etkin uygulama ve denetim araçlarının bulunmadığı

hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde **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 (ihlalden etkilenen 950'den fazla kişinin bulunduğu, ihlale veri sorumlusunun ihmalkarlığının sebebiyet verdiği) Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca, **300.000 TL idari para cezasının uygulanmasına,**

B) Kurumumuza ve ilgili kişilere yapılan bildirim ile ilgili olarak;

- Veri ihlaliyle ilgili Kurula bildirim yapılmadığı dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında Kişisel Verileri Koruma Kurulunun 24/01/2019 tarih ve 2019/10 sayılı Kararı ile **belirlenen 72 saat içerisinde bildirim yükümlülüğünü yerine getirmeyen 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, **100.000TL idari para cezasının uygulanmasına,**

C) Kurumumuza yönelik bilgi ve belge gönderimi hakkında;

- Bir kamu tüzel kişiliğine haiz veri sorumlusunun, söz konusu olay dahilinde kendilerinden bilgi/belge talebinde bulunulmasına rağmen Kurumumuza **herhangi bir cevap vermediği,**
- Bir özel hukuk tüzel kişiliğine haiz veri sorumlusunun, ihlale konu olayın suç niteliği taşıması nedeniyle Kurumumuz tarafından resen incelemeye ilişkin karar verilemeyeceği, zira olayın yargı organları tarafından değerlendirilmesi gerektiğini iddia ettiği ve Kurumumuza bir takım bilgi ve belge göndermiş olmakla birlikte; Kurulun, inceleme konusuyla ilgili istemiş olduğu; ihlalden etkilenen kişi sayısı, ihlalden etkilenen kişisel veriler gibi ihlal ile ilgili açıklayıcı **birçok bilgi ve belgeyi Kurumumuza göndermemiş olduğu**

hususları dikkate alındığında Kanun'un 15 inci maddesinin (3) numaralı fıkrasında yer alan *"Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır."* hükmü çerçevesinde veri sorumluların Kurulun **bilgi belge talebine ilişkin cevap verilmesinde gerekli dikkat ve özenin gösterilmesi hususunda talimatlandırılmasına**

karar verilmiştir.

Yayın Tarihi : 21/06/2021
Karar Tarihi : 27/04/2021
Karar No : 2021/427
Konu Özeti : Bir e-ticaret sitesi (veri sorumlusu) nezdinde gerçekleşen veri ihlali hakkında yapılan resen inceleme



Bir e-ticaret sitesindeki (veri sorumlusu) partner firmanın, e-ticaret sitesindeki müşteri hizmetleri paneli üzerinden üçüncü kişiler konumundaki firmaların bilgilerine erişmesiyle yapmış olduğu ihbar kapsamında konuya ilişkin olarak Kişisel Verileri Koruma Kurulu tarafından resen inceleme başlatılmıştır.

Partner firmasının Kurumumuza intikal eden yazılarında;

- Partner firmanın elektronik adisyon takip sistemi ve dokunmatik bilgisayar ürünlerinin internet ortamında satışına ilişkin, veri sorumlusu ile partner şirket olmak adına başvuruda bulunduğu,
- Firmanın, ürünlerini sisteme yüklerken giriş yaptığı bölümün aktif olmadığını fark etmeleri üzerine e-ticaret sitesinin müşteri hizmetlerini arayarak durumu ilettiklerinde, partner sayfasındaki bildirim bölümünden konuya ilişkin iletişime geçilmesi gerektiğinin belirtildiği, firmanın bu doğrultuda bildirim paneline giriş yapıp bildirim göndermeye çalıştıklarında sürekli hata aldığı,
- Bu hatalardan dolayı Partner Firmanın bildirim linkini tarayıcıya yazıp giriş yapmaya çalıştığı, bu suretle veri sorumlusunun kullanmış olduğu müşteri hizmetleri (CRM) paneline erişildiği, açılan panelde tekrar kullanıcı adı ve şifre istendiği, mevcut kullanıcı adı ve şifreleriyle giriş yapılmaya çalışıldığı, erişim sağlanamayınca şifrelerinin bloke edildiği düşünülerek yeni şifre talep edildiği, e-posta adreslerine gelen şifre ile sisteme giriş yapıldığında veri sorumlusunun CRM paneline ulaşıldığı, bu sistem açığıyla ilgili veri sorumlusuna e-posta gönderildiği,
- Konuya ilişkin veri sorumlusunun avukatının kendilerini arayarak, belirli bir ücret karşılığında kendilerini danışman şirket olarak atayacaklarını, veri sorumlusu tarafından ilgili firmaya bir şifre verilerek sisteme giriş yapılacağını, veri sorumlusunun onayı ile sistem açığı bulunup bulunmadığına yönelik kontrol sağlamak amacıyla girdiğini gösterir bir senaryo hazırlayacaklarını ve söz konusu senaryoyu destekleyecek bir gizlilik sözleşmesi imzalayacaklarını belirttiği, veri sorumlusunun ofisinde bir toplantı gerçekleştirildiği, yapılan toplantıda güvenlik açığına ilişkin görüşme gerçekleştirildiği ve gizlilik sözleşmesinin imzalandığı

