

**KİŞİSEL VERİLERİN KORUNMASI HUKUKU  
BİLGİLENDİRME REHBERİ**

# KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ

Kişisel verilerin hukuk düzenince korunmasının kökeni, bireyi devlete karşı koruma fikrinde yatmaktadır. Özellikle Nazi Almanya'sında Devlet tarafından Yahudilere karşı yapılan ayrımcılık, bireye ait kişisel verilerin devlet tarafından dahi bilinmemesi gerektiğine ilişkin fikirleri alevlendirmiştir. Sonrasında gelişen bilgi teknolojilerine ilişkin yöntemler ve şirketlerin büyümesi ile birlikte kişisel verilerin devlete karşı olduğu kadar en az şirketlere ve diğer bireylere karşı da korunması gerektiği fikri oturmaya başlamıştır.

Kişilerin siyasi görüşleri, ideolojileri, dini tutumları, cinsel eğilimleri, etnik kökenleri gibi kıstaslara göre (o kişilerin haberi ve rızası olmadan) sınıflandırılması, fişlenmesi, bu bilgilerin elden ele dolaşması satılması gibi hususlar insan onuruna aykırı olup bireylerin mahremiyetlerine (ve hatta özgürlüklerine) de büyük bir müdahaledir. Aynı zamanda bu verilerin istenmeyen kişilerin eline geçme riski de tehlikeyi daha da artırmaktadır. Bu sebeple bireylere ait her türlü kişisel verinin (belirli istisnalar dışında) açık rıza olmadan kaydetme, paylaşma vb yollarla işlenmesinin yasaklanması genel bir ilke olarak kabul edilmiştir. İşte bu sebeplerle birçok ülkede olduğu gibi Türkiye'de de kişisel verilere ilişkin Avrupa Birliği ülkelerindeki standartlara benzer ölçülerde birçok hukuki koruma getirilmiştir.

## Neden Her Türlü Kişisel Veri Korunuyor?

Bilindiği üzere kişisel verilerin korunması hukukunun amacı yalnızca sağlık, etnik köken gibi hassas verileri değil, kişinin günlük su tüketiminden en sevdiği renge kadar her türlü kişisel veriyi korumak. Bu bakış açısı çeşitli kesimlerce fazla korumacı ve abartılı bulunsa da esasında bu yaklaşımın arkasında bireyi teknolojinin getirdiği güce karşı korumak var. Özellikle bilginin gittikçe daha büyük bir güç olması ve Big Data (Büyük Veri), IoT (Internet of Things: Nesnelerin İnterneti) gibi konseptlerin gelecekte varacağı nokta, bizi bu "abartılı" korumanın amacını anlamaya bir nebze yaklaştıracaktır.

## Big Data

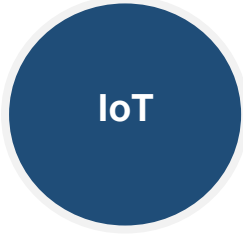
Big Data, İnternette ve veri tabanlarında yapılan tüm paylaşımları, fotoğraf arşivleri, log dosyaları gibi farklı alanlardan elde edilen tüm verilerin analiz edilerek fayda sağlanabilecek hale getirilmesidir. Her gün atılan milyonlarca Tweet, Whatsapp mesajları, Facebook gönderileri, izlenen filmler, beğeniler, tıklamalar, sayfada kalma süresi veya akıllı saat takılı bir kolun hareketleri gibi sayısız veri Big Data'nın konusunu oluşturmaktadır. Big Data'yla uğraşan veri bilimcilerinin görevi ise bu devasa veri yığınına anlamlı bütünlere dönüştürmek, istatistikî bilgi toplamak ve kullanıcıları sınıflandırmaktır.

Herkes tarafından yaygın şekilde kullanılmaya başlanan akıllı telefonlar ve sosyal medya araçlarının sürekli veri toplaması, Big Data alanında da devrim yaratacak ham maddeyi üretmektedir.

Artık bir kişinin İnternet aktivitelerinden, arkadaşlarından, paylaşımlarından ve gösterdiği reaksiyonlardan kaç yaşında olduğu, tahmini gelir düzeyi, dini, ırkı, uyku düzeni, cinsel eğilimi, zeka seviyesi ve yaşam biçimi gibi birçok özellik (insan tarafından incelenmesine gerek olmaksızın) bilgisayar tarafından büyük isabet oranıyla tahmin edilebilmekte ve reklamlar da buna göre yönlendirilmektedir. Zira kişinin cümleyi kuruluş biçiminden profil fotoğrafının çözünürlüğüne, fare hareketlerinden tuşlara basma hızına, kullanılan kelime türlerinden ve beğenme (like/fav) eğilimlerine kadar birçok ayrıntı artık veri analistleri açısından oldukça değerlidir.

