



## KİŞİSEL VERİLERİMİZ

# Güvende mi?

Türkiye Finans Katılım Bankası A.Ş. Hukuk Müşavirliği-Müşavir Avukat **Saadet Gündüz Alkan**  
Türkiye Finans Katılım Bankası A.Ş. KVK Yönetimi Servisi-Yöneticisi **Emre Gizlenci**

**6** 698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") 7 Nisan 2016 tarihinde Resmî Gazete'de yayımlandıktan sonra daha çok hayatlarımıza dâhil olan kişisel verilerin korunması kavramı, aslında bundan çok daha önce hukukumuzda farklı düzenlemeler içerisinde yer alıyordu. İlk kez bu kanunla konuyu düzenleyen genel bir kanun getirilmiş oldu. Bizi genel bir kanuni düzenleme hazırlanmasına yönelten etkenler ise, vize serbestisine yönelik AB ile yürütülen üyelik müzakereleri, uluslararası iş birliği ve ticaretin artırılması ile insan haklarının etkin biçimde korunması olarak sıralanabilir.

Öncelikle belirtmek gerekir ki; kişisel verilerimiz kişilik hakkımız kapsamında Türk Medeni Kanunu'nun 24 ve devamındaki hükümlere göre korunmaktaydı. Ayrıca Anayasanın 20. maddesine 2010'da getirilen ek fıkra ve

2004'te Resmî Gazete'de yayımlanan Türk Ceza Kanunu'nun ("TCK") 135 ve devamındaki hükümleri kişisel verilerin korunmasına ilişkin hüküm getirdiğinden önemlidir. Avrupa'da ise 1970'li yıllardan itibaren kişisel verilere ilişkin yasal düzenlemeler getirilmiştir. Örnek vermek

gerekirse; Almanya Hessen Eyaleti veri koruma kanunu 1970, İsveç veri koruma kanunu 1973 ve Fransa veri koruma kanunu 1978 tarihlidir.

Ülkemiz bankacılık sektörü açısından ise verilerin korunması yeni bir düzenleme değildir. Bankacılık Kanunu'nun 73. maddesinde müşteri sırrının ve banka sırrının korunması gerektiği yer almakta olup 159.

maddeye göre 73. maddeyi ihlal edenlerin bir yıldan üç yıla kadar hapis cezası ve bin günden iki bin güne kadar adli para cezası ile cezalandırılacağı hüküm altına alınmıştır. Keza sektörde önemli düzenlemelerden biri de 2007

*Günümüzde kamu kurum ve kuruluşları ile özel şirketlerde pek çok kişisel veri bulunmaktadır*

tarihli "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelerle İlişkin Tebliğ"dir. Bu hâliyle bankacılık sektörü ülkemizde verinin ve sırların korunması tahtında öteden beri Bankacılık Düzenleme ve Denetleme Kurumu'nun şemsiyesi altında sıkı şekilde regüle edilmektedir.

Günümüzde kamu kuruluşlarında ve özel şirketlerde pek çok veri ve dolayısıyla kişisel veri bulunmaktadır. Bu verilerin işlenmesi, analiz edilmesi yoluyla farklı verilere de erişmek mümkün olabilmektedir. Örneğin; akıllı telefonlara uygulamalar yüklerken uygulamalar sizlerden konum, kamera, mikrofon, takvim gibi verilere erişim için izin vermenizi istemektedir, eğer sadece uygulamayı kullanırken erişmelerine izin verme seçeneğini seçmezseniz başka zamanlarda da sizin konum, kamera, mikrofon, takvim gibi verilerinize erişebilmekte ve eriştikleri verileri size başkaca ürün pazarlamada kullanabilmektedirler. Bu ve buna benzer nedenlerle kişisel verilerin korunması ve diğer menfaatler dengesinin sağlanması zarureti doğmuştur.

Kişisel verilerin hukuka aykırı yollardan yetkisiz kişilerin ellerine geçmesi sebebiyle ilgili kişilerin maddi-manevi zararlarının doğması, kişilerin yapacağı seçimlerin yönlendirilmesi ve yönetilmesi mümkündür. Zira bu durumun bir örneği Facebook'un ABD'de yargılanmasına sebep olan 50 milyon kişinin kişisel verilerinin Cambridge Analytica şirketi tarafından analiz edilmesi ve kişilerin siyasi tercihlerinin yönlendirilmesi vakasında görülmektedir.

