KİŞİSEL VERİLERİ KORUMA KURULU'NUN 18 MAYIS 2021 TARİHİNDE YAYIMLANAN KARARLARI HAKKINDA ÖZET BİLGİLENDİRME

1. Belediyeler tarafından sunulan internet hizmetlerine ilişkin 25/02/2021 tarihli ve 2021/140 sayılı karar[1]

Kişisel Verileri Koruma Kurulu'na ("Kurul") intikal eden ihbarlarda, belediyelere ait internet sitelerinde yer alan emlak vergisi veya beyan bilgisi sorgulama sayfalarında yalnızca T.C. kimlik numarası girilerek vatandaşların emlak bilgilerine ulaşılabildiği gerekçesiyle konunun 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") kapsamında incelenmesi talebinde bulunulmuştur.

Kurul, bu konuda gerçekleştirdiği incelemede öncelikle "Kişisel Veri Güvenliği" rehberini dikkate alarak kişisel veri içeren sistemler için; i) erişimin sınırlı olması, ii) kişilere yetki ve sorumlulukları kapsamında gerekli ölçüde erişim yetkisi tanınması, iii) ilgili sistemlere erişimin kullanıcı adı ve şifre kullanılarak sağlanması, iv) uzaktan erişim aşamasında iki kademeli kimlik doğrulama kontrolünün uygulanması gerektiğini vurgulamıştır.

Kurul netice itibariyle, bazı belediyelerin internet üzerinden sağladıkları vergi ödeme hizmetlerine erişimin üyelik ve şifre veya çift doğrulama yolu ile sağlandığı ve dolayısıyla bu uygulamanın Kanun'a uygun olduğuna işaret etmiştir. Öte yandan, bazı belediyelerin ise hızlı sorgulama veya borç ödeme uygulamalarında kişilerin borç bilgisine tek bir bilgi girilerek erişebildiği ve uygulanan bu yöntemin Kanun'un 12.maddesinin 1 numaralı fıkrasının (b) bendine aykırı olduğu tespit edilmiştir.

Sonuç olarak, Kurul, bazı belediyelerin Kanun'a aykırı uygulamaları yönünden konu hakkında Çevre ve Şehircilik Bakanlığı'na ve Türkiye Belediyeler Birliği'ne bilgi verilmesine ve kişilerin borç veya emlak bilgilerine erişimin yalnızca tek bir bilgi girilerek sağlanmasına ilişkin mevcut uygulamalar yerine;

i) Belediyelerin sunduğu emlak vergisi, beyan bilgisi veya benzer nitelikteki hizmetlere ilişkin sorgulama sayfalarında gerekli idari ve teknik tedbir alınarak veri güvenliğinin arttırılması,

ii) T.C. kimlik numarası veya vergi numarası bilgilerinin yanı sıra kişilerden farklı kişisel verilerinin talep edilerek çift katmanlı bir doğrulama uygulaması oluşturulması,

iii) SMS ile doğrulama, üyelik yapılması yöntemlerinin seçilmesi çerçevesinde belediyelerin hizmet sunma yöntemlerinin mevzuat kapsamında yeniden değerlendirilerek gerekli önlemlerin alınması hususunda **Belediyelerin talimatlandırılmasına** karar vermiştir.

[1] Erişim için: https://www.kvkk.gov.tr/Icerik/6965/2021-140

2. İlgili kişinin kişisel verilerinin site yönetim hizmetini sağlayan veri sorumlusu şirket tarafından bir mobil uygulama ile hukuka aykırı olarak paylaşılmasına ilişkin 13/04/2021 tarihli ve 2021/359 sayılı karar[2]

Şikâyete konu olayda ilgili kişi özetle; oturduğu site yönetiminden sorumlu olan veri sorumlusu şirketin (Site Yönetim Hizmeti Sunan Şirket) kendisine ait telefon numarasını yönetim hizmetleri kapsamında kullanılan bir mobil uygulama ile rızası dışında paylaştığı ve söz konusu uygulamadan kendisine bilgi mesajı gönderildiği gerekçesiyle Kanun kapsamında gerekli yaptırımların uygulanmasını talep etmiştir.