ifadelerine yer verilmiştir.

Veri sorumlusunun meydana gelen veri ihlali ile ilgili Kurumumuzun konuya ilişkin tebligatlarına verilen cevap yazılarında ise;

- Pazar yeri modeli ile satış yapmak üzere kendilerine başvuran şahısların veri sorumlusu nezdinde satış yapabilmelerini teminen giriş yapmaları amacı ile kendilerine tahsis edilen kullanıcı adı ve şifre ile sisteme giriş sağladıkları,
- Şahısların daha sonra sistemde bir açık bulduklarını, kendilerine ait doküman yükleme sayfası dışında üçüncü kişiler konumundaki firmaların bilgilerine de eriştiklerini beyan ederek veri sorumlusuna müracaat ettikleri,
- Akabinde bahse konu veri güvenliği açığına ilişkin, veri sorumlusu ile şahıslar arasında kişisel verilerin korunması amacıyla firmanın sisteme ilk girdiği tarihten itibaren başlayacak şekilde bir gizlilik sözleşmesi imzalandığı, sözleşme ile bu şahısların, ellerindeki tüm verileri veri sorumlusuna teslim edeceklerini ve kendi sistemlerindeki yedekler dahil tüm veriyi imha edeceklerini, tüm sürecin gizliliğini de en üst düzeyde sağlayacaklarını taahhüt ettikleri,
- Söz konusu sözleşmenin başlangıç tarihi olayın oluş tarihi olduğundan firma tarafından bilgilere erişilmesinin veri sorumlusu ile firma arasında akdedilen sözleşme kapsamında gerçekleştiği ve bu anlamda herhangi bir hukuka aykırı erişimin bulunmadığı,
- Taraflar arasında bu minvalde bir sözleşme imzalanmışsa da daha sonra bu şahısların veri sorumlusundan şantaj yolu ile para istedikleri, veri sorumlusunun bu şahıslara herhangi bir ödeme yapmadıkları ve sonunda da Kişisel Verileri Koruma Kurumuna başvurdukları,
- İhlale konu olayın suç niteliği taşıması nedeniyle Kurumumuz tarafından re'sen incelemeye ilişkin karar verilemeyeceği zira konunun yargı organları tarafından değerlendirilmesi gerektiği,
- Konuya ilişkin Cumhuriyet Başsavcılığına suç duyurusunda bulunulduğu

belirtilmiştir.

Partner Firmanın yapmış olduğu ihbar bildiriminin ve veri sorumlusu yazılarının incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun **27/04/2021 tarih ve 2021/427 sayılı Kararı ile;**

A. Teknik ve idari tedbirler ile ilgili olarak;

- Veri sorumlusu tarafından kendi tedarikçisi konumunda olan firma yetkililerinin, veri sorumlusunun sistemine giriş yaptıklarında üçüncü kişilere ait kişisel verilere erişim sağladıkları ve erişimin sağlandığı ilk tarih itibarıyla bu hususta yetkili olmadıkları, bu anlamda bahsi geçen “Gizlilik Sözleşmesi” öncesinde “veri sorumlusu uhdesinde bulunan kişisel verilere yetkisiz erişim sağlandığının anlaşıldığı, hukuka aykırı erişimin meydana gelmesinden sonra veri sorumlusu ile şahıslar arasında imzalanan gizlilik sözleşmesi ile geçmişe dönük olarak, meydana gelmiş olan veri ihlalinin ortadan kaldırılmasının hukuken mümkün olmadığı,

