15 Şubat 2018

FRANSA ULUSAL BİLİŞİM ve ÖZGÜRLÜKLER KOMİSYONU'NUN DARTY KARARINDAN DERSLER

Fransa Ulusal Bilişim ve Özgürlükler Komisyonu (CNIL) (Komisyon), 8 Ocak 2018 tarihinde verdiği kararla elektronik şirketi Darty'ye 100.000 Avro para cezası verdi. Bu karar, Kişisel Verileri Koruma Kurulu'nun (Kurul) 21.12.2017 tarih ve 2017/62 sayılı ilke kararı ile birlikte değerlendirildiğinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) uygulaması bakımından önümüzdeki süreçte büyük öneme sahip olacaktır.

Karara konu olan olayda, Darty'nin satış sonrası hizmetlerine ilişkin olarak internet sitesinde güvenlik açığı olduğu şeklindeki bir şikâyet üzerine Komisyon tarafından başlatılan incelemede; başvuru formuna ilişkin linkteki açık sebebiyle, satış sonrası hizmet talebi için form dolduran Darty müşterilerinin diğer müşterilerin isim, soy isim, e-posta adresi ve telefon numarası gibi bilgilerine kolaylıkla ulaşılabildiği tespit edildi.

Komisyon tarafından yapılan incelemelerde, satış sonrası hizmete ilişkin olarak e-posta adresi ve şifre ile başvuru formu dolduran müşterilere başvurularını takip edebilmek amacıyla http://darty.epticahosting.com/selfdarty/requests.do?id=*XXX* şeklinde bir URL adresi gönderildiği tespit edilmiştir. Yalnızca bu adresteki tanımlama numarasının değiştirilmesiyle, örneğin bir sonraki ardışık numaranın yazılmasıyla, diğer kullanıcıların formlarına da ulaşılabildiği anlaşılmıştır. Komisyon bu metotla toplamda 912.938 kullanıcının formunun dolayısıyla da bu formlar aracılığıyla müşterilerin kişisel verilerinin ulaşılabilir olduğunu ortaya çıkarmıştır. Bunun üzerine Darty, Komisyon tarafından kişisel verilerin ihlali sebebiyle uyarılmış ve söz konusu hatanın derhal düzeltilmesi talep edilmiştir.

Daha sonra şirkette yapılan incelemelerde de aynı durumun devam ettiği fark edilmiş; uyarıya rağmen bu süreçte yeni formların işleme konulduğu ve kişisel verilere halen ulaşılabilir olduğu tespit edilmiştir. Ancak yerinde incelemeler yapıldıktan sonra sorunun tamamen çözüldüğü Komisyona iletilmiştir. Ayrıca Komisyon, Darty'nin söz konusu hataya sebep olan online formların oluşturulması konusunda EPTICA adında başka bir şirketten hizmet aldığını öğrenmiştir. Satış sonrası talepler için müşterilerin ulaşabileceği iki yol daha mevcuttur ancak bahsi geçen URL adresi yoluyla talep formu oluşturulması işlemi EPTICA şirketinden sağlanan hizmet yoluyla uygulamaya konulmuştur.

Kararda temel olarak Darty şirketinin, satış sonrası talepler çerçevesinde, müşterilerinin kişisel verilerinin güvenliğinin sağlanması için gerekli tedbirleri alıp almadığı tartışılmıştır. Darty, kişisel verilerin ihlaline sebep olan URL adresi bakımından veri sorumlusu niteliğine sahip olmadığını, online formun içeriğini, formatını belirleyen ve geliştiren EPTICA şirketinin veri sorumlusu olarak kabul edilmesi gerektiğini iddia etmiştir. Komisyon ise veri sorumlusunun tespitinde; toplanacak verilerin neler olduğu, ne kadar süreyle saklanacağı ve bu verilere kimlerin erişebileceği gibi unsurlara karar verenin belirleyici olduğunu belirtmiştir. Veri işleyenin faaliyetlerinin ise daha çok işlemenin teknik boyutuyla ilgili olduğunu vurgulamıştır. Ancak veri işleyenin; elde ettiği verileri, sözleşmesel yetkilerini aşarak, katma değer içeren bir hizmet üretmek maksadıyla kullanması halinde veri sorumlusu olarak değerlendirilmesi söz konusu olabilecektir.

Komisyon mevcut olayda, erişilen talep formunun iki şirket arasındaki sözleşmenin gereği olarak EPTICA tarafından kullanıma sunulmasının, EPTICA'yı veri sorumlusu olarak değerlendirmek bakımından yeterli olmadığını belirtmiştir. Ayrıca söz konusu formlar aracılığıyla toplanan verilere yalnızca Darty şirketi çalışanlarının erişim yetkisi olduğunu da vurgulayan Komisyon, verilerin işlenmesi bakımından Darty şirketinin veri sorumlusu olarak değerlendirilmesi gerektiğine kanaat getirmiştir.