İşte bu noktada kişinin ilk aşamada hassaslık içermeyen bir verisi, diğer verilerle bütünleşince bir anlam kazanmakta ve politik davranış, cinsel eğilim, kişilik skorları, din, yaş, zekâ, alkol /sigara kullanma durumu, ruh hali ve sağlık durumu gibi birçok husustaki bilgiye kişinin (aralarında bağı yokmuş gibi gözükən) verileri ile ulaşılabilir.

Kişisel verilerin koruması hukuku, hareketleri öngörülebilir hatta yönlendirilmeye açık hale gelen bireylerin, bu durumunun suiistimal edilerek bireyin, devletlerin/şirketlerin elinde birer "maskota" dönüşmesini engellemek için vardır. Ayrıca bu tespitlerden ötürü bireyin ayrımcılığa uğramasını engellemek de bu çabaların bir amacıdır. Zira önemsiz gibi gözükən kişisel verilerin bile etkili şekilde korunmaması; örneğin intihar eğilimi olduğu big data sayesinde tespit edilen bir bireye kredi verilmemesi gibi sonuçlara yol açabilecektir.



Benzer şekilde; kendi aralarında iletişime geçerek insan müdahalesi olmaksızın çalışan cihazların yaygınlaşması ile ilgili bir konsept olan Internet of Things (Nesnelerin İnterneti) ile de üretilen kişisel veri devasa boyutlara varacaktır. IoT sayesinde örneğin kombi, alarm ve kahve makinesi entegre şekilde çalışacak, uyanmanıza 1 saat kala oda sıcaklığı artırılacak, 5 dakika kala da kahveniz hazır olacaktır. Buzdolabınız domates azalınca siparişi kendisi verecek, teslimat drone ile gerçekleşecektir. İlk bakışta uzak bir gelecek gibi gözükse de uzmanlar, bu tarz teknolojilerin 10 yıl içerisinde yaygınlaşacağını belirtmektedirler.

Kişisel verilerin korunması hukuku açısından ise; bu teknoloji sayesinde üretilen kişisel verinin güvenliği büyük önem arz etmektedir. Zira akıllı ev sistemini “hack”leyen bir hırsız ev sahibinin hangi saatler arasında evde olmadığını kolayca tespit edebilecek veya sağlıksız beslendiğinizi bilen bir buzdolabının bu verileri bir sigorta şirketinin eline geçerse size yüksek fiyatlardan sigorta satmak istenecektir.

Sonuç olarak; Big Data, IoT gibi teknolojilerin bugün bile geldiği nokta mahremiyet ve temel hak ve hürriyetler açısından tehlikeli boyuttayken gelecekte varacağı tahmin edilen nokta korkutucudur. İnsan onurunun bir gereği olarak hem bireylere hem de devletlere karşı korunan kişisel veriler; yeni yöntemler ve teknolojilerin gelişmesi ile çok daha fazla korunmaya muhtaç hale gelmiştir. Bu bağlamda kişisel verilerin korunması hukukunun amacı ise teknolojik ve sektörel gelişmelere engel olmadan hakkaniyet çerçevesinde bireylerin başta mahremiyet olmak üzere haklarını korumaktır.

# KİŞİSEL VERİLERİN KORUNMASI KANUNU UYGULAMASI

## 1. TEMEL KAVRAMLAR

[6698 sayılı Kişisel Verilerin Korunması Kanunu](#) ("**Kanun**") 7 Nisan 2016 tarihinde Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir. Kanun, veri işlerken uyulması gereken genel ilkeler, kişisel veri işleme şartları, veri sorumlusunun aydınlatma yükümlülüğü ve veri sahibinin hakları gibi birçok konuyu düzenlemekte; şirketlerin ve çalışanlarının dikkat etmesi gereken yeni düzenlemeler getirmektedir.

### 1 KİŞİSEL VERİ NEDİR?

Kişisel veri kavramı, Kanun'da şu şekilde tanımlanmıştır:

***"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"***

Her türlü bilgi deyimini ile yalnızca bireyin adı soyadı, doğum tarihi, doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil; aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve buna benzer özelliklerine ilişkin bilgiler de kast edilmektedir.