- İhlalin veri sorumlusu tarafından kendi tedarikçisi konumunda olan firmanın da bulunduğu tedarikçi grubuna “tüm bildirimlerde arama” yetkisinin verilmesi sonucunda oluştuğunun tespit edildiği, bu durumun yetkisiz erişime ilişkin düzenli kontrolün sağlanmadığının ve yetkilendirme süreçlerinin kontrol edilmeyerek veri ihlali öncesinde veri sorumlusu tarafından ilgili kişiler üzerinde oluşabilecek potansiyel zararları önlemek adına gerekli tedbirlerin alınmadığının göstergesi olduğu

hususları dikkate alındığında, 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrasında kapsamında 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, **600.000 TL idari para cezası uygulanmasına,**

B. Kuruma ve ilgili kişilere yapılan bildirim ile ilgili olarak:

Veri sorumlusu nezdindeki kişisel verilere hukuka aykırı olarak erişilmesi dolayısıyla, Firma nezdinde erişimi gerçekleştirenler yönünden yürütülen cezai soruşturmaya konu fiil ile veri sorumlusunun veri güvenliğini sağlamaya ilişkin gerekli her türlü teknik tedbiri almaması nedeniyle oluşan veri ihlalinin Kurula bildirme yükümlülüğünün farklı fiiller olduğu, ihlalin 22.10.2019 tarihinde gerçekleşmesi ve 22.10.2019 tarihinde tespit edilmiş olmasına rağmen

- Veri ihlalden etkilenen ilgili kişilere bildirimde bulunulmadığı,
- Kişisel Verileri Koruma Kuruluna ihlal bildiriminde bulunulmadığı

hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası kapsamında Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında belirlenen 72 saat içerisinde bildirimde bulunma yükümlülüğüne aykırı davranan veri sorumlusu hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **200.000 TL idari para cezası uygulanmasına,**

Kurumumuzun bilgi belge talep yazısına cevap verilmediği dikkate alındığında, Kanuna uyum konularında **azami dikkat ve özenin gösterilmesi hususunda veri sorumlusunun talimatlandırılmasına,**

karar verilmiştir.

Yayın Tarihi : 21/06/2021
Karar Tarihi : 06/05/2021
Karar No : 2021/470
Konu Özeti : İlgili kişinin yemek kartı hesap hareketlerine ilişkin kişisel verilerine erişim talebinin veri sorumlusu tarafından yerine getirilmediği iddiası



İlgili kişinin Kuruma intikal eden şikayetinde özetle; kendisine işvereni tarafından tahsis edilen yemek kartına ait hesap hareketlerinin tarafına iletilmesinin veri sorumlusu Şirketten talep edildiği, veri sorumlusu tarafından verilen cevapta ise istenilen bilginin sağlanması için kimliği doğrulayacak ilave bilgiler talep edildiği, bunun üzerine dilekçe ve kimlik görüntüsünün veri sorumlusuna e-posta aracılığıyla iletildiği, veri sorumlusu şirketin gönderdiği e-postada ise ilgili bilgilerin ekte paylaşıldığı ancak ilave güvenlik önlemi alınması nedeniyle ekte paylaşılan dokümana erişilebilmesi için e-postada yer alan cep telefonu numarasının aranması gerektiğinin belirtildiği, getirilen bu ilave güvenlik önleminin hukuka aykırı olup şahsına ait verilere erişmesinin engellendiği ve hesap hareketlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'na ("**Kanun**") uygun olarak paylaşılmadığı belirtilerek Kanun kapsamında gereğinin yapılması talep edilmektedir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup, alınan cevabi yazıda özetle;