Darty formların büyük bir kısmının banka kartı numarası gibi hassas verileri içermediğini dolayısıyla önemli mağduriyetlere yol açmayacak nitelikte veriler olduğunu belirtmiştir. Ancak Komisyon, **kişisel veriler kasıtlı olarak ya da olmayarak yetkisiz üçüncü kişiler tarafından erişilebilir hale geldiği takdirde ihlalin oluşacağını** hatırlatmıştır. Nitekim olayda da bir güvenlik açığının mevcut olduğunu ve URL'lerin filtrelenmesi işleminin veri sorumlusu tarafından bilgi güvenliği konusunda test edilmesi gereken temel konulardan birisi olduğunu önemle belirtmiştir.

Ek olarak, söz konusu hatanın ancak Darty'ye yapılan ikinci uyarı neticesinde sonlandırıldığını ve arada geçen 13 günlük süre içerisinde 5.783 formun daha müşterilerce oluşturulduğu vurgulanmıştır. Ayrıca kararda, bu süre zarfında Darty'nin güvenlik açığının kapatılması konusunda EPTICA'ya yönelik olarak günlük takip yapmadığı, ilk yapılan uyarının ardından yalnızca bir kere daha talepte bulunmakla yetindiği ifade edilmiştir.

Sonuç olarak, bütün bu unsurlar göz önünde bulundurularak yetkisiz kişilerin işlenen verilere erişiminin engellenmesi adına gerekli önleyici tedbirleri almadığı gerekçesiyle Darty'nin kişisel verilerin korunmasını ihlal ettiğine karar verilmiştir.

Söz konusu kararın ülkemizdeki kişisel verilerin korunması bakımından iki önemli sonucu bulunmaktadır:

> **1) Veri işleme faaliyetinin dışardan hizmet alımı yoluyla gerçekleştirilmesi, veri sorumlusunun sorumluluğunu ortadan kaldırmamaktadır.**
>
> **2) Veri sorumlusu; veri güvenliğinin sağlanması adına gerekli olan, başta önleyici olmak üzere, tüm teknik ve idari tedbirleri almalıdır. Söz konusu önleyici tedbirlerin yerine getirilmemesi dahi ihlalin oluşumuna sebep olabilecektir.**

Bilindiği üzere 6698 sayılı Kanun'un 3/ı maddesine göre veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır. Veri işleyen ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir.

Komisyon'un kararında da belirtildiği üzere dışardan hizmet alımı yoluyla veri sorumlusunun kendisine ait kişisel verilerin işlenmesini başka bir şirkete sağladığı durumda dahi kendi niteliği ve yükümlülükleri değişmemektedir. Bu kapsamda 6698 sayılı Kanun'un 12/1. maddesinde vurgulandığı üzere veri sorumlusu; "**kişisel verilerin hukuka aykırı olarak işlenmesini önlemek"**, **"kişisel verilere hukuka aykırı olarak erişilmesini önlemek"** ve **"kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak"** zorundadır.

Fransa'daki düzenlemelere paralel olarak 6698 sayılı Kanun da kişisel veri işleme faaliyetlerine ilişkin hukuki yükümlülüklerin yerine getirilmesi bakımından veri sorumlusunu esas alan bir sorumluluk rejimini benimsemiştir. Nitekim Kanun'un 12/2. maddesinde de düzenlendiği üzere, **"veri sorumlusunun kişisel**

verilerin işlenmesi faaliyetlerini yaptığı sözleşme ile veri işleyene devretmesi halinde dahi yükümlülükleri devam edecek" ve veri işleyen ile birlikte müştereken sorumlu olacaktır. Dolayısıyla veri sorumlusu şirketler bakımından veri işleyen üzerindeki denetim yükümlülüğü devam edecektir.

Yukarıda yer verilen Darty kararının en önemli sonuçlarından birisi de veri sorumlusunun kişisel verilerin korunması için yeterli önleyici teknik tedbirleri alma gerekliliğidir. Nitekim Komisyon, bahsi geçen URL filtrelemesi tedbirinin bilgi güvenliğini temin etmeye yönelik gerekli bir teknik tedbir olduğunu önemle vurgulamıştır. Komisyon, benzer şekilde 2017 yılında Hertz şirketine ceza verdiği kararda da belirttiği üzere, **yetkisiz kişilerin kişisel verilere erişimini engellemek adına gerekli teknik tedbirlerin alınmamış olmasını başlı başına ihlalin oluşumu için yeterli görmüştür.** Örneğin Hertz kararında güvenlik açığının derhal giderilmesi adına şirket tarafından gerekli adımların atılmış olması dahi Komisyon tarafından ceza uygulanmasını engelleyememiştir.