Bu arada geçtiğimiz günlerde Avrupa Birliği Veri Koruma Tüzüğü'nün ("GDPR") 25 Mayıs 2018'de yürürlüğe girmesinden sonra ilk kez GDPR'a istinaden Portekiz'de ceza verilmiştir. Bu olayda, Portekiz'de bir hastanenin sistemine personelinin gerçek olmayan hesaplarla kaydolabildiği, hastanede 296 doktor olmasına rağmen hastanenin sisteminde kayıtlı 985 doktor olduğu, bu nedenle Portekiz Veri Otoritesi'nin ("CNPD") bu hastaneye 400.000 Euro ceza verdiği, hastanenin de bu cezaya itiraz ettiği belirtilmektedir. Cezaların caydırıcı olması kişisel verilerin korunması için özen gösterilmesi bakımından önemlidir. KVKK'nın 18. maddesine göre veri güvenliğine ilişkin yükümlülüğünü yerine getirmeyenler aleyhine hükmedilebilecek idari para cezaları 15.000 TL ile 1.000.000 TL arasında değişmektedir. Ayrıca Türk Ceza Kanunu'nun 135-140. maddeleri arasında düzenlenen suçlar oluştuğunda hapis cezaları vardır.



VERİ GÜVENLİĞİNE  
İLİŞKİN  
YÜKÜMLÜLÜĞÜNÜ  
YERİNE  
GETİRMEYENLER  
ALEYHİNE  
HÜKMEDİLEBİLECEK  
İDARİ PARA  
CEZALARI

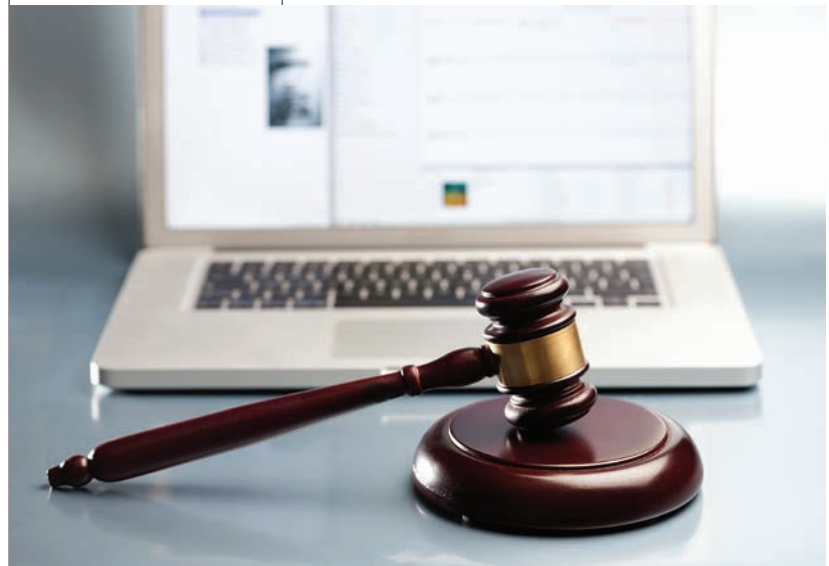
**15.000**  
TL İLE  
**1.000.000**  
TL ARASINDA  
DEĞİŞMEKTEDİR

## Günümüz teknolojisinde kişisel verilerin güvende olması bireylerin bu kişisel verileri hukuki çerçevede kullanmasına bağlıdır

Ülkemizde KVKK'nın 12. maddesine istinaden veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Keza KVKK'nın 12. maddesine göre, veri sorumlusu adına bu kişisel verileri işleyenler de müştereken sorumlulardır.

Bu anlamda KVKK ile beraber düzenleyici ve denetleyici bir otorite olarak karşımıza çıkan Kişisel Verileri Koruma Kurumu'nun ("Kurum") büyük bir misyonu bulunmaktadır. Kurum yayınladığı altı adet yönetmelik, iki adet tebliğ, yirmi bir adet kurul kararı, iki adet taahhütname, yirmi bir adet rehber, pek çok ilde düzenledikleri farkındalık toplantıları, sosyal medyayı etkin olarak kullanma ve yayınladıkları videolarla, bir kısım veri sorumluları için kayıt aşamasını başlattıkları VERBİS'le ve 198 Alo Veri Koruma hattıyla kişisel veri koruma faaliyetlerine hızla devam etmektedir.