Bu kapsamda, gerçek kişi hakkındaki görüşler, elektronik cihazların IP adresleri ve MAC adresleri, ses kayıtları, konum bilgisi, adli sicil kaydı, parmak izi, T.C. kimlik numarası, fotoğrafı, kan grubu bilgisi, sağlık raporu vb. veriler de kişisel veri niteliği taşımaktadır.

**Örnek:** Bir yöneticinin deneme süresindeki çalışanın performansına ilişkin tuttuğu notlar kişisel veridir.

**Örnek:** Bir velayet davasında çocuğa, ailesine ilişkin bir çizim yaptırılmıştır. Bu çizim çocuğun ailesine karşı duygularını göstereceği için kişisel veri sayılmaktadır. Hatta söz konusu çizimden hareketle anne ve babanın aile içi davranışları da anlaşılıyorsa, çizim aynı zamanda anne ve babanın da kişisel verisi sayılır.

Kanun'a göre bir bilginin kişisel veri sayılması için öncelikle bir gerçek kişiye ait olması gerekmektedir. Dolayısıyla tüzel kişilere ilişkin bilgiler kişisel veri niteliği taşımazlar.

**Örnek:** Şirket adı, şube adresi gibi veriler tek başlarına kişisel veri sayılmazlar. Diğer bir deyişle, örneğin, bir şirketin adresini veri tabanına kaydetmek kişisel veri işleme olarak nitelendirilmez.

**Bilginin kişisel veri sayılması için, kimliği belirli ya da belirlenebilir bir kişiye ilişkin olması gerekir:**

Belirli olma, bir gerçek kişinin yer aldığı gruptaki diğer kişilerden ayırt edilebiliyor olması anlamına gelmektedir. Çoğu durumda, ad ve soyadı ile diğer birtakım bilgilerin kullanılması bir kişiyi belirlemek için yeterli olmaktadır.

Ancak, ad ve soyadı her zaman bireyleri belirlemek için yeterli olmamakta; belirli bir kişiye ilişkin bilgiden söz edebilmek için birtakım ek verilere ihtiyaç duyulabilmektedir.

**Örnek:** Ahmet Demir ismi tek başına bir kişisel veri sayılmaz. Zira belirlenebilir bir kişiyi işaret etmeye elverişli değildir. Bu bilgi; iş adresi, telefon numarası gibi bilgilerle birlikte değerlendirildiğinde ise belirli bir kişiyi göstereceğinden kişisel veri niteliğinde olacaktır.

Bunun yanı sıra, bir kişinin adının bilinmemesi de onun belirlenemeyeceği anlamına gelmemektedir.

**Örnek:** Çiğdem Apartmanı'nda oturan ve X marka otomobili olan, orta yaşlı, uzun boylu kadın ibaresi (bu tanıma uyan tek bir kişinin olması durumunda) kişisel veridir.

**Örnek:** Cinsiyet, yaş ve maaş verilerinin kombinasyonu orta ölçekli bir şirketteki çalışanlardan birini, adı belirtilmese dahi, belirli kılacaktır.

Bilginin ait olduğu gerçek kişinin belirlenebilirliğinin tespitinde, veri sorumlusunun kimliği belirlemek amacıyla başvurabileceği makul tüm yollar göz önüne alınmalıdır. Ayrıca, bu

yolların gerektirdiđi aba ve bu abanın veri sorumlusunun ilgili faaliyeti gerekleřtirme amacı ile orantılı olup olmayacađı da deđerlendirilmelidir.

## 2 HASSAS VERİLER HANGİLERİDİR?

Hassas (özel nitelikli) kişisel veriler, kişisel verilerin özel bir türüdür. Bu bilgilerin kişiler hakkında ayrımcılıđa yol açabilecek şekilde kullanılabilme ihtimalini gören Kanun koyucu, hassas kişisel verilerin işleme şartlarını özel olarak düzenlemiřtir. Hassas veriler Kanun'un 6. maddesinde sınırlı sayıda olmak üzere düzenlenmiřtir. Buna göre ařađıdaki veriler hassas veri olarak kabul edilmektedir:

Irk ve etkin köken

Siyasi düşünce ve felsefi inan

Din, mezhep ve diđer inanlar

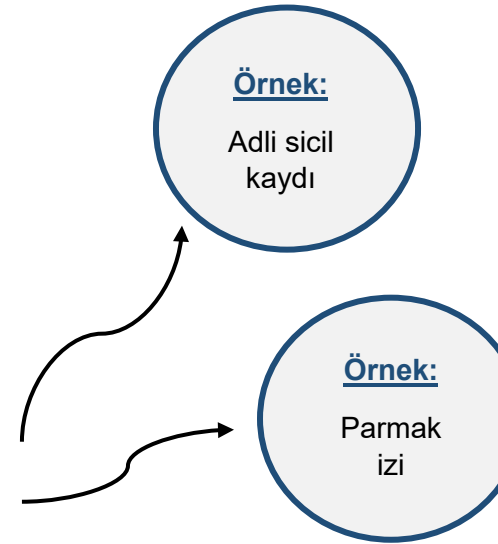
Kılık ve kıyafet

Dernek, vakıf, sendika üyeliđi

Sađlık ve cinsel hayat

Ceza mahkumiyeti ve güvenlik tedbirleri

Biyometrik ve genetik verilerdir.



