

## SİRKÜLER NO: 2019/26

**Konu: Kişisel Verilerin Korunması Kanunu hk.**

**Özet:** Avrupa Birliğine uyum kapsamında hazırlanan Kişisel Verilerin Korunması Kanunu, 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

- **Kanunun amacı, kişisel verilerin işlenmesinde;**
  - Özel hayatın gizliliği
  - Kişilerin temel hak ve özgürlüklerini korumak ve
  - Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.
- **Kanun başlıca iki kitleyi ilgilendirmektedir;**
  - Kişisel verileri işlenen gerçek kişiler (Personel, müşteri, şirket yetkilisi veya ortağı gibi)
  - Bu verileri işleyen gerçek ve tüzel kişiler (Kamu kurumları, ticari ve sınai işletmeler, reklam şirketleri, elektronik ticaret şirketleri, sağlık kuruluşları ve hastaneler, telekomünikasyon şirketleri gibi)
- **Kanunun uygulama alanı;**
  - Kişisel veri toplayan, barındıran, işleyen, depolayan ve gerektiğinde anonim hale getiren veya silen kişi veya kuruluşlar açısından, uyulması gereken kurallar belirlenmektedir.
  - Verileri işlenen gerçek kişiler açısından da kişisel verilerine yönelik haklarının korunmasına ilişkin usul ve esaslar ile ihlalde bulunanlara uygulanacak yaptırımlar belirlenmektedir.
- **Kanunun geniş özetine aşağıda, uygulamaya ilişkin basit bir akış şemasına da sirkülerin sonunda yer verilmiştir.**

### 6698 sayılı KİŞİSEL VERİLERİN KORUNMASI KANUNU (Geniş özet)

#### Kanunun Amacı

Kişisel verilerin işlenmesinde;

- Özel hayatın gizliliğini korumak
- Kişilerin temel hak ve özgürlüklerini korumak
- Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

#### Kapsama Giren Kişiler

- Kişisel verileri işlenen gerçek kişiler ile
- Bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler.

#### Başlıca Tanımlar

- **Kişisel veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- **Özel nitelikli kişisel veri:** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri,
- **Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

- **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,
- **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- **Kişisel verilerin işlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- **İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,
- **Açık rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- **Anonim hâle getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

### **Kişisel Verilerin İşlenmesinde Genel ilkeler**

- 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.

### **Kişisel verilerin işleme şartları**

- Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.
- **Genel nitelikli kişisel verilerin ilgili kişinin açık rızası aranmaksızın işlenebilecek işlenebilme şartları:**
  - a) Kanunlarda açıkça öngörülmesi.
  - b) 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.
  - c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
  - d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
  - e) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
  - f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
  - g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.
- **Özel nitelikli kişisel verilerin ilgili kişinin açık rızası aranmaksızın işlenebilecek işlenebilme şartları:**
  - h) Sağlık ve cinsel hayat dışındaki genel nitelikli kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.
  - i) Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak;
    - Kamu sağlığının korunması,
    - Koruyucu hekimlik,
    - Tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi,
    - Sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla,

- i. Sır saklama yükümlülüğü altında bulunan kişiler veya
- ii. Yetkili kurum ve kuruluşlar tarafından
- iii. Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla işlenebilir.

### **Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi**

Kanuna uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

### **Kişisel verilerin aktarılması**

- Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.
- Kişisel verilerin ilgili kişinin açık rızası aranmaksızın işlenmesine ilişkin şartlar, yeterli önlemler alınmak kaydıyla bu verilerin aktarılmasında da geçerlidir.
- Kişisel verilerin yurt dışına aktarılmasında, kişisel verinin aktarılacağı yabancı ülkede;
  - o Yeterli korumanın bulunması,
  - o Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

## **HAKLAR VE YÜKÜMLÜLÜKLER**

### **Veri sorumlusunun aydınlatma yükümlülüğü**

Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

- a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
- b) Kişisel verilerin hangi amaçla işleneceği,
- c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür.