KVKK ile ilgili yüksek yargı kararlarına baktığımızda on civarında karar olduğunu görmekteyiz. Mevcut kararlarda icra dairelerinin KVKK'ya aykırı olarak kişisel verileri talep





*Açık rıza,  
belirli bir  
konuya ilişkin,  
bilgilendirmeye  
dayanan ve  
özgür iradeyle  
açıklanan  
rıza olarak  
tanımlanmıştır*

ettiği ve işlediği görülmektedir. Bu alanın gelişmesi ve kişisel verilerin güvende olabilmesi için yaşanan vakaların yargı kararlarına dönüşmesine de ihtiyaç bulunmaktadır. Kişisel verilerin KVKK'nın 4. maddesinde belirtilen ilkelere aykırı olarak sınırsız süre tutulması bireysel özerkliğe zarar vermektedir. Diğer taraftan unutulma hakkı (right to be forgotten) vardır. Bireyin üzerinde olumsuz etkileri olabilecek durumlar hâlen erişilebilir durumda ise bireyin bunun kaldırılmasını talep etme hakkı vardır.

Sonuç olarak; günümüz teknolojisinde kişisel verilerin güvende olmasının bireylerin bu kişisel verileri hukuki çerçevede kullanmasına bağlı olduğu kanaatindeyiz. Aksi takdirde kişisel veriler hukuki çerçevenin dışında kullanıldığında toplum için çok büyük zararları olabilecektir. 2016 yılından beri hayatımızda yer edinen KVKK ile beraber bir Anayasal hak olan kişisel verinin korunması ile ticari hayatın gelişerek paralel şekilde ilerleyeceği, bu konuda kurulan düzenleyici ve denetleyici otoritenin de uygulamaya yön vereceği kanaatindeyiz.

#### **Kanun Kapsamında Hayatımıza Yeni Giren Form ve Bilgilendirmeler**

KVKK'da veri sorumlularına iki yıllık uyum süresi tanınmıştı. Bu süre 7 Nisan 2018 tarihi itibarıyla

de sona erdi. Bu kapsamda hatırlayanlar olacaktır; perakende, mağazacılık, giyim, akaryakıt, ulaşım gibi sektörlerden doğrudan müşteri verisi işleyen firmalar, kullanıcılarını SMS ve elektronik posta yağmuruna tuttu. Üyelik sözleşme ve koşullarını yenileyen işletmeler, müşteri ve üyelerinden yasal izinleri alabilmek için müşterilerine bilgilendirme yaptılar. Bu bilgilendirmelerin en önemli sebebi, verilerin elde edilmesi sırasında ilgili kişilere karşı aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5 bin TL ile 100 bin TL arasında idari para cezası uygulanmasıdır. Peki, nedir bu "Aydınlatma Yükümlülüğü?"

Kanun, kişisel verileri işlenen ilgili kişilere bu verilerinin kim tarafından, hangi amaçlarla ve hukuki sebeplerle işlenebileceği, kimlere hangi amaçlarla aktarılacağı hususunda bilgi edinme hakkı tanımakta ve bu hususları, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ele almaktadır.

Aydınlatma yükümlülüğünün yerine getirilmesi hususunda kanunda öngörülen herhangi bir şekil şartı bulunmamaktadır. Dolayısıyla kural olarak söz konusu bilgilerin veri sahibine sözlü olarak (örneğin, fiziki ortamda ya da çağrı merkezi kanalıyla) verilmesi yeterlidir. Ancak aydınlatma yükümlülüğünün yerine getirildiğinin ispatının veri sorumlusuna ait olduğu göz önüne alındığında, aydınlatmanın yazılı olarak veya elektronik ortamda

kayıtlara ilişkin kopyaların saklanması daha

#### **ORGAN BAĞIŞ ORANI**

**DANİMARKA**  
%4

**HOLLANDA**  
%28

**İNGİLTERE**  
%17

**ALMANYA**  
%12

**AVUSTURYA**  
%100

**BELÇİKA**  
%98

**FRANSA**  
%100

**MACARİSTAN**  
%100

**POLONYA**  
%100

**PORTEKİZ**  
%100

**İSVEÇ**  
%86



## “Açık Rıza” kavramına en iyi örnek ülkeler arasında organ bağış oranlarının farklılık göstermesidir. Bunun sebebi basit bir düzenlemedir

sağlıklı olacaktır. Bu noktada şunu belirtmekte de fayda var: Aydınlatma metinlerinin veri sahibi tarafından onaylanması aranmamaktadır, bilginin kişiye sunulduğunun ispat edilmesi yeterli olacaktır.

Kanunla birlikte hayatımıza giren diğer bir ifade ise, “Açık Rıza”. Peki, açık rıza nedir ve hangi yöntemle alınmalıdır? sorusuna cevap vermeden önce gelin birlikte ilginç bir araştırmayı birlikte inceleyelim: Avrupa’da yapılan bir araştırmada ülkelerin organ bağış oranları inceleniyor. Bazı ülkelerin yüksek bağış oranına sahip olduğu, bazılarının ise çok düşük oranda kaldığı tespit ediliyor. Araştırmacılar önce bunun nedenini; dinî, kültürel, ekonomik ve yaşam tarzı farklılığı olduğunu düşünüyor. Ancak ülke detayına inildiğinde; ülkelerin dinî, kültürel ve ekonomik olarak birbirlerine çok benzedikleri ve başka bir sebebin olması gerektiğini fark ediyor. Daha sonra yapılan incelemeler bu büyük farklılığın çarpıcı nedenini ortaya çıkarıyor: “Ülkelerin kullandıkları organ bağış formu”...

Danimarka, Hollanda ve Almanya gibi ülkelerde öldükten sonra organlarının bağışlanmasını istiyorsanız formdaki kutucuğu işaretlemeniz gerekiyor. Ancak Avusturya, Fransa ve Portekiz gibi ülkelerde organ bağışı yapmak istemiyorsanız kutucuğu işaretlemeniz gerekiyor. Basit gibi duran bir düzenleme ile çok farklı sonuçlar elde etmenin mümkün olduğunu bu araştırmada görmüş oluyoruz. Bu araştırma alınacak açık rızalar için hem veri sorumluları hem de ilgili kişiler açısından önemli dersler veriyor.

Açık rızaya tekrar dönecek olursak: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza olarak tanımlanmıştır. Tanımdan hareketle açık rızanın aşağıdaki üç şartı taşınması gerektiği söylenebilir:

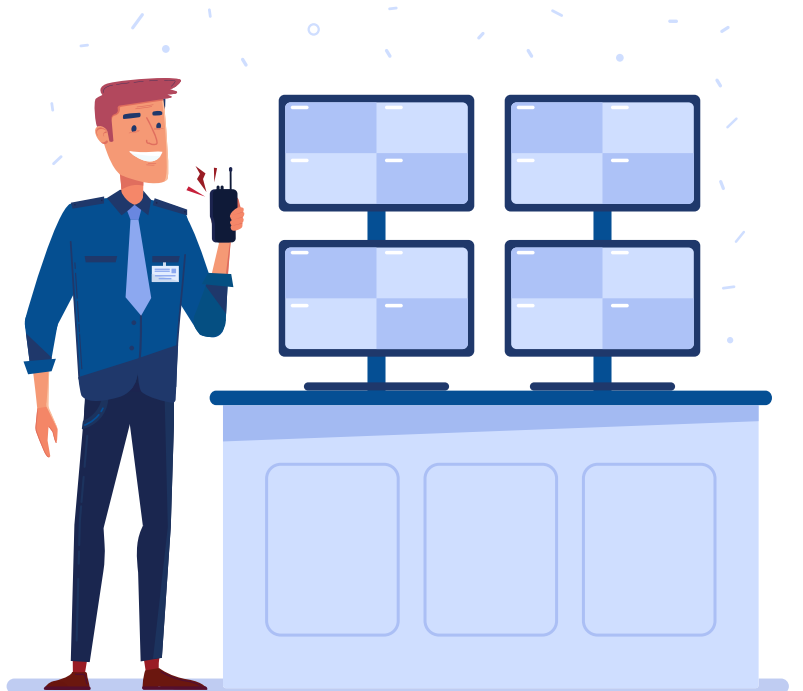
- 1) Açık Rızanın Belirli Bir Konuya İlişkin Olması
- 2) Açık Rızanın Özgürce Verilmesi
- 3) Açık Rızanın Bilgilendirmeye Dayanması

Kanunda açık rıza alınmasına özellikli bir şekil şartı getirilmemiştir. Ancak ileride bir uyumsuzluk olması durumunda, açık rıza alındığının gösterilebilmesi için ispat edilebilir



# 198

ALO VERİ KORUMA HATTIYLA KİŞİSEL VERİ KORUMA FAALİYETLERİ HIZLA DEVAM ETMEKTEDİR



yöntemlerle rıza alınması gerekmektedir. Açık rıza ilgili kişiler tarafından istenildiği zaman geri alınabilmektedir. Bu bilgiler ışığında, kanun ile birlikte hayatımıza yeni giren; form, bilgilendirme ve prosedürlere maruz kaldığımız düşünülse de, verilerimizin kim tarafından hangi amaçlarla işlendiğinin bilinmesi, yasa dışı aktarımların önüne geçilmesi ve bazı veri işleme faaliyetlerinin açık rızaya bağlanması, hem veri hem de veri sahiplerinin haklarını koruma anlamında önem arz etmektedir.