Site Yönetim Hizmeti Sunan veri sorumlusu Şirket, yönetim firması olduğu gerekçesiyle kişisel verilerin aktarıldığı iddia edilen uygulamanın yönetim hizmeti sunmaya yönelik kullanılan bir program olduğunu, site sakinlerinin kişisel verilerinin kesinlikle üçüncü kişilerle paylaşılmadığı, muhtemelen ilgili kişinin özgür iradesi ile programa kaydolarak SMS ile bilgilendirildiğini iddia etmiştir. Öte yandan, ilgili uygulamayı sunan veri işleyen şirket (Uygulama Hizmeti Sunan Şirket) ile yalnızca aralarında bir hizmet sözleşmesi olduğunu vurgulamış ve şirketlerine üçüncü taraftan gelen bir ürüne ilişkin indirim hakkında yönetim hizmetlerini gerçekleştirmek üzere halihazırda kullanılmakta olan uygulama (ilk uygulama) ile site sakinlerine bilgi verildiğini, söz konusu indirimden yararlanabilmek için yeni uygulamaya (ikinci uygulama) üye olmanın tamamen ilgili kişinin kendi inisiyatifinde olduğunu, ikinci uygulamaya kendileri tarafından kişisel veri aktarımı yapılmadığını belirtmiştir.

İlk Uygulama Hizmetini Sunan Şirket ise Kurul'a verdiği cevaplarında, Site Yönetim Hizmeti Sunan veri sorumlusu Şirket'e, bilgisi ve isteği dahilinde, yönetim hizmetlerini gerçekleştirmek amaçlı kullandığı ilk uygulamada kayıtlı olan verilerin ikinci uygulamaya aktarılabilmesi için ilk uygulamaya giriş yetkisi tanımlaması yapıldığını, bu tanımlama ile birlikte Site Yönetim Hizmeti Sunan Şirket'in platform değişikliği ve/veya ek platform kullanımı sonucu ilk uygulamadaki kullanıcı bilgilerinin ikinci uygulamayla paylaşabildiğini ve bu paylaşımla birlikte ilgili kişinin sisteme giriş yapabilmesi için telefon numarasına bilgilendirme SMS'i gönderildiğini açıklamıştır.

Sonuç olarak, Kurul, Site Yönetim Hizmeti Sunan veri sorumlusu Şirket ile Uygulama Hizmeti Sunan Şirket arasında akdedilmiş olan Protokol maddeleri ile Uygulama Hizmeti Sunan Şirket'in sunduğu cevapları değerlendirdiğinde, Site Yönetim Hizmeti Sunan veri sorumlusu Şirket'in savunmalarını yerinde bulmayarak, site yönetim işlerinden ayrı bir amaca hizmet eden isteğe bağlı ikinci uygulamaya katılımın, **Kanun'un 5. maddesinin 2. fıkrasında yer alan işleme şartlarına dayandırılamayacağını, ancak ilgili kişinin açık rızası ile gerçekleştirilebilecek iken ilgili kişiden açık rıza alınmadığını** tespit etmiş ve Kanun'un 12. maddesinin 1. fıkrasına aykırı hareket eden veri sorumlusu Şirket hakkında Kanun'un 18. 1. fıkrasının (b) bendi kapsamında **100.000 TL idari para cezası uygulanmasına** karar vermiştir.

[2] Erişim için: https://www.kvkk.gov.tr/Icerik/6966/2021-359

3. Bir sigorta şirketi tarafından hizmetin açık rıza şartına bağlanması hakkındaki ihbara ilişkin 20/04/2020 tarihli ve 2021/389 sayılı karar[3]

Başvuruya konu olayda, ilgili kişi veri sorumlusu Sigorta Şirketi'nden bireysel emeklilik sözleşmesi yaptırmıştır. İlgili kişi, poliçe bilgilerine ulaşmak üzere veri sorumlusu Şirket'in internet sitesine girmeye çalıştığında kişisel verilerin işlenmesine rıza göstermek için karşısına çıkan bir onay kutucuğunu işaretlemek zorunda bırakıldığını ve kutucuğun işaretlenmemesi halinde hiçbir işlem yapılamadığını iddia etmiştir. İlgili kişi, veri sorumlusu Şirket'in bu kapsamda hukuka aykırı davranışları olduğunu ileri sürerek Kanun kapsamında gereğinin yapılmasını talep etmiştir.

a) Aydınlatma Metninin Mevzuata Uygunluğuna İlişkin Değerlendirme

Veri sorumlusu Şirket'in ilgili kişiye sunduğu aydınlatma metninde, ilgili kişilerin kişisel verileri için *"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."* ifadelerinin yer aldığı, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in ("Tebliğ") 5. maddesinin 1. fıkrasının (h) bendi uyarınca, kişisel verilerin **Kanun'un 5 ve 6. maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğinin açıkça belirtilmesi gerekirken, veri sorumlusu Şirket'in bu kapsamda bir bilgilendirmede bulunmadığı** Kurul tarafından tespit edilmiştir.