**NOT:** T.C. Kimlik No, maař, medeni hal, aile içi sırlar, kredi kartı numarası gibi bilgiler çođunlukla sanılanın aksine hassas veri deđildir.

### 3

## KİŞİSEL VERİLERİ İŞLEMEK NE DEMEKTİR?

Kişisel verilerin işlenmesi; 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlemi kapsar.

***Kısacası, veriler üzerinde yapılan her türlü faaliyet veri işlemedir.***

**Örnek:** Kişisel veriyi elde ettikten sonra hiç kullanmayan, sadece veriyi sisteminde saklayan kişi de veri işlemektedir.

### 4

## VERİ SORUMLUSU - VERİ İŞLEYEN

Kanun, kişisel verilerin korunması ve hukuka uygun işlenmesi bakımından asıl yükü veri sorumlusuna yüklemektedir. Bu nedenle veri sorumlusunun kim olduğunun tespiti büyük bir önem arz etmektedir.

### Veri Sorumlusu

Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.

Günlük dil ile ifade edecek olursak veri sorumlusu, veri işleme faaliyetinin genel anlamda “neden” ve “nasıl” yapıldığını belirleyen kişidir.

**NOT:** Şirketteki görevleri kapsamında veri işleyen şirket çalışanları veri sorumlusu değildir. Şirket tüzel kişiliğinin kendisi veri sorumlusu olarak kabul edilir.

### Veri İşleyen

Veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir.



**Örnek:** Şirketin anlaşmalı olduğu, şirket adına verileri saklayan bulut hizmeti sağlayıcıları veri işleyendir.

## ***Veri sorumlusu mu veri işleyen mi olduğumu nasıl tespit edeceğim?***

Bir şirketin veri sorumlusu olduğunu tespit etmek için aşağıdaki konularda karar yetkisinin olup olmadığı dikkate alınabilir:

- Hangi kişisel verilerin toplanacağı,
- Kişisel verilerin hangi amaçlarla işleneceği,
- Hangi kişilerin kişisel verisinin toplanacağına,
- Kişisel verilerin kimlere, hangi amaçla aktarılacağı,
- Kişisel verilerin hangi süre ile saklanacağı

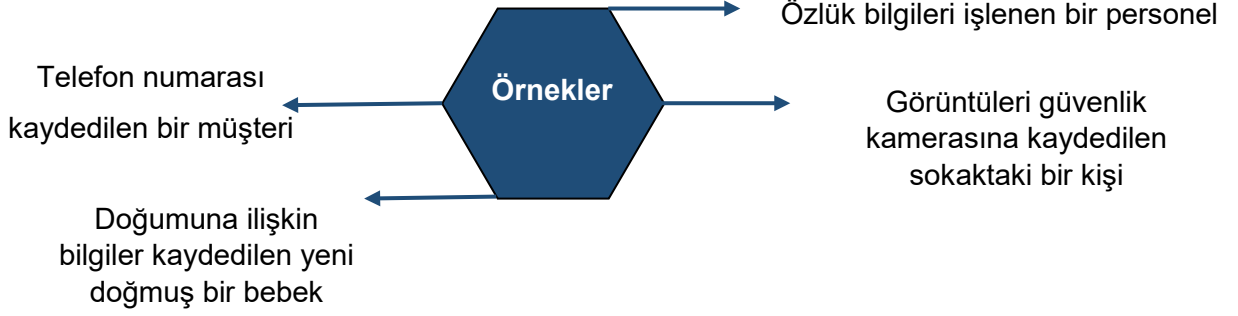
konularındaki kararlar ancak veri sorumlusu tarafından alınabilir.