- İlgili kişinin gmail adresinden veri sorumlusuna gönderdiği e-postada ... nolu yemek kartı kullanıcısı olduğunu belirterek Kanun'un 11'inci maddesi uyarınca tüm hesap hareketlerini ve işlenen verileriyle ilgili açıklamaları talep ettiği, yapılan inceleme sonucunda söz konusu e-posta adresi sistemde kayıtlı olmadığından, ilgili iletişim kanalının teyit edilemediği ve ayrıca ilgili kişi tarafından sunulan kart numarasının hatalı bir numara olduğunun görüldüğü,
- Veri sorumlusunun ilgili kişinin talebine verdiği cevapta, kimliğini doğrulayacak bazı ilave bilgiler istenildiği, veri sorumlusunun talebi üzerine ilgili kişi tarafından gönderilen e-postanın ekinde yer alan ıslak imzalı dilekçedeki talebin "*Tarafıma ait .. numaralı kartın tüm hesap hareketlerinin ... @gmail.com e-posta adresine gönderilmesi için gereğinin yapılmasını arz ederim.*" şeklinde olduğu, bildirilen e-posta adresine yanıt verildiği ve başvurunun konusu olan tüm bilgilerin e-postanın ekinde ilgili kişiyle paylaşıldığı,
- İlgili kişinin daha önce veri sorumlusu sisteminde tanımlı olmayan ve "gmail" gibi altyapısı yurtdışında barındırılan bir e-posta adresine kişisel verilerinin gönderilmesini talep etmesi nedeniyle risk değerlendirmesi yapılarak e-posta ortamında güvenliği en üst düzeyde temin etmek amacı doğrultusunda talebin yanıtlandığı ve ek olarak dosyanın şifrelendiği, ilgili kişinin dosya şifresinin kendisine verilmesi için doğrudan arayabileceği bir telefon numarasının kendisine bildirildiği ve bu güvenlik tedbirinin neden alındığının açıkça izah edildiği

ifade edilmiştir.

Konuya ilişkin olarak yapılan incelemede, Kişisel Verileri Koruma Kurulunun **06/05/2021 tarihli ve 2021/470 sayılı Kararı ile;**

- 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11'inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığı; erişim hakkının bilgi talep etme hakkını tamamlayarak ilgili kişinin kişisel verileri üzerindeki haklarını kullanabilmesi için kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkan sağladığı,
- Kanun'un 12'nci maddesinin (1) numaralı fıkrası gereğince 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,
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ kapsamında, veri sorumlusunun ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlü olduğu; ayrıca, Kurum tarafından veri güvenliğinin sağlanmasına atfedilen önem doğrultusunda yayımlanan Kişisel Veri Güvenliği Rehberi'nde **(Teknik ve İdari Tedbirler)** Kanun'un 12'nci maddesi kapsamında veri güvenliğini sağlamak amacıyla veri sorumlusunun temin etmesi gereken teknik ve idari tedbirlere ilişkin başlıca yöntemlerin bölümler halinde açıklandığı, hangi önlemlerin alınması gerektiği konusunda ise Rehber'de belirtildiği üzere öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerektiği,
- Şifreleme yöntemi ile temel olarak haberleşen kişiler arasındaki veri alışverişinin, üçüncü kişilerin okuyamayacağı şekilde güvenli olarak yapılmasının amaçlandığı; **veri sorumlusunun, ilgili kişinin kişisel verisine erişimini engellemekle birlikte ilgili kişi için orantısız bir külfete yol açmayacak şekilde e-posta aracılığıyla gönderilen dosyanın şifreli olarak gönderimini sağladığı** ve şifrenin de e-postada yer alan telefon numarası arandığında kendisiyle paylaşılacağı belirtiltiği,

- Veri sorumlusu tarafından yapılan risk analizi doğrultusunda, ilgili kişinin kullanımındaki yemek kartının hesap hareketleri ve yükleme bilgilerine ilişkin kişisel verileri içeren dosyanın ilgili kişi tarafından belirtilen ve alt yapısı yurt dışında olan “gmail” hesabına e-posta aracılığıyla gönderileceği için bu verileri içeren dosyanın şifrelenerek gönderilmesi ile veri güvenliğinin üst düzeyde sağlanmasının amaçlandığının ifade edildiği; Kurulun 31/05/2019 tarihli ve 2019/157 sayılı Kararında belirtildiği üzere, Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulmasının söz konusu olacağı; bu doğrultuda, Kanunun 12’nci maddesinin (1) numaralı fıkrasının (b) bendi gereğince kişisel verilere hukuka aykırı olarak erişilmesini önleme yükümlülüğü altında olan veri sorumlusunun aldığı ilave güvenlik önleminin ilgili kişinin iddia ettiği üzere Kanuna aykırılık değil, Kanunun titizlikle uygulanması olduğu

değerlendirmelerinden hareketle;

- İlgili kişinin Kanun’un 11’inci maddesinin (1) numaralı fıkrasının (b) bendi doğrultusunda, kullandığı yemek kartının hesap hareketlerine ilişkin veri sorumlusu tarafından işlenen kişisel verilerine erişim talebi üzerine; veri sorumlusu tarafından e-posta aracılığıyla ilgili kişi tarafından belirtilen “gmail” adresine gönderilen ve kişisel verileri içeren söz konusu dosyanın şifrelenmesinin ilgili kişinin iddiasının aksine Kanun’un 12’nci maddesinin (1) numaralı fıkrasının (b) bendi gereğince kişisel verilere hukuka aykırı olarak erişilmesini önlemek amacıyla uygun **güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmek adına makul bir tedbir olduğuna, alınan bu güvenlik tedbirine ilişkin gerekli açıklamanın ilgili kişiye yapıldığı ve e-posta içerisinde yer alan telefon numarası arandığında şifrenin ilgili kişiyle derhal paylaşılacağı belirtildiği** dikkate alındığında kişisel verilere erişim hakkının engellenmediğine, **bu doğrultuda veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına**

karar verilmiştir.

Karar Tarihi : 14/06/2021
Karar No : 2021/593
Konu Özeti : Prof. Dr. Birol CİVELEK Veri İhlal Bildirimi



Veri sorumlusu sıfatını haiz olan Prof. Dr. Birol CİVELEK tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- İhlalin 10 Haziran 2021 tarihinde gerçekleştiği,
- Siber saldırı sonucu, muayenehane hastalarına ait tıbbi amaçla yalnızca sır saklama yükümlülüğü altında bulunan ve doktor tarafından erişilebilen bulut ortamında yer alan fotoğrafların çalındığı,
- İhlali gerçekleştiren kişi tarafından çeşitli iletişim yolları ile tehdit mesajları alınmaya başlanması ile ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının hastalar olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik (hastanın ismi), görsel ve işitsel kayıtlar (kaydedilen sağlık hizmetine ait öncesi sonrası fotoğraflar) olduğu,
- İhlalden etkilenen kişi sayısının 600 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 28/06/2021
Karar No : 2021/633
Konu Özeti : INTERGEN Genetik ve Nadir Hastalıklar Tanı
Araştırma & Uygulama Merkezi Veri İhlal Bildirimi



Veri sorumlusu sıfatını haiz olan INTERGEN Genetik ve Nadir Hastalıklar Tanı Araştırma & Uygulama Merkezi tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İşten ayrılan bilgi işlem çalışanı tarafından bulunduğu departman itibariyle yetkilerini kötüye kullanarak işten ayrılmadan önce verilerin kopyalandığı,
- İhlalden etkilenen kişi grupları arasında çalışanlar, kullanıcılar, hastalar ve çocukların olduğu,
- Adli bilgi işleme başvurulduktan sonra gelen rapor neticesinde verilerin kopyalandığının tespit edildiği,
- İhlalden etkilenen kişisel veri kategorilerinin tespit edilemediği, ihlalden etkilenmiş olabilecek kişisel verileri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, risk yönetimi, finans, görsel ve işitsel kayıtlar ile özel nitelikli kişisel veri kategorilerinden sağlık bilgileri ve genetik veri kategorileri olduğu,
- İhlalden etkilenen kişi sayısının yaklaşık 10.000 olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

 **BERKERBERKER**

Hukuk Bürosu
Büyükdere Cad. No.185
Kanyon Kompleksi C Blok
K:8 D:9 34394 Şişli, İstanbul
+90 212 353 03 00
+90 212 353 03 02
info@berkerberker.com