Öte yandan, aydınlatma metninin *"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 ve açıkça belirtilmesi gerektiği**, ayrıca metinde yer alan kurum ve kuruluşların isimlerinin de güncellenmediğinin anlaşıldığı belirtilmiştir.

Son olarak, ihbara konu online sistemde Sigorta Şirketi müşterilerinin tek bir kutucuk işaretlemek suretiyle hem aydınlatma metnine hem de kişisel verilerinin işlenmesine onay verdikleri gözlemlenmiştir. Ancak Kurul, Tebliğin 5. maddesinin 1. fıkrasının (f) bendi uyarınca kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, **aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiğini,** dolayısıyla kişisel verilerin işlenmesinin hukuki sebebinin açık rıza olduğu durumlar için ayrı bir açık rıza metninin de oluşturulması gerektiğini vurgulamıştır.

b) Açık Rızanın Hizmet Şartına Bağlanıp Bağlanmadığına İlişkin Değerlendirme

Kurul, veri sorumlusu Şirketin internet sitesindeki *"Bireysel Emeklilik Sözleşmesi Teklif Formu"*nda *"İnternet Ortamında Sunulacak Hizmetlere İlişkin Hükümler"* başlığı altında yer alan ifadelere göre, taraflar arasında akdedilen Hizmet Sözleşmesi ile ihbara konu uygulamanın

[3] Erişim için: https://www.kvkk.gov.tr/Icerik/6967/2021-389

kullanımında talep edilen verilerin esasen veri sorumlusunun internet üzerinden sunduğu hizmetlerde şifre dışında geliştirilen bir yöntem olarak görülebileceğini belirterek, online sistemde talep edilen verilerin Kanun'un 5. maddesinin 2. fıkrasında yer alan *"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* işleme şartına dayalı olarak işlenmesi gerektiğini, hizmetin açık rıza şartına bağlanmasının söz konusu olmadığı yönünde değerlendirme yapmıştır.

Bununla birlikte Kurul, ihbara konu uygulama kapsamında sunulan aydınlatma metninde aynı zamanda kişisel verilerin işlenmesi için açık rıza alındığı tespitinden hareketle, veri sorumlusu Şirket'in "kişisel veri işleme faaliyetinin hukuki sebebinin açık bir şekilde ifade edilmesi" yükümlülüğünü yerine getirmediğini tekraren vurgulamış, **açık rıza dışında yer alan işleme şartlarından biri bulunmasına rağmen yine de ilgili kişilerden açık rıza alınmasının aldatıcı ve hakkın kötüye kullanımı nitelikte olması sebebiyle,** veri sorumlusu Şirket'in bu eyleminin Kanun'un 4. Maddesinde sayılan genel veri işleme ilkelerinden *"hukuka ve dürüstlük kurallarına uygun olma"* ilkesine aykırı olduğunu belirlemiştir.

Sonuç olarak, Kurul, veri sorumlusu Şirketin Kanun'un 5.maddesindeki işleme şartları mevcut iken ilgili kişilerin açık rıza almasını *"hukuka ve dürüstlük kurallarına uygun olma"* ilkesine aykırı bularak Kanun'un 12. maddesinin 1. fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, Kanunun 18. maddesinin 1. fıkrasının (b) bendi uyarınca **250.000 TL idari para cezası uygulanmasına** karar vermiştir. Öte yandan Kurul, açık rıza ve aydınlatma metinlerini ayrı ayrı düzenlemesi ve aydınlatma yükümlülüğünü Kanun ve Tebliğ hükümleri ile uyumlu olacak şekilde düzelterek Kurula bilgi vermesi hususunda **veri sorumlusunun talimatlandırılmasına** hükmetmiştir.