Veri sorumlusu, akdedeceği bir sözleşme ile aşağıdaki konularda karar alma yetkisini veri işleyene bırakabilir:

- Kişisel verilerin toplanmasında hangi bilişim sistemlerinin kullanılacağı,
- Kişisel verilerin nasıl saklanacağı,
- Veri güvenliğinin sağlanmasının detayları,
- Kişisel verilerin bir şirketten diğerine aktarılmasında kullanılacak yöntem,
- Veri saklama periyoduna uyulmasını sağlamak için kullanılacak yöntem,
- Kişisel verilerin silinmesinde kullanılacak yöntem.

Bu listeler sınırlı olmamakla birlikte, veri sorumlu ile veri işleyenin rollerinin farklılığını ortaya koymaktadır. Bunlara göre, veri işleyen veri sorumlusu adına yürüttüğü faaliyetlerde teknik bilgisini kullanmakta özgürdür.

*Veri sahibi, kişisel verisi işlenen gerçek kişidir.*



Kural olarak, kişilik ölümle sona erdiğinden ölmüş kişiler veri sahibi sıfatını taşımazlar. Ancak belirli hallerde bu kişiler hakkındaki bilgiler de kişisel veri niteliğinde olabilir.

**Örnek:** kişinin ölüm sebebi, biyolojik olarak çocuklarında da olması zorunlu olan bir genetik hastalığı ortaya çıkarıyorsa kişisel veri sayılır. Dikkat edilmesi gerekir ki bu durumda veri sahibi, ölmüş kişinin kendisi değil çocuklarıdır.

Dolayısıyla kişisel verilerin korunması hukuku gerçekten de oldukça geniş bir alanı düzenlemektedir. Ancak kişisel verilerin korunması hukuku yalnızca “gerçek kişilerin verilerini” koruma altına almaktadır. Dolayısıyla ancak gerçek kişiler “veri sahibi” olabilir.

Bu kapsamda; vakıf, sendika, şirket gibi tüzel kişiler veri sahibi sayılmıyorken işçi, tüketici ve gerçek kişi tacirler ise kişisel verileri koruma hukukunun kapsamında birer veri sahibi olarak nitelendirilirler.

## 2. KİŞİSEL VERİLERİN İŞLENME KURALLARI

6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin elde edilmesi, kullanılması, saklanması gibi veri işleme faaliyetlerini tamamen yasaklamamakla birlikte, bu faaliyetlerin gerçekleştirilmesini belirli kurallara bağlamıştır. Bu kurallar aşağıda detaylı olarak açıklanmaktadır:

### 1

### GENEL İLKELER

Kanun'un 4. maddesinde kişisel verilerin işlenmesinde uyulması gereken genel ilkeler belirtilmiştir. Bu ilkeler şunlardır.

- Hukuka ve dürüstlük kurallarına uygun olma
- Doğru ve gerektiğinde güncel olma
- Belirli, açık ve meşru amaçlar için işlenme
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Veri işleme faaliyeti, açık rıza da dâhil olmak üzere, hangi hukuki sebebe dayanırsa dayansın veri sorumlusu genel ilkelere uymakla yükümlüdür. Diğer bir deyişle, veri sahibinin açık rızasının alınmış olması kişisel verilerin Kanun'un genel ilkelere aykırı işlenebileceği anlamına gelmez.

### **Belirli, Açık ve Meşru Amaçlar İçin İşlenme:**

Bu ilke, veri sorumlusunun veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılar. Amacın meşru olması, veri sorumlusunun yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.

**Örnek:** Bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi meşru amaç kapsamında, kan gruplarını işlemesi meşru amaç kapsamında değerlendirilemeyecektir.

**Örnek:** Bir marketin müşterilerinin etnik kökenlerine göre ürünleri farklı fiyatlandırmak için etnik köken bilgisini işlemesi halinde de amaç meşru kabul edilemez.

### **İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma:**

Bu ilke, işlenen verilerin belirlenen amaçların gerçekleştirilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını ifade eder.

**Örnek:** Bir şirketin alacak tahsil birimi, belirli bir borçluya erişmeye çalışmaktadır. Bu amaçla borçlu ile aynı isme sahip birçok kişinin bilgilerini toplar. Araştırma sonrasında söz konusu kişilerin borçlu olmadığı ortaya konulur. Bu aşamadan sonra, alacak tahsil biriminin yapması gereken bu kişilerin bilgilerini sistemden silmektedir. Zira bu verilerin işleme amacıyla ilgili olmadığı ortaya çıkmıştır. Ancak kişilerin tekrar sebepsiz bir şekilde aynı araştırmaya konu olmaları için gereken asgari bilgileri sistemde tutması mümkün olacaktır.

### **İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme:**

Bu ilkeye göre, veri sorumluları, ilgili mevzuata verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Salt gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır.