### **İlgili kişinin hakları**

Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

- a) Kişisel veri işlenip işlenmediğini öğrenme,
- b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir.

### **Veri güvenliğine ilişkin yükümlülükler**

#### **(1) 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.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

## **BAŞVURU VE ŞİKÂYET**

### **Veri sorumlusuna başvuru**

(1) İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

(2) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir.

(3) Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir.

### **Kurula şikâyet**

(1) Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

(2) Veri sorumlusuna başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.

(3) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.

### **Veri Sorumluları Sicili**

(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır.

Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

## **SUÇLAR VE KABAHAATLER**

### **Suçlar**

1) Kişisel verilerle ilgili suçlar;

a. Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

- b. Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.
  - c. Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.
- 2) Yukarıdaki maddelerde tanımlanan suçların;
    - a. Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
    - b. Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.
  - 3) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde altı aydan bir yıla kadar hapis cezası verilir.
  - 4) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması **şikayete bağlıdır**.
  - 5) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

#### **Kabahatler**

- 1) Aydınlatma yükümlülüğünü yerine getirmeyen veri sorumluları veya yetkilendirdiği kişiler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,
- 2) Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyen veri sorumluları hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,
- 3) Kurul tarafından şikâyet üzerine veya re'sen verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,
- 4) Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir.

#### **Geçiş hükümleri**

- 1) Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir.
- 2) Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir.
- 3) Bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir.

#### **KİŞİSEL VERİLERİ KORUMA KURULU KARARLARI (Seçilmiş karar özetleri)**

- **(21/12/2017 - 2017/62) Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri almasına ...**

• (31/01/2018 - 2018/10) **Veri Sorumlularınca Alınması Gereken Önlemler**

- 1- Kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
- 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik
- a) Kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,  
b) Gizlilik sözleşmelerinin yapılması,  
c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,  
ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,  
d) İşten ayrılan çalışanların yetkilerinin derhal kaldırılması, kendisine tahsis edilen envanterin iade alınması,
- 3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise
- a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,  
b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,  
c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,  
ç) Güncellemelerinin sürekli takip edilmesi, güvenlik testlerinin düzenli yapılması, test sonuçlarının kayda alınması,  
d) Yazılımların güvenlik testlerinin düzenli olarak yapılması, test sonuçlarının kayda alınması,  
e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- 4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise
- a) Ortamın niteliğine göre güvenlik önlemi (elektrik kaçağı, yangın, su baskını, hırsızlık vb) alınması,  
b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- 5- Özel nitelikli kişisel veriler aktarılacaksa
- a) E-postayla aktarılacak verilerin; şifreli, kurumsal e-postayla veya Kayıtlı Elektronik Posta (KEP) ile aktarılması,  
b) Taşınabilir ortamlarda (flash, CD, DVD vb) aktarılacak verilerin; kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,  
c) Sunucular arasında aktarılacak verilerin; VPN veya SFTP yöntemiyle veri aktarılması,  
ç) Kağıt ortamında aktarılacak verilerin; çalınma, kaybolma ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir.
- **Muhtelif kararlarla Veri Sorumluları Siciline kayıt yükümlülüğünden istisna edilenler**
- Yalnızca otomatik olmayan yollarla kişisel veri işleyenler
  - Noterler
  - Dernekler, vakıflar ve sendikalar (yalnızca amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağlılarına yönelik kişisel veri işleyenler.)
  - Siyasi partiler
  - Avukatlar
  - Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler
  - Gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri
  - Arabulucular
  - Çalışan sayısı 50'den az ve mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumluları (ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar)
- (03/09/2019 - 2019/265) VERBİS Kayıt Süreleri 31.12.2019'a uzatılanlar
- Yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan veri sorumluları
  - Yurtdışında yerleşik veri sorumluları

Bilgilerinize sunarız.

PARETO YEMİNLİ MALİ MÜŞAVİRLİK  
BAĞIMSIZ DENETİM DANIŞMANLIK LTD. ŞTİ.