4. Bir hastanenin veri ihlal bildirimi hakkında 20/04/2021 tarihli ve 2021/407 sayılı karar[4]

Veri sorumlusu Hastane'nin tespit edilmesinden 25 gün sonra Kuruma bildirdiği veri ihlaline konu olayda, hastanede çalışan bir hekimin aralarında özel nitelikli kişisel verilerinin de bulunduğu hasta dosyalarını arşivden alarak hastane çalışanları aracılığıyla hastane dışına çıkardığı iddia edilmiştir.

a) Teknik ve İdari Tedbirlere İlişkin Değerlendirme

Veri ihlaline ilişkin yapılan incelemede, arşiv dosyalarının bulunduğu arşiv odasına yetkili olmayan kişilerin de giriş sağlayabildiği ve kamera kayıtlarının kontrolünün sağlanmadığı tespit edilmiş ve dolayısıyla idari tedbirlerin yeterli ölçüde alınmadığı değerlendirilmiştir.

İhlalden 789 hasta etkilenmesine rağmen, yalnızca 54 adet hasta dosyası geri alınmış, bu nedenle hasta dosyalarının kaybı önlenememiş ve gerekli tedbirler alınmamıştır.

[4] Erişim için: https://www.kvkk.gov.tr/Icerik/6968/2021-407

Ayrıca, hastaların sağlık ve genetik verileri kapsamında özel nitelikli kişisel verilerinin işlenmesine ilişkin çalışanlara kişisel verilerin korunması eğitiminin yeterli bir şekilde verilmediği tespit edilmiştir.

Öte yandan, veri sorumlusu Hastane'nin söz konusu veri ihlalini 17 gün sonra tespit etmesi, kişisel veri güvenliği politika ve prosedürlerini yeterli ve iyi bir şekilde hazırlamadığı ve güvenlik önlemlerini etkili bir şekilde almadığı hususlarının gerekçesi olmuştur.

Açıklanan bu nedenlerle, Kanun'un 12. maddesinin 1. fıkrası çerçevesinde **veri güvenliğini sağlamaya yönelik gerekli tedbirleri almayan** veri sorumlusu hakkında, Kanun'un 18. maddesinin 1. fıkrasının (b) bendi uyarınca **450.000 TL. idari para cezası uygulanmasına** karar verilmiştir.

b) Kuruma ve İlgili Kişilere Yapılan Bildirime İlişkin Değerlendirme

Veri sorumlusu hastane, veri ihlalini tespit edilmesinden 25 gün sonra Kurula bildirmiş ve geç bildirim sebebi olarak hastaneden çıkarılan dosyaların suçüstü yakalanılması üzerine başlatılan adli süreçleri göstermiştir. Yürütülen bu sürece rağmen, veri sorumlusu hastane tarafından hastaneye gelen bir kişi dışında ilgili kişilere söz konusu ihlal bildirilmemiştir.

Sonuç olarak, Kurul, Kanun'un 12. maddesinin 5. fıkrası ve Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kurul'un 24.01.2019 tarih ve 2019/10 sayılı Kararı'nda yer alan "en kısa sürede" ifadesinin 72 saat olarak yorumlanmasına yönelik değerlendirmeleri çerçevesinde **veri ihlali bildirim yükümlülüğünü yerine getirmeyen** veri sorumlusu hakkında Kanun'un 18 inci maddesinin 1. fıkrasının (b) bendi uyarınca **150.000 TL idari para cezası uygulanmasına** ve ihlalden etkilenen ilgili kişilere 24.01.2019 tarih ve 2019/10 sayılı Karar'da yer alan hususları içeren bir bildirim yapılarak sonucundan Kurula bilgi verilmesi hususunda **veri sorumlusunun talimatlandırılmasına** karar verilmiştir.

Bilgilerinize sunarız.

Saygılarımızla,

Koyuncuoğlu & Köksal Avukatlık Bürosu

* Bilgi notumuzda yer verilen açıklamalar, Türkiye Cumhuriyeti'nin yürürlükte olan mevzuatı ve ilgili resmi mercilerin kamuya yaptığı bilgilendirmeler esas alınarak hazırlanmış olup, tereddütlü hususlarda nihai işlemler gerçekleştirilmeden evvel tarafımızdan görüş ve destek alınmasını tavsiye ederiz. Aksi takdirde, burada yer verilen açıklamalar temel alınarak yapılacak işlemler ve bunların sonuçlarıyla ilgili olarak Avukatlık Büromuz sorumlu tutulamaz.