**Örnek:** 6102 sayılı Türk Ticaret Kanunu uyarınca tacirler, ticari yazışmalarını 10 yıl süre ile saklamak zorundadır.

**Örnek:** bir şirket, gerek olmamasına rağmen ileride lazım olabileceği ihtimaline binaen müşterilerinin fotoğraflarını veya T.C. kimlik numarasını almamalıdır.

2

## VERİ İŞLEME ŞARTLARI

Kişisel verilerin hukuka uygun olarak işlenebilmesi için genel ilkelere uyulmasının yanı sıra Kanun'un 5. maddesinde sayılan veri işleme şartlarından en az birinin mevcut olması gerekmektedir. Bu şartlar şöyle sıralanabilir:

### A. Veri Sahibinin Açık Rızası

Veri sahibinin açık rızası; belirli bir konuya ilişkin olmalı, bilgilendirmeye dayanmalı ve özgürce verilmiş olmalıdır.

- **Açık Rızanın Belirli Bir Konuya İlişkin Olması**

Rızanın belirli bir konuya ilişkin olmasının anlamı, rıza beyanının hangi verilerin işlenebileceğini ve hangi amaçlarla işleme yapılabileceğini açıkça göstermesidir. Veri sorumlusu, rızanın hangi veri işleme faaliyetlerini kapsayacağı konusunda sınırı çizmelidir. Veri işlemenin spesifik amacı belirtilmeden, birçok amacı kapsayabilecek genel ifadeler kullanılarak alınan rızalar hukuka uygun değildir.

**NOT:** Veri sahibinin bütün verilerinin her türlü amaçla işlenebileceğini onaylamış olması geçerli bir rıza oluşturmayacaktır.

- **Açık Rızanın Özgürce Verilmesi**

Rızanın geçerliliği için taşıması gereken diğer şart ise, özgürce verilmiş olmasıdır. Geçerli bir rızadan söz edebilmek için veri sahibinin kişisel verilerinin işlenmesine aldatma, zorlama veya korkutma altında onay vermemiş olması gerekir.

**NOT:** Veri sahibini işlenen veri türleriyle veya işlemenin sonuçlarıyla ilgili yanlış yönlendirerek alınan rıza özgürce verilmiş sayılmayacaktır, dolayısıyla geçerli değildir.

Veri sahibinin rızası, bir sözleşmenin ifasına ya da bir hizmetin sunulmasına bağlanamaz. Bu durumlarda da rızanın özgürce verildiğinden söz edilemeyecektir.

**Örnek:** “Şirketimiz ile sözleşme yapmak için kişisel verilerinizin işlenmesine onay vermek zorundasınız” şeklinde bir yaklaşımla alınan rıza geçersizdir.

Ayrıca, rızanın özgürce verilmiş olduğunun kabulü için veri sahibine rızasını dilediği zaman geri alma imkânı da tanınmış olmalıdır.

**Örnek:** Günümüzde X-Ray cihazları alışveriş merkezleri, havalimanları gibi birçok kamuya açık alanda kullanılmaktadır. Cihazdan geçiş anında veri sahibinin kişisel verileri işlendiğinden, bu anda veri işleme şartlarından birinin mevcut olması gerekir. X-Ray cihazlarından geçişin veri sahibinin tercihine bırakıldığı hallerde, kişi uçağını kaçırmamak ya da şüpheli bir kimse izlenimi vermemek adına cihazdan geçişi kabul edecektir. Dolayısıyla, geçmemenin olumsuz sonuçları yüzünden geçiş tercihi yapacaktır. Bu şekilde alınan rıza yeterince özgür olarak verildiği kabul edilmemektedir. Burada veri işleme faaliyetinin dayanağı açık rıza değil, meşru menfaat olarak uygulanmalıdır.

**Örnek:** Havayolu şirketleri, ABD'ye yapılan uçuşlarda yolcuların PNR bilgilerini ABD yetkili mercileri ile paylaşmaktadırlar. Bu veri aktarımı yolcu ile havayolu şirketi arasındaki sözleşmeye bağlandığında, veri sahibine yolculuk etmek istediği takdirde verilerinin işlenmesine rıza vermek zorunda kalacaktır. Dolayısıyla bu rıza özgürce verilme şartını taşımayacaktır.

- **Açık Rızanın Bilgilendirmeye Dayanması**

Geçerli bir açık rızadan söz edebilmek için, veri sahibine kişisel verilerin işleme amacı, hangi verilerin işleneceği vb. hususlarında bilgi verilmiş olması zorunludur. Bilgilendirme yapılmadan onay alınmış olması halinde, alınan onay geçersiz olacaktır. Veri sahiplerine yeterli bilginin sunulduğunun kabulü için aşağıdaki iki şartın sağlanması gerekir:

1. **Bilginin niteliği:** Bilgi, ortalama bir veri sahibinin anlayabileceği açıklıkta ve sektöre özgü teknik terimler kullanılmadan verilmelidir. Bilgilendirme metni asgari olarak Kanun'un 10. maddesinde yer alan konuları kapsamalıdır.

**2. Bilginin ulařılabilirlik ve görülebilirliđi:** Bilgilendirme, veri sahiplerine dođrudan yapılmalıdır. Bilginin herhangi bir yerde ulařılabilir olması yeterli deđildir. Ayrıca, bilgilendirme metni kolaylıkla okunabilir boyut ve yazı stilinde olmalıdır.

**Örnek:** Bir internet sitesine üye olurken form altına eklenebilecek, yanında onay kutucuđu olan “Kiřisel verilerimin Aydınlatma Metni’nde belirtilen řekilde iřlenmesine izin veriyorum.” ifadesinin kullanıcı tarafından onaylanmasıyla açık rıza alınabilir. (Ancak rızanın geçerliliđi için, Aydınlatma Metni bir köprü ile dođrudan bilgilendirme metnine açılmalıdır.)

### **Açık Rıza Ne Zaman Alınmalıdır?**

Veri sahibinin açık rızası, kiřisel verilerinin iřlenmesinden önce alınmalıdır. Aksi halde, iřlemenin bařladıđı zamandan rızanın alındıđı zamana kadar geçen sürede gerçekteřen iřlemeler hukuka aykırı olacaktır.

### **Açık Rıza Nasıl Alınmalıdır?**

Kanun’da açık rıza alınması için spesifik bir řekli řartı getirilmemiřtir, açık rıza sözlü olarak dahi alınabilecektir; örneđin yazılı bir sözleşmeyle rıza alınabileceđi gibi, veri iřlemesini açıkça onaylayan sözlü bir beyan da yeterli sayılır. Hatta sözlü bir beyan dahi olmaksızın, kiřinin açık onayını gösteren aktif davranıřları rıza için yeterli sayılacaktır. Ancak, kanunen açık rıza alınırken ilgili kiřinin aktif bir hareketi aranmaktadır, diđer bir deyiřle zımni rıza olarak alınan rıza Kanun kapsamında geçerli sayılmayacaktır.

Yine de ileride bir uyuřmazlık dođması halinde, açık rıza alındıđının gösterilebilmesi için ispat edilebilir yöntemlerle rıza alınması gerekmektedir.

Sonuç olarak, veri sahibinin açık rızası bilgilendirmeye dayanmalı, belirli bir konuya iliřkin olmalı ve özgürce verilmelidir. Açık rıza, kiřisel veri iřleme faaliyetinin bařlamasından önce elde edilmelidir. Rızanın geçerliliđi için yazılı olarak alınması zorunlu olmasa da ispat kolaylıđı açısından sözlü olarak alınması tavsiye edilmemektedir.

## B. Kanunlarda Açıkça Öngörülmesi

**Örnek:** Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetine ilişkin verilerini işlemesi

## C. Fiili İmkânsızlık Nedeniyle Rızasını Açıklayamayacak Durumda Bulunan Veya Rızasına Hukuki Geçerlilik Tanınmayan Kişinin Kendisinin Ya Da Bir Başkasının Hayatı Veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması

**Örnek:** Kişinin şuurunun yerinde olmadığı bir durumda, beden bütünlüğünün korunması amacıyla tıbbi müdahale yapılması sırasında kan grubu vb. kişisel verilerinin işlenmesi

**Örnek:** Kaçırılan bir kişinin kurtarılması amacıyla, telefon veya kredi kartı bilgilerinin işlenerek yerinin belirlenmesi

## D. Bir Sözleşmenin Kurulması Veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

**Örnek:** Bir satış sözleşmesinin ifası için, alıcının adres ve iletişim bilgilerinin işlenmesi bu kapsamda değerlendirilir.

**NOT:** Bu veri işleme şartının uygulanabilmesi için işlenen kişisel verilerin sözleşmenin taraflarına ait olması gerektiği unutulmamalıdır. Dolayısıyla, iki tüzel kişi arasındaki sözleşmelerin ifası için tüzel kişilerden birinin çalışanının verilerinin işlenmesi hüküm kapsamında değildir.

## E. Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması

**Örnek:** 6102 sayılı Türk Ticaret Kanunu'nun 82. maddesi uyarınca bir tacir, belirli belgeleri 10 yıl süre ile saklamak zorundadır. Tacirin bu hukuki yükümlülüğünü yerine getirmesi için işlediği kişisel veriler bakımından bu veri işleme şartı uygulanacaktır.



**Örnek:** 4857 sayılı İş Kanunu'nun 75. maddesi uyarınca işveren, çalıştırdığı her işçi için bir özlük dosyası düzenlemekle yükümlüdür. Bu yükümlülüğün yerine getirilmesi kapsamında işlenen kişisel veriler bakımından da bu veri işleme şartı uygulamalara bulacaktır.

## F. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Veri sahibi tarafından alenileştirilmiş kişisel veriler veri sahibinin alenileştirme amacıyla örtüşecek biçimde ve genel ilkelere uygun olarak açık rızası aranmaksızın işlenebilir.

Alenileştirme, herhangi bir şekilde kamuoyuna açıklanmak anlamına gelir. Dolayısıyla bir verinin aleni kabul edilebilmesi için kamuya açıklanmış olması gerekir. Aynı organizasyon çatısı altında kamuya açıklama amacı güdülmeksizin verilerin paylaşılması alenileştirme anlamına gelmeyecektir.

Örneğin, kişinin verileri aynı şirkette, platformda ya da bir tüzel kişilik altında olmasa da aynı ekipte çalıştığı 30 kişinin yer aldığı bir mail grubuna göndermesi halinde alenileştirmeden söz edilemez. Veya yalnızca belirli bir arkadaş/takipçi kitlesine yapılan kişisel veri içeren paylaşımların da aleni olduğu savunulamaz. Bu noktada Kanun'un amacına uygun olarak veri sahibinin niyeti esas alınmalıdır.

**Örnek:** Linked-in'de herkese açık bir profili bulunan kişinin verilerinin, iş teklifi amacıyla işlenmesi bu şekildedir.

## G. Bir Hakkın Tesisi, Kullanılması Veya Korunması İçin Veri İşlemenin Zorunlu Olması

**Örnek:** Bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasi veya kayyımın, kısıtlının mali bilgilerini tutması bu kapsamda değerlendirilir.

## H. İlgili Kişinin Temel Hak Ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması

Bu hükmün uygulanabilmesi için aşağıdaki üç şartın birlikte gerçekleşmesi gerekmektedir:

- Veri sorumlusunun meşru bir menfaatinin bulunmalıdır.
- Bu meşru menfaatin sağlanması için kişisel verilerin işlenmesi zorunlu olmalıdır.
- Veri işleme faaliyeti, veri sahiplerinin temel hak ve özgürlüklerine zarar vermemelidir.

**Örnek:** İşletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaatini teşkil etmektedir.

### **HASSAS VERİLERİN İŞLENME ŞARTLARI:**

Hassas verilerin işleme şartları Kanun'un 6. maddesinde özel olarak düzenlenmiştir. Hükümde ilk olarak, hassas verilerin veri sahibinin açık rızasına dayanılarak işlenebileceği belirtilmiştir. Açık rızanın olmadığı durumlar bakımından ise, sağlık ve cinsel hayata ilişkin veriler ile diğer hassas veriler bakımından bir ayırım yapılmıştır. Buna göre;

- **Sağlık ve cinsel hayata ilişkin olanlar dışındaki hassas veriler;** ancak kanunlarda öngörülen hallerde açık rıza aranmaksızın işlenebilir.
- **Sağlık ve cinsel hayata ilişkin veriler ise;** ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

**NOT:** *Kişisel sağlık verilerinin işlenmesi, 20 Ekim 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'te özel olarak düzenlenmiştir.*

Kişisel verilerin aktarılması, yurt içinde ya da yurt dışında farklı gerçek ya da tüzel kişilikle paylaşılması, internette yayınlanması, başka bir yolla kamuoyuna sunulması ya da ifşa edilmesi gibi birçok fiili kapsar.

Kişisel verilerin yurt içinde üçüncü ve kurumlara aktarılması mümkündür. Bunun için veri sahibinin açık rızasının ya da Kanun m.5/2 ve 6/3'te sıralanan veri işleme şartlarından birinin bulunması gerekir.

Yurtdışına veri aktarımı ise özel şartlara bağlanmıştır. Bunun için;

1. Kanun'da sayılan veri işleme şartlarından biri bulunmalı
2. Kişisel verilerin aktarılacağı ülkede yeterli koruma bulunmalıