Mayıs 2021

KVKK KURUL KARARLARI

BERKERBERKER

Yayım Tarihi : 18/05/2021
Karar Tarihi : 25/02/2021
Karar No : 2021/140
Konu Özeti : **Belediyeler tarafından sunulan internet hizmetleri**

Kurumumuza iletilen çeşitli ihbarlarda belediyelerin internet üzerinden emlak vergisi veya beyan bilgisini sorgulama sayfalarında yalnızca TC kimlik numarası girilerek vatandaşın emlak bilgilerine ulaşılmasının kişisel verilerin korunması açısından sorun teşkil ettiği ifade edilmiş, konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında incelenmesi talep edilmiştir.

Konuya ilişkin başlatılan inceleme neticesinde Kişisel Verileri Koruma Kurulunun 25/02/2021 tarih ve 2021/140 sayılı Kararı ile;

- Kanunun 12 nci maddesinin (1) numaralı fıkrasında "Veri sorumlusu; 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 zorundadır." hükmüne, anılan maddenin (4) numaralı fıkrasında veri sorumluları ile veri işleyen kişilerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacının dışında kullanamayacağı hükmüne, (5) numaralı fıkrasında ise işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kurula bildireceği, Kurulun, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebileceği hükümlerine yer verildiği,

- Kurumumuz internet sayfasında da yayımlanan "Kişisel Veri Güvenliği Rehberi"nde kişisel veri içeren sistemlere erişimin sınırlı olması gerektiği, kişilere yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınması ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanabileceği, ayrıca uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanmasının önemli olduğu hususlarına yer verildiği,

- Yapılan incelemeler neticesinde bazı belediyeler tarafından internet üzerinden verilen vergi ödeme hizmetlerinin üyelik ve şifre ya da çift doğrulama yolu ile sisteme giriş yapılması sureti ile gerçekleştirildiği ve bu uygulamaların Kanuna uygun olduğu, ancak bazı belediyeler tarafından sunulan hızlı sorgulama ya da borç ödeme uygulamalarında sadece tek bir bilgi girilerek kişilerin borç bilgisine ulaşılabildiği; her ne kadar kişiye ait isim ya da mülke ilişkin bilgilere erişim mümkün olmasa da borca ilişkin bilgiye erişim sağlanabildiğinin anlaşıldığı, bu durumun Kanunun 12 nci maddesinin 1 numaralı fıkrasının (b) bendinde yer alan hükme aykırı olduğu

değerlendirmelerinden hareketle;

- **Bazı belediyelerin bu yöndeki Kanuna aykırı uygulamaları nedeniyle konu hakkında Çevre ve Şehircilik Bakanlığına ve Türkiye Belediyeler Birliğine bilgi verilmesine,**

- Diğer taraftan, yalnızca tek bir bilginin girilerek (örneğin TC kimlik no, vergi no gibi) kişilerin borç ya da emlak bilgilerine erişim sağlanmasına yönelik uygulamalar yerine belediyeler tarafından sunulan emlak vergisi, beyan bilgisi veya benzeri nitelikteki hizmetlere ilişkin sorgulama sayfalarında veri güvenliğini arttırmaya yönelik olarak gerekli idari ve teknik tedbirlerin alınması, bu bağlamda örneğin çift katmanlı doğrulamayı mümkün kılabilecek şekilde TC Kimlik numarası ya da vergi numarasının girilmesinin yanı sıra kişilerden farklı kişisel verilerin de talep edilmesi, SMS ile doğrulama, üyelik yapılması gibi yöntemlerin seçilmesi ve bu itibarla belediyelerin hizmet sunma yöntemlerinin kişisel verilerin korunması mevzuatı çerçevesinde yeniden değerlendirilerek **gerekli önlemlerin alınması hususunda Belediyelerin talimatlandırılmasına**

karar verilmiştir.

Yayım Tarihi : 18/05/2021
Karar Tarihi : 13/04/2021
Karar No : 2021/359
Konu Özeti : **İlgili kişinin kişisel verilerinin ikamet ettiği sitede yönetim hizmetleri veren veri sorumlusu şirket tarafından bir mobil uygulama ile hukuka aykırı olarak paylaşılması**

İlgili kişinin Kuruma intikal eden şikayetinde özetle; oturduğu sitenin yönetiminden sorumlu şirketin kendisine ait telefon numarasını yönetim hizmetleri kapsamında kullanılan bir mobil uygulama ile rızası dışında paylaştığı ve ilgili uygulamadan kendisine bilgi mesajı gönderildiği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gerekli yaptırımların uygulanması talep edilmiştir.

Konuya ilişkin olarak başlatılan inceleme çerçevesinde ilgili sitenin yönetim işlemlerini yürüten şirket (Site Yönetim Hizmeti Sunan Şirket) ile aktarım yapılan uygulama ile ilgili hizmeti sunan şirketin (Uygulama Hizmeti Sunan Şirket) savunmaları istenilmiştir.

Bu kapsamda Yönetim Hizmeti Sunan Şirketten alınan cevabi yazıda özetle;

- İlgili kişinin ikamet ettiği Sitenin Temsilciler Kurulu ile Şirketleri arasında hizmet sözleşmesinin bulunduğu, mezkur sözleşme kapsamında yükümlülüklerinin Kat Mülkiyeti Kanunu ve Site Yönetim Kurulu kararlarına uygun olacak şekilde; sitenin ortak alanlarında çalışacak personelin tahsisi ve çalıştırılması, site yönetim faaliyetlerine danışmanlık verilmesi, sitenin finansal durumunun analizi ve bilanço hazırlanması, site denetim kurulunun denetim işlemleri sırasında refakat edilmesi, sitenin gelir-gider muhasebe işlemlerinin usule uygun olarak yapılması olduğu,

- Dolayısıyla Şirketlerinin, bir yönetim firması olduğu ve yönetim firması olması sebebiyle hizmetlerini sunarken birçok yönetim programından yararlanıldığı, kişisel verilerin aktarıldığı iddia edilen uygulamanın da Şirketin bu anlamda yönetim hizmetlerini verirken kullandığı bir program olduğu, site sakinlerinin kişisel verilerinin kesinlikle üçüncü kişilerle paylaşılmadığı, muhtemel olarak ilgili kişinin kendisinin programa kaydolduğundan SMS ile bilgilendirme aldığı,

- Söz konusu uygulamayı sunan Şirket ile aralarında hizmet sözleşmesi bulunduğu, ilgili kişiye ait kişisel verilerin mezkur uygulamaya aktarılması ya da uygulamaya kaydının taraflarınca yapılması gibi bir durumun söz konusu olmadığı, Şirketlerine üçüncü bir taraftan gelen yüksek meblağlı bir ürünle ilgili indirimin site sakinlerince yönetim hizmetlerinin gerçekleştirilmesi için hali hazırda kullanılan bir uygulama (ilk uygulama) üzerinden site sakinlerine bilgi verme amaçlı olarak bildirildiği, kişisel verilerin aktarıldığı iddia edilen yeni uygulamaya (ikinci uygulama) üye olmayı gerektiren bu indirimden yararlanabilmenin tamamen ilgili kişinin inisiyatifinde olduğu, ilgili kişinin kendi seçimi ile yeni uygulamaya/ikinci uygulamaya kaydolduğu, bu çerçevede aydınlatılmanın söz konusu uygulama ve ilgili kişinin arasında bir durum olduğu,

- İlgili kişinin mezkur uygulamaya kaydının Şirketlerince yapılmadığı, ilgili kişinin uygulamaya kendi özgür iradesiyle kayıt olduğu

şeklinde açıklamalara yer verilmiş ve yazıları ekinde hem halihazırda kullanılan ilk uygulama hizmetini sunan şirket hem de şikayet konusu kişisel verilerin aktarıldığı iddia edilen ikinci uygulama hizmetini sunan şirket ile imzalanan hizmet sözleşmelerine ve taraflar arasındaki KVKK Protokolüne yer verildiği görülmüştür.

Şikayet konusu Uygulama Hizmetini Sunan Şirketten alınan yazıda ise,

- Yönetim Hizmeti Sunan Şirket ile aralarında akdedilen hizmet sözleşmesi kapsamında bu Şirkete bulut hizmeti sağlandığı, sisteme kullanıcı kaydı ve girişi, hesap oluşturma ve sair tüm işlemlerin Yönetim Hizmeti Sunan Şirket tarafından oluşturulduğu, bu sebeple kendilerinin veri sorumlusu sıfatını haiz olmadığı, sağlanan bulut hizmetinin kapsamı gereği veri işleyen sıfatını haiz oldukları,

- Sunulan bulut program hizmetinin bir sözleşmenin kurulması veya ifası ile doğrudan doğruya ilgili olduğu, ilgili kişinin ikamet ettiği sitede 634 sayılı Kat Mülkiyeti Kanunundan kaynaklanan borç ve yükümlülüklerin gereklerinin ifası için sitede ikamet eden kişilerin verilerinin işlenmesinin zorunlu olduğu,

- İlgili kişinin kişisel verilerinin Kanunun 5 inci maddesinin (2) numaralı fıkrasının (f) bendi çerçevesinde işlenebileceği, bu kapsamda açık rıza aranması durumunun söz konusu olmadığı, böyle bir rızanın aranacağı düşünülse bile söz konusu aydınlatma ve açık rızanın alınması yükümlülüğünün Yönetim Hizmeti Sunan Şirkete ait olduğu,

- İlgili kişinin kişisel verilerinin Yönetim Hizmeti Sunan Şirket tarafından bulut sistemine girilmesi suretiyle elde edildiği, bu kapsamda ilgili kişiye ait kişisel verilerin Yönetim Hizmeti Sunan Şirket tarafından elde edilerek bulut sisteme girişinin yapıldığı, Yönetim Hizmeti Sunan Şirket tarafından ilgili kişinin girişinin yapılmasının ardından bulut programının otomatik olarak ilgili kişiye kayıt mesajı gönderdiği,

- Yönetim Hizmeti Sunan Şirket ile aralarındaki hizmet sözleşmesi kapsamında gerçekleşecek platform değişikliği ve/veya ek platform kullanımı sebebiyle; halihazırda yönetim hizmetlerinin ifası için kullanılan ilk uygulamada kayıtlı verilerin şikayete konu edilen ikinci uygulamaya aktarılabilmesi için Yönetim Hizmeti Sunan Şirketin bilgisi ve isteği dahilinde Şirketlerine ilk uygulamaya giriş yetkisi tanımlaması yapıldığı ve bu tanımlama ile birlikte platform değişikliği ve/veya ek platform kullanımı sonucu ilk uygulamada kayıtlı verilerin ikinci uygulamaya otomatik olarak aktarıldığı,

- Yönetim Hizmeti Sunan Şirket tarafından ilk uygulamaya kaydı yapılan kullanıcıların bilgi aktarımının otomatik olarak ikinci uygulamaya yapıldığı ve ilgili kişinin sisteme giriş yapabilmesi için telefon numarasına bilgilendirme SMS'i gönderildiği

açıklamalarına yer verilmiştir.

Söz konusu iddialar, tarafların savunmaları ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 13/04/2021 tarih ve 2021/359 sayılı Kararı ile;

- Öncelikle somut hadisede ilgili kişinin şahsına ait telefon numarasının rızası dışında uygulama ile paylaşıldığı iddiası kapsamında veri sorumlusunun tespit edilmesi gerektiği, veri sorumlusunun tespit edilebilmesi adına Site Temsilciler Kurulu ile Yönetim Hizmeti Sunan Şirket arasındaki sözleşmelerin de incelendiği, bu doğrultuda Yönetim Hizmeti Sunan Şirketin Site Temsilciler Kurulu ile akdettiği sözleşme kapsamında ilgili kişinin ikamet ettiği sitede yönetim hizmetleri verdiği, bu anlamda söz konusu hizmetlerin ifası gereği Yönetim Hizmeti Sunan Şirketin 3. kişilerle sözleşme yapabileceği, bu sözleşmeler kapsamında sorumluluğun Yönetim Hizmeti Sunan Şirkete ait olduğu, Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen uygulama/ikinci uygulama ile hizmet sözleşmesi akdettiği ve bu sözleşmenin eki niteliğinde olan KVKK Protokolünde hizmet sözleşmesinde Yönetim Hizmeti Sunan Şirketin veri sorumlusu sıfatını haiz olduğuna yer verildiği dikkate alındığında Yönetim Hizmeti Sunan Şirketin kişisel verilerin aktarıldığı iddia edilen ikinci uygulama ile yaptığı sözleşme kapsamında kişisel verilerin işlenme amaç ve yöntemini belirleyen kişi olarak veri sorumlusu sıfatını taşıdığı,

- Uygulama Hizmetini Sunan Şirketin ise Yönetim Hizmeti Sunan Şirketin verdiği yetki kapsamında onun adına veri işleme faaliyetini gerçekleştiren veri işleyen sıfatını haiz olduğu,

- Kanunun "*Kişisel Verilerin İşlenme Şartları"* başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- Diğer taraftan veri sorumlusu Şirket ve veri işleyen Uygulama Hizmeti Sunan Şirket arasında akdedilmiş olan Protokolün "Protokol Koşulları" başlıklı maddesinde;

    - Yönetim Hizmeti Sunan Şirketin hizmet sözleşmesi kapsamında uygulamayı kullanarak uygulama ile yazılı olarak, elektronik ortamda veya sair şekillerde bilgi, belge ve veri paylaşacağı,

- Yönetim Hizmeti Sunan Şirketin uygulama ile paylaşacağı her türlü verinin sözleşme ilişkisi kapsamında uygulamaya aktarıldığını ve KVKK anlamında gerekli kabul edilmesi halinde Protokolün paylaşılacak her türlü kişisel veri bakımından açık rıza niteliğinde olduğunu kabul, beyan ve taahhüt edeceği,

- İlgili kişilerin KVKK kapsamında açık rıza vermesi gerekli ise ilgili kişilerin verilerinin uygulama ile paylaşılması hususunda ilgili kişilerden açık rıza aldığını kabul beyan ve taahhüt edeceği

hususlarına yer verildiği,

- Bununla birlikte, şikayet konusu kapsamında Uygulama Hizmetini Sunan Şirketten alınan cevap yazısından; Yönetim Hizmeti Sunan Şirket ile aralarındaki hizmet sözleşmesi ile birlikte gerçekleşecek platform değişikliği ve/veya ek platform kullanımı sebebiyle; Yönetim Hizmeti Sunan Şirketin kullandığı ilk uygulamada kayıtlı verilerin ikinci uygulama ile paylaşılabilmesi için veri sorumlusu Şirketin bilgisi ve isteği dahilinde ikinci uygulamaya giriş yetkisi tanımlaması yapıldığı ve bu tanımlama ile birlikte platform değişikliği ve/veya ek platform kullanımı sonucu ilk uygulamada kayıtlı verilerin otomatik olarak ikinci uygulama ile paylaşıldığı ve ilgili kişinin sisteme giriş yapabilmesi için telefon numarasına bilgilendirme SMS'i gönderildiği,

- Bu kapsamda, veri sorumlusu Yönetim Hizmeti Sunan Şirket her ne kadar ilgili kişinin kişisel verilerini ikinci uygulama ile paylaşmadığını iddia etse de, bu uygulama ile aralarında akdedilmiş olan Protokol maddelerine ve Uygulama Hizmeti Sunan Şirketten alınan cevap yazısına göre taraflar arasında söz konusu kişisel veri paylaşımı hususunun mümkün olduğu; keza Uygulama Hizmeti Sunan Şirketten alınan cevap yazısından da veri sorumlusu Şirketin kullanmış olduğu ilk uygulamada mevcut verilerin ikinci uygulama ile paylaşılması kapsamında veri sorumlusu Yönetim Hizmeti Sunan Şirket tarafından ikinci uygulamaya yetki tanındığı, bu yetki çerçevesinde aralarında ilgili kişinin de bulunduğu ilk uygulamadaki kullanıcı bilgilerinin ikinci uygulama ile paylaşıldığı,

- İkinci uygulamaya katılımın, site yönetim işlerinden ayrı bir amaca hizmet ettiği ve isteğe bağlı olduğunun anlaşıldığı, bu uygulamaya ilgili kişilerin katılımını sağlamak amacıyla kişisel verilerin işlenmesinin ise Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer alan işleme şartlarına dayandırılamayacağı ancak ilgili kişinin açık rızası ile gerçekleştirilebileceği, diğer taraftan somut hadisede ise ilgili kişinin açık rızasının alınmadığı hususları göz önünde bulundurulduğunda kişisel verilerin hukuka aykırı işlendiği kanaatine varıldığı

değerlendirmelerinden hareketle;

- Kişisel verilerin aktarıldığı iddia edilen uygulamaya katılımın, site yönetim işlerinden ayrı bir amaca hizmet ettiği ve isteğe bağlı olduğu, bu uygulamaya ilgili kişilerin katılımını sağlamak amacıyla kişisel verilerin işlenmesinin Kanunun 5 inci maddesinin (2) numaralı fıkrasında yer alan işleme şartlarına dayandırılamayacağı ancak ilgili kişinin açık rızası ile gerçekleştirilebileceği, **ilgili kişinin açık rızasının ise alınmadığı hususları göz önünde bulundurularak kişisel verilerin hukuka aykırı işlendiği kanaatine varılmış olup, bu çerçevede Kanunun 12 nci maddesinin (1) numaralı fıkrası hükmüne aykırı hareket eden veri sorumlusu Yönetim Hizmeti Sunan Şirket hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Yayım Tarihi : 18/05/2021
Karar Tarihi : 20/04/2021
Karar No : 2021/389
Konu Özeti : **Bir sigorta şirketinin hizmeti açık rıza şartına bağlaması hakkında ihbar**

Kuruma intikal eden şikâyette;

Kuruma intikal eden bir ihbarda; ihbar eden ilgili kişinin bir sigorta şirketinden **(Şirket)** bireysel emeklilik sözleşmesi **(BES)** yaptırdığı, Şirketin internet sayfasından poliçe bilgilerine ulaşmak için giriş yapmaya çalıştığında bir onay kutucuğu sunularak kişisel verilerin işlenmesine rıza göstermek zorunda bırakıldığı, bu kutucuğu işaretlememesi halinde hiçbir işlem yapamayacağının anlaşıldığı, ancak kişisel verilerinin işlenmesine onay vermek zorunda bırakılmasının hukuka aykırı olduğu belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

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

- İnternet sayfası üzerinden müşterinin kim olduğunun anlaşılması, kimlik doğrulamasının yapılabilmesi, tazminat taleplerinin alınabilmesi, poliçe/sözleşme ve teminatlarının kontrolü, hasar takibi, müşteri talebi doğrultusunda ya da otomatik olarak müşteriye e-posta ile bilgilendirme yapılması amaçlarına yönelik müşterilere ait kişisel veri ve özel nitelikli kişisel verilerin işlenebildiği, bu kişisel verilerin ise kimlik numarası, telefon numarası, doğum tarihi, baba adı, kişiye ait sağlık bilgileri, sağlık hizmeti faturaları ve buna bağlı sağlık harcama bedeli talepleri, e-posta adresi olarak sıralanabileceği ve bu verilerin Kanunun 5 inci maddesinin birinci fıkrası uyarınca, ilgili kişinin açık rızası olması halinde ve yine anılan maddenin ikinci fıkrasına göre açık rızanın aranmayacağı tahdidi olarak belirtilen hallerde Kanuna uygun olarak işlendiği,

- İnceleme konusu olan uygulamanın ilgili hizmetlerin verildiği tek mecra olmadığı ve söz konusu hizmetlerin kişisel verilerin işlenmesinde alınan açık rıza şartına bağlanmadığı,

- Şirketin hem kişisel verilerin korunmasına ilişkin mevzuat çerçevesinde hem de ticari elektronik iletiler hakkında mevzuat gereği, kişisel verileri işleme kapsam ve koşulları konusunda ilgilileri aydınlatma/bilgilendirme ve gerektiğinde bu aydınlatmanın yapıldığını da ispat etme yükümlülüğü bulunduğu, bu sebeple uygulama girişinde ilgililere aydınlatma metni iletildiği, sağlık verileri başta olmak üzere yukarıda belirtilmiş olan kişisel verilerin işlenmesi söz konusu olabileceğinden, bir kez sisteme bağlanan bir kullanıcının, web üzerinden sunulmakta olan başka hizmet(ler)i de almak isteyebileceğinin önceden öngörülmesi mümkün olmadığından, açık rıza talep edilmesi gerektiğinin düşünüldüğü,

- Şirket tarafından internet sayfası üzerinden sunulmakta olan ürün ve hizmetlere asıl erişimin Türkiye'nin hemen her noktasında faaliyet gösteren sigorta acenteleri aracılığı ile sağlandığı, çağrı merkezinin de müşterilere kesintisiz olarak hizmet verdiği; ayrıca, başka bir alternatif olarak da Şirketin kurumsal internet sayfası ve mobil uygulamaları ile müşterilere bir takım ürünlere elektronik ortamdan da erişme imkânı sunulduğu, dolayısıyla Şirketin internet sayfası üzerinden sunulan çeşitli hizmetlere ulaşılabilecek başka mecra ve kanalların da mevcut olduğu,

- Şirketin açık rıza bildirimi ve aydınlatma bildirimlerinin internet sayfasında yer alan iki ayrı linkte yer aldığı

ifade edilmiştir.

Söz konusu ihbar dilekçesindeki iddialar, veri sorumlusunun savunması ve ilgili mevzuat hükümlerinin birlikte incelenmesi neticesinde Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/389 sayılı Kararı ile;

A. Aydınlatma Metninin Mevzuata Uygunluğuna İlişkin Olarak:

- 6698 sayılı Kanunun 10 uncu maddesi uyarınca kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişinin ilgili kişileri kişisel verilerin işlenme faaliyeti hakkında anılan maddede yer verilen unsurları içerecek şekilde bilgilendirmesi ve bu kapsamda, Kanunun 10 uncu maddesinde yer alan aydınlatma yükümlülüğünün, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ **(Tebliğ)** hükümlerine uygun olarak yerine getirilmesi gerektiği,

- Tebliğin 4 üncü maddesinde; aydınlatma yükümlülüğünün kapsamının, 5 inci maddesinde ise veri sorumlusunun aydınlatma yükümlülüğünü yerine getirirken uyması gereken hususların düzenleme altına alındığı,

- Sigorta faaliyetleri çerçevesinde sigortacının müşteriye karşı olan yükümlülüklerini ifa edebilmesi için çeşitli kişisel verilerin işlenmesi gerekli olabileceğinden, söz konusu kişisel verilerin işlenmesinde Kanuna ve Tebliğe uygun aydınlatmanın yapılmasının önem arz ettiği, Şirketin cevabi yazısında belirttiği linklerde, "Online İşlemler" sayfasında sisteme giriş için doldurulması gereken kutucukların alt kısmında "*Gizlilik ve Kişisel Verilerin Korunması Esasları'nı okudum, kabul ediyorum. Burada paylaşmış olduğum kişisel/özel nitelikli kişisel verilerimin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde işlenmesine açık rıza veriyorum.*" ifadesine yer verildiği, "Gizlilik ve Kişisel Verilerin Korunması Esasları" ibaresinin üzerine tıklandığında ise aydınlatma metninin açıldığının tespit edildiği, veri sorumlusunun cevabi yazısında belirtilmiş olan her iki linkte de yer alan aydınlatma metinleri incelendiğinde, söz konusu metinlerin birebir aynı olduğunun anlaşıldığı,

- Bu çerçevede her iki aydınlatma metninde de "*D-Kişisel Verileriniz Toplama Yöntemi ve Hukuki sebebi" başlığı altında "Sigorta poliçeleri ve emeklilik sözleşmelerinin taraflarına ait kişisel/özel nitelikli kişisel veriler; acentelerimiz, internet uygulamalarımız ve çağrı merkezimiz aracılığı ile doğrudan doğruya sizlerden ve sigorta sözleşmelerinden kaynaklanan yükümlülüklerin yerine getirilebilmesi için kamu kurumları tarafından tarafımıza erişim yetkisi verilen veri tabanlarından derlenmektedir."* ifadelerine yer verildiğinin görüldüğü,

- Metnin devamında kişisel verileriniz, "*6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde sadece sigortacılık faaliyetlerinin yürütülmesi amacı ile ve bu amacın gerektirdiği yasal sürelerle sınırlı olarak işlenmektedir.*" şeklinde açıklama yapıldığı, ancak Tebliğin 5 inci maddesinin birinci fıkrasının (h) bendinde de düzenlendiği üzere, Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan "hukuki sebep"ten kastın, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiği olduğu, bu anlamda hukuki sebep olarak Kanunda düzenlenen 5 inci veya 6 ncı maddelerden hangisine veya hangilerine dayanıldığına ilişkin bir bilgilendirmede bulunulmadığının anlaşıldığı,

- Bununla birlikte, mezkûr metnin "C-Kişisel Verilerinizi Kimlere ve Hangi Amaçla Aktarıyoruz?" başlığı altında geçen "sigortacılık ve sair mevzuat" ibaresinin muğlak olduğu, zira kişisel verilerin aktarımı hangi mevzuat kapsamında gerçekleştiriliyor ise ayrı ayrı açıkça belirtilmesi gerektiği, ayrıca metinde yer alan kurum ve kuruluşların isimlerinin de güncellenmediğinin anlaşıldığı,

- Diğer taraftan, ihbar edenin başvurusuna konu online sisteme veri sorumlusunun hizmetlerinden faydalanmak amaçlı üyelik kurulduktan sonra müşteriye ait TC kimlik numarası ile cep telefonu numarasının girilmesi sureti ile giriş yapılabildiğinin görüldüğü, sisteme giriş için doldurulması gereken kutucuğun alt kısmında yer alan "*Gizlilik ve Kişisel Verilerin Korunması Esasları'nı okudum, kabul ediyorum. Burada paylaşmış olduğum kişisel/özel nitelikli kişisel verilerimin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuat çerçevesinde işlenmesine açık rıza veriyorum*." ifadesine yer verildiği, dolayısıyla tek bir kutucuk işaretlendiğinde ilgili kişinin hem aydınlatma metnine hem de kişisel verilerinin işlenmesine onay verdiği, ancak Tebliğin 5 inci maddesinin birinci fıkrasının (f) bendine göre, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiğinin hüküm altına alındığı, dolayısıyla kişisel verilerin işlenmesinin hukuki sebebinin açık rıza olduğu durumlar için ayrı bir açık rıza metninin de oluşturulması gerektiği

B. Açık Rızanın Hizmet Şartına Bağlanıp Bağlanmadığına İlişkin Olarak:

- Kanunun “Tanımlar” başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde açık rızanın, “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” şeklinde tanımlandığı, bu anlamda açık rızanın öncelikle belirli bir konuya ilişkin ve o konu ile sınırlı olarak verilmesi bu doğrultuda veri sorumlusu tarafından açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerektiği, diğer bir deyişle, açık rıza beyanının genel nitelikte olmaması, belirli bir konuya özgülenmiş ve o konu ile sınırlı olması gerekmekte olup, açık uçlu veri işleme faaliyetlerine ilişkin rıza alınamayacağı, bununla birlikte, açık rıza bir irade beyanı olduğundan, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerektiği ayrıca kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olmasının beklenildiği, bu sebeple, bilgilendirmenin, veri işleme ile ilgili bütün konularda açık ve anlaşılır bir biçimde gerçekleştirilmesi ve mutlaka verinin işlemesinden önce yapılmasının önem arz ettiği, diğer yandan, açık rızanın geçerlilik kazanabilmesi için kişinin yaptığı davranışın bilincinde ve kendi kararı olması gerektiği, bu çerçevede açık rızanın özgür iradeyle açıklanması gerektiğinden, herhangi bir ürün ve/veya hizmetin sunumunun da (ya da herhangi bir üründen ve/veya hizmetten yararlandırılması) ilgili kişi tarafından açık rıza verilmesi şartına bağlanmaması, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerektiği,

- Diğer taraftan, kişisel verilerin işlenme şartlarının düzenlendiği Kanunun 5 inci maddesinin birinci fıkrasında; kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, bununla birlikte ikinci fıkrasında belirtilen şartlardan (-Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) birinin varlığı halinde ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğunun hükme bağlandığı,

- Bununla birlikte, Kanunun “Genel ilkeler” başlıklı 4 üncü maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği, bu çerçevede kişisel verilerin işlenmesinde “*a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”* şeklinde sayılan ilkelere uyulmasının zorunlu olduğunun düzenleme altına alındığı, anılan madde hükmünden açıkça anlaşılacağı üzere, kişisel verilerin işlenmesinde her hal ve şartta Kanunun 4 üncü maddesinde sayılan genel ilkelere uyulmasının hukuki bir gereklilik olduğu,

- Öte yandan, 4682 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununun (**4682 sayılı Kanun)** “Emeklilik sistemine katılma ve emeklilik sözleşmesi” başlıklı 4 üncü maddesinin birinci fıkrasına göre;

"(…) Sisteme katılmak için şirket ile emeklilik sözleşmesi akdedilir. Emeklilik sözleşmesi; şirket nezdinde bireysel emeklilik hesabı açılması, hesaba katkı payı ödenmesi, ödenen katkı paylarının tercih edilen fonlarda yatırıma yönlendirilmesi ve hesapta biriken paraların hak sahiplerine ödenmesine ilişkin esas ve usuller ile tarafların bu kapsamdaki diğer hak ve yükümlülüklerini düzenleyen sözleşmedir. Emeklilik sözleşmesi, katılımcı ile bireysel emeklilik sözleşmesi şeklinde veyahut bir istihdam ilişkisine dayalı olarak veya katılımcı adına bir kuruluş ile grup emeklilik sözleşmesi şeklinde yapılabilir. Emeklilik sözleşmesine ve emeklilik sözleşmesinde bulunacak hususlara ilişkin esas ve usuller Kurulun görüşü alınarak Müsteşarlık tarafından belirlenir."

hükmünün düzenlendiği, 09.11.2012 tarihli Resmi Gazetede yayımlanan Bireysel Emeklilik Sistemi Hakkında Yönetmeliğin (BES Yönetmeliği) 3 üncü maddesinin birinci fıkrasının (z) bendine göre teklif formunun, emeklilik planına, plan kapsamında sunulan fonlara, yapılan kesintilere, katkı payı tutarına, emeklilik sözleşmesinin taraflarına ve katılımcının yatırım tercihlerine ilişkin hususlar ile benzeri bilgileri içeren form olarak tanımlandığı, yine, anılan Yönetmeliğin "Bilgilendirme, teklif ve sözleşmenin düzenlenmesi" başlıklı 5 inci maddesinde;

"*Bilgilendirme, teklif ve sözleşmenin düzenlenmesi*

MADDE 5 – (1) Şirket, bireysel emeklilik sistemine girmek isteyenlere, sisteme girme kararını etkileyebilecek hususlar hakkında bilgi verir; dürüstlük ilkeleri çerçevesinde, emeklilik sözleşmesinin müzakeresi ve düzenlenmesi sırasında katılımcıya veya sözleşmeyi düzenleyen sponsora veya işverene sistemin işleyişine ilişkin teknik konularda yardımcı olur, tarafların hak ve yükümlülüklerine ilişkin gerekli her türlü bilgiyi sağlar, yanıltıcı her türlü hâl ve davranıştan kaçınır. Bakanlık ilgililere yapılacak bilgilendirmenin asgari içeriğini ve yöntemini belirler.
(2) Şirket, kişinin emekliliğe yönelik beklentilerine, gelir düzeyine ve yaşına uygun bir emeklilik planı teklifi sunar. (…)"

hükmünün yer aldığı,

- Bu çerçevede, veri sorumlusunun internet sitesinde yer alan "Bireysel Emeklilik Sözleşmesi Teklif Formu"nun (Teklif Formu) incelenmesinden "İ*nternet Ortamında Sunulacak Hizmetlere İlişkin Hükümler"* başlığı altında yer verilen ifadelerden ilgili kişi ile veri sorumlusu arasında akdedilen Hizmet Sözleşmesi ile ihbar konusu uygulamanın kullanımında talep edilen verilerin veri sorumlusunun internet üzerinden sunduğu hizmetlerde şifre dışında geliştirilen bir yöntem olarak görülebileceği, bu durumda, veri sorumlusunun anılan kişisel veriler için Kanunun 5 inci maddesinin ikinci fıkrasında yer alan "*Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması*" veri işleme şartına dayanacağı değerlendirildiğinden hizmetin açık rıza şartına bağlanmasından söz edilemeyeceği, bununla birlikte ihbara konu olayda söz konusu uygulamanın kullanımı için sunulan aydınlatma metninde aynı zamanda kişisel verilerin işlenmesi için açık rıza alındığı, dolayısıyla veri sorumlusunun savunmasında açık rıza ve aydınlatma kavramlarını iç içe geçmiş belirsiz bir biçimde kullandığının görüldüğü, bu noktada söz konusu kişisel veri işleme faaliyetinin hukuki sebebinin açık bir şekilde ifade edilmesinin veri sorumlusunun yükümlülüğü olduğunun altının çizilmesi gerektiği,

- Ayrıca söz konusu kişisel veri işleme faaliyeti, Kanunda yer alan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı ve bu durumun ise Kanunun 4 üncü maddesinin ikinci fıkrasının (a) bendinde düzenlenen "hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırılık teşkil ettiği

değerlendirmelerinden hareketle,

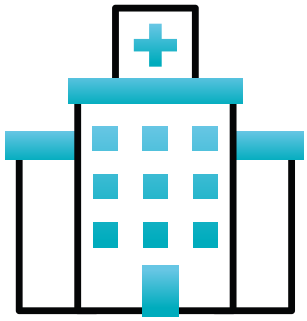
- Kanunun 5 inci maddesinde yer alan diğer işleme şartları mevcut iken ilgili kişilerin açık rızasının alınmasının Kanunun 4 üncü maddesinde yer alan "hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırı olduğu dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **söz konusu uygulamanın ihbar eden dışında pek çok kişi üzerinde olumsuz etki doğurabileceği, veri sorumlusunun sunduğu hizmet bakımından geniş bir müşteri kitlesi bulunduğu, Şirketin kusuru, ekonomik durumu ve haksızlık içeriği gibi hususlar da göz önünde bulundurularak 250.000 TL idari para cezası uygulanmasına,**

- **Açık rıza alınması ile ilgili kişiye aydınlatma yapılması tek bir onaya bağlandığından açık rıza ve aydınlatma metinlerinin ayrı ayrı düzenlenmesi ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,**

- **Aydınlatma metninde muğlak ifadelere yer verildiği dikkate alındığında veri sorumlusunun** aydınlatma yükümlülüğünü Kanun ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümleri ile uyumlu olacak şekilde **düzenlenmesi ve sonucundan Kurula bilgi verilmesi hususunda talimatlandırılmasına**

karar verilmiştir.

Yayım Tarihi : 18/05/2021
Karar Tarihi : 20/04/2021
Karar No : 2021/407
Konu Özeti : **Bir hastanenin veri ihlali bildirimi**



Veri sorumlusu bir hastane tarafından Kuruma intikal ettirilen veri ihlal bildiriminde;

- Veri ihlalinin; hastanede çalışan hekimin hastalarına ait dosyaların arşivden alınarak kendisinin talimatıyla bazı hastane çalışanları aracılığıyla hastane dışına çıkarılmasıyla gerçekleştiği,

- Veri ihlalinin; dosyaları hastane dışına çıkarmaya teşebbüs eden bir çalışanın görülmesinden 17 gün sonra kamera kayıtlarının incelenmesi neticesinde tam olarak tespit edildiği,

- İhlalden; 789 hastanın etkilendiği, ancak 54 dosyanın teslim alınarak yedieminliğe teslim edildiği,

- İhlalden; kimlik, iletişim, sağlık bilgileri ve genetik verilerin hasta kartında yer alan bilgiler (T.C Kimlik numarası, adı, soyadı, baba adı, ana adı, sosyal güvenlik numarası, özel sigorta, anlaşmalı kurum, çalıştığı kurum, uyruğu, doğum tarihi, cinsiyet, medeni hali, kan grubu, mesleği, vergi dairesi, vergi numarası, adres, posta kodu, e-posta, ev telefonu, iş telefonu, cep telefonu, son randevu cep ve ev telefonu, sigortalı durumu, emekli olup olmadığı, poliçe no, engel durumu, çalışan adı, tedavi olunan doktorlar ve branşlar gibi bilgiler) ile hasta dosyası anamnez içeriğinin (kullandığı ilaçlar, alışkanlıklar, alerjik öyküsü, soygeçmiş, psikolojik durum, bulgular, laboratuvar tetkikleri, öntanı, tanı, tedavi ve bakım planı, geçirmiş olunan hastalıklar, ameliyatlar vb. bilgiler) etkilendiği,

- Hekimin bir hastasının hastaneye gelmesi üzerine, tedavi geçmişinin hekim tarafından alındığı bilgisinin kendisine verildiği,

- İhlalin gerçekleşmesinden önce ihlal ile ilgili çalışanlardan (eski çalışan dahil 9 kişi) biri hariç hepsinin kişisel verilerin korunması eğitimi aldığı,

- İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği, geç bildirim sebebi olarak; ilgili dosyaların hastaneden çıkartılırken hastane yönetimi tarafından suçüstü yakalandığı, hemen polis çağırılarak, dosyanın polis nezaretinde hastaneye teslim edilmesi ile verilerin dışarı çıkartılmasına engel olunarak veri ihlalinin oluşmasının önlendiği hususlarına rağmen kriz masasının oluşturulduğu, kovuşturmanın derinleştirilmesine karar verildiği, bu maksatla; doktor ve ekibinden savunmaların alındığı, doktorun takip ettiği dosyaların tarandığı, arşiv, poliklinik, otopark başta olmak üzere hastanenin çeşitli alanlarına ilişkin kamera kayıtlarının incelendiği ve nihayetinde yapılan inceleme ve tahkikatlar neticesinde görülen lüzum üzerine savcılığa suç duyurusunda bulunulduğu ve Kuruma bildirim yapıldığı şeklinde açıklandığı

ifadelerine yer verilmiştir.

Konuya ilişkin yürütülen inceleme neticesinde Kişisel Verileri Koruma Kurulunun 20/04/2021 tarih ve 2021/407 sayılı Kararı ile,

A. Teknik ve idari tedbirler ile ilgili olarak;

- Veri ihlal bildirimine konu olayın; hastanede çalışan hekimin hastalarına ait kişisel veri/özel nitelikli kişisel verilerin yer aldığı dosyaların bulunduğu poşetlerin, kendisinin talimatıyla bazı hastane çalışanları aracılığıyla hastane dışına çıkarılmasıyla gerçekleştiği,

- Kamera kayıtlarının kontrolünün sağlanmadığı, hastalara ait kayıtların tutulduğu arşiv odasına yetkili olmayan kişilerin girebildiği ve başhekimliğin izni olmadan hastalara ait kişisel veri/özel nitelikli kişisel verilerin yer aldığı dosyaların arşivden çıkartılabildiği hususlarının veri güvenliğinin sağlanmasını temin etmeye yönelik fiziksel ortamların güvenliğini sağlayacak idari tedbirlerin yeterli ölçüde alınmadığının göstergesi olduğu,

- İhlalden 789 hastanın etkilendiği ancak karakol tutanağına göre tespit edilen 54 adet hasta dosyasının geri alınarak yedieminliğe teslim edildiği, geri kalan dosyaların akıbetinin ise bilinmediği dikkate alındığından hasta dosyalarının kaybolması durumunun önlenemediği ve bu durumun söz konusu hasta dosyalarının kaybolmasına yönelik risklerin azaltılmasına dair yeterli tedbirlerin alınmadığını gösterdiği,

- İhlalden; kimlik, iletişim, lokasyon, özlük, genetik veri, sağlık verileri gibi veri kategorilerine ait çok sayıda kişisel verinin ve özel nitelikli kişisel verinin etkilenmiş olduğu hususunun ilgili kişilerin ihlal sebebiyle önemli olumsuz etkilere maruz kalmaları olasılığının bulunduğunun göstergesi olduğu,

- İhlal ile ilgili olan çalışanların, sağlık verileri ve genetik veriler de dahil olmak üzere özel nitelikli çok sayıda kişisel verinin işlenme sürecinde yer aldığı göz önünde bulundurulduğunda; veri sorumlusu tarafından çalışanlara tanımlanan kişisel verilerin korunması eğitiminin tamamlanmasının sağlanmadığı, Kuruma gönderilen belgelerde yer alan bilgilerin incelenmesi neticesinde; münhasıran kişisel verilerin korunmasına yönelik eğitimin; sadece 3 çalışan tarafından alınmış olduğu, kişisel verilerin korunması eğitiminin diğer çalışanlara tanımlanmış olmasına rağmen söz konusu çalışanların eğitimlere hiç başlamadıkları ve bu hususta hastane tarafından bir aksiyon alınmadığı, 3 çalışanın kişisel verilerin korunması eğitimi aldıkları ifadesinin “Kalite Müdürlüğü Eğitimi” başlığı altında yer alan konulardan biri arasında kişisel verilerin korunmasının yer almasına istinaden yapıldığı, 2 çalışana ihlalin başlangıç tarihinden sonra eğitim verilmiş olduğu, eğitim tanımlanan 1 çalışanın ise kişisel verilerin korunması ile ilgili hiçbir eğitim almamış olduğu, eski çalışanın kişisel verilerin korunması ile ilgili eğitim almış olmasına rağmen arşiv odasındaki belgelerin taşınmasına yardım ettiğinin anlaşıldığı, bu durumun ise çalışanlara kişisel verilerin korunmasına yönelik yeterli eğitimin verilmediğinin göstergesi olduğu,

- İhlal şüphesini doğuran olayların bulunmasına rağmen; ihlalin 17 gün sonra tespit edilmesinin veri sorumlusu tarafından kişisel veri güvenliği politika ve prosedürlerinin iyi bir şekilde hazırlanmadığı veya takip edilmediği, ayrıca bu durumun alınan mevcut güvenlik önlemlerinin etkili kullanılamadığı hususlarının göstergesi olduğu

dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli 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 450.000 TL idari para cezası uygulanmasına,**

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

- İhlalin tespit edilmesinden 25 gün sonra Kuruma bildirildiği, geç bildirim sebebinin, ilgili dosyaların hastaneden çıkartılırken hastane yönetimi tarafından suçüstü yakalanıldığı, hemen polis çağırılarak, dosyanın polis nezaretinde hastaneye teslim edilmesi ile verilerin dışarı çıkartılmasına engel olunarak veri ihlalinin oluşmasının önlendiği, kriz masasının oluşturulduğu, kovuşturmanın derinleştirilmesine karar verildiği, bu maksatla; doktor ve ekibinden savunmaların alındığı, doktorun takip ettiği dosyaların tarandığı, arşiv, poliklinik, otopark başta olmak üzere hastanenin çeşitli alanlarına ilişkin kamera kayıtlarının incelendiği ve nihayetinde yapılan inceleme ve tahkikatlar neticesinde görülen lüzum üzerine savcılığa suç duyurusunda bulunulduğu ve Kuruma bildirim yapıldığı şeklinde açıklandığı

- İlgili kişilerden hastaneye gelen bir kişi dışında, hiç birine ihlalin bildirilmemiş olduğu

hususları dikkate alındığında Kanunun 12 nci maddesinin (5) numaralı fıkrası hükmü ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına yönelik ifadeleri çerçevesinde **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 150.000 TL idari para cezası uygulanmasına,**

- İlgili kişilere Kurulun 24.01.2019 tarih ve 2019/10 sayılı Kararında yer alan hususları içeren bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına

karar verilmiştir.

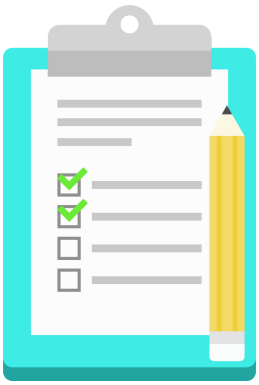
Karar Tarihi : 04/05/2021
Karar No : 2021/463
Konu Özeti : **Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. A.Ş. Veri İhlal Bildirimi**

Veri sorumlusu sıfatını haiz olan Bulut Elektromarket Bilgi Teknolojileri ve Dış Tic. A.Ş. tarafından Kuruma gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri sorumlusunun sunucularına bir siber saldırı gerçekleştirildiği ve saldırı sonucunda sunuculara erişimin engellendiği,
- İhlalden çalışanlar ve müşterilerin etkilendiği,
- İhlalden etkilenen kişi ve kayıt sayısının henüz bilinmediği, tespit çalışmalarının devam ettiği,
- İhlalden kimlik, iletişim, lokasyon, özlük, hukuk, işlem, müşteri işlem, işlem güvenliği, fiziksel mekan güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim ve pazarlama verilerinin etkilendiği,
- Özel nitelikli kişisel veriler arasında sağlık bilgileri ve ceza mahkumiyeti ve güvenlik tedbirlerine ilişkin verilerin etkilendiği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.



Karar Tarihi : 04/05/2021
Karar No : 2021/462
Konu Özeti : ClearVoiceResearch.com, LLC Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan ClearVoiceResearch.com, LLC tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- İhlalin yetkisiz bir kullanıcı tarafından 2015 Ağustos ve Eylül aylarına ait yedeklerin herkese açık hale getirilmesi sonucunda meydana geldiği,
- 17 Nisan 2021 tarihinde yetkisiz bir kullanıcı tarafından, ClearVoice'un 2015'teki anket katılımcılarının profil bilgilerini içeren eski veritabanlarından birine ilişkin, yedek dosyasına eriştiğini belirten bir e-posta alınması ile ihlalin tespit edildiği,
- İhlalden kimlik, iletişim, doğum tarihi, 2015 yılına ait şifreler, ırk ve etnik köken, siyasi düşünce, sendika üyeliği, sağlık bilgilerine ilişkin kişisel verilerin etkilendiği,
- İhladen etkilenen Türkiye'de yerleşik kişi sayısının 184.205 olduğu,
- İhlalden etkilen ilgili kişi grubunun çalışanlar olduğu

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 18/05/2021
Karar No : 2021/498
Konu Özeti : E-Data Teknoloji Pazarlama A.Ş. Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan E-Data Teknoloji Pazarlama Anonim Şirketi tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- Veri ihlalinin, veri sorumlusunun "www.bayipazar.com" internet sitesine ait veri tabanının SQL injection açıklığının kullanılması sonucu kullanıcı bilgilerini içeren veri tabanına erişilmesiyle gerçekleştiği,

- Veri tabanından elde edilen kullanıcı adı ve şifre bilgileriyle internet sayfasına giriş yapıldığı,
- İhlalden etkilenen ilgili kişi sayısının 721 olduğu,

- İhlalden etkilenen kişisel verilerin ad, soyad, e-posta adresi, kullanıcı adı ve şifre bilgilerinin olduğu,

- İlgili kişilerin "kvkk@e-data.com.tr" ve "dmflegal@dmflegal.com.tr" e-posta adreslerinden veri ihlali ile ilgili bilgi edinebileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 20/05/2021
Karar No : 2021/517
Konu Özeti : **Pakten Sağlık Ürünleri Sanayi ve Ticaret A.Ş. Veri İhlal Bildirimi**

Veri sorumlusu sıfatını haiz olan Pakten Sağlık Ürünleri Sanayi ve Ticaret A.Ş. tarafından Kurumumuza gönderilen kişisel veri ihlali bildiriminde özetle;

- SQL Injection saldırısıyla veri sorumlusu internet sitesinin veri tabanı yönetim bilgilerinin ele geçirildiği,
- Saldırganlar tarafından fidye talebiyle mesaj gönderilmesiyle ihlalin tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlalden siteye üye olan müşterilerin ad-soyad, adres, e-posta ve telefon numarası bilgilerinin etkilendiği,
- İhlalden etkilenen kişi sayısının 2541 olduğu,
- İlgili kişilerin e-posta: bilgi@onlem.com.tr, çağrı merkezi: 0850 201 75 40, Whatsapp Hattı: 0535 830 93 23 vasıtası ile söz konusu ihlale ilişkin bilgi alabilecekleri

ifade edilmiştir.

Konuya ilişkin inceleme devam etmektedir.

Karar Tarihi : 27/05/2021
Karar No : 2021/537
Konu Özeti : Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir) Veri İhlal Bildirimi

Veri sorumlusu sıfatını haiz olan Rahmet Ragıp Kuğu (Serbest Muhasebeci Mali Müşavir) tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusunun bilgisayar ve internet sisteminin fidye yazılımı saldırısına maruz kaldığı,
- Bilgisayar korsanlarına fidye ödenmesiyle ihlale konu sistemlerin kullanıma açıldığı,
- İhlalin 31.03.2021-06.04.2021 tarihleri arasında gerçekleştiği ve 04.04.2021 tarihinde tespit edildiği,
- İhlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, müşteriler ve potansiyel müşteriler olduğu,
- İhlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, özlük, hukuki işlem, müşteri işlem, işlem güvenliği, finans, mesleki deneyim, görsel ve işitsel kayıtlar olduğu,
- İhlalden etkilenen ilgili kişi ve kayıt sayısının tam olarak tespit edilemediği, ancak yaklaşık olarak 130 gerçek ve tüzel kişi müşterinin ihlalden etkilenmiş olduğunun tahmin edildiği

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