Hatırlanacağı üzere ülkemizde de Kurul yayımlamış olduğu 21.12.2017 tarih ve 2017/62 sayılı ilke kararında veri güvenliğinin sağlanmasına ilişkin olarak veri sorumlusunun yükümlülüklerine dikkat çekmiştir. Kararda özellikle banko, gişe ve masa gibi müşteriye hizmet sunulan alanlarda yaşanan problemler değerlendirilmiştir. Kurul, başta bankacılık ve sağlık sektörleri olmak üzere birden fazla çalışan ile bitişik düzende müşteriye hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik hizmetlerinin yapıldığı kuruluşlar gibi özel ve kamu kurum ve kuruluşlarının kişisel verilerin korunması konusunda gerekli teknik ve idari tedbirleri alması gerektiğini vurgulamıştır. Bu tedbirler, Kurul tarafından iki şekilde somutlaştırılmıştır: 1) Banko, gişe, masa gibi bölümlerde yetkisi olmayan kişilerin yer almaması gerekmektedir. 2) Aynı anda birbirlerine bitişik veya yakın şekilde hizmet alan müşterilerin birbirlerinin kişisel verilerini duymasını, görmesini veya ele geçirmesini engelleyecek biçimde tedbirlerin alınması gerekmektedir.

Kurul tarafından yayımlanan kararda çeşitli sektörler spesifik olarak sayılmış olsa da uygulama bakımından pek çok sektörü etkileyebilecek nitelikte olduğunu söylemek mümkündür. Nitekim kararda veri güvenliğine ilişkin önleyici tedbirlerin önemine dikkat çekilmiştir. Kanun'un 12. maddesi çerçevesindeki yükümlülükleri hatırlatan Kurul, **gerekli teknik ve idari tedbirleri almaması halinde veri sorumlusunun Kanun'un 18. maddesi çerçevesinde cezalandırılacağını** belirtmiştir.

Bu noktada, veri güvenliği kapsamında Kurul tarafından yakın zamanda yayımlanan "Kişisel Veri Güvenliği Rehberi"nin alınması gerekli teknik ve idari tedbirleri somut bir şekilde ortaya koyduğu da hatırlatılmalıdır. Bilindiği üzere Rehber'de; veri sorumlusu tarafından düzenli olarak kontroller yapılması, bu yapılan kontrollerin belgelenmesi, geliştirilmesi gereken hususların belirlenmesi ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmesi gerektiği önemle vurgulanmıştır. Ayrıca veri sorumlusunun yapacağı ya da yaptıracağı bu denetimler kapsamında hizmet sağlayıcıyı yerinde inceleyebileceği de belirtilmiştir.

Sonuç olarak, Fransa Ulusal Bilişim ve Özgürlükler Komisyonu'nun Darty kararı ve Kişisel Verileri Koruma Kurulu'nun 2017/62 sayılı ilke kararı birlikte değerlendirildiğinde veri sorumlusu şirketlerin kişisel verilerin korunması için gerekli tüm idari ve teknik tedbirleri alma yükümlülüğü son derece büyük önem arz etmektedir. **Şüphesiz ki bu yükümlülük yalnızca ihlal gerçekleştikten sonra alınacak tedbirleri değil, ihlalin önlenmesi adına önceden alınması gerekli tedbirleri de kapsamaktadır.** Bu çerçevede veri işleme faaliyetinin dışardan hizmet alımı yoluyla sağlanması dahi veri sorumlusunun bu yükümlülüklerini

ortadan kaldırmayacaktır. Bu nedenle veri sorumlusu şirketlerin, Kanun kapsamındaki uyum faaliyetlerini en kısa sürede tamamlayarak veri güvenliği ihlalini önleyecek teknik ve idari tüm tedbirleri alması gerekmektedir.

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu, 4054 sayılı Rekabetin Korunması Hakkında Kanun'a benzer bir metotla, kişisel verilerin korunmasına ilişkin AB mevzuatı esas alınarak hazırlanmıştır. 4054 sayılı Kanun'un gelişimi bakımından AB ülkelerindeki uygulamaların çok büyük bir öneme sahip olduğu tecrübesi göz önünde bulundurulduğunda, benzer bir uyum ihtiyacının 6698 sayılı Kanun bakımından da söz konusu olacağı açıktır. Bu nedenle kişisel verilerin korunmasına ilişkin olarak AB ülkelerindeki gelişmelerin yakından takip edilmesi doğru ve tutarlı politikaların entegre edilmesi bakımından büyük bir önem arz etmektedir.

Arı Avukatlık Bürosu

ARI Avukatlık Bürosu

Atatürk Mah. Ataşehir Bul.
42 Ada Gardenya 7/1 Blok Kat:11 No:68
34758 Ataşehir/İSTANBUL
Tel/Faks: +90 (216) 455 09 81/455 46 05
e-posta: info@ari.av.tr
Url: www.ari.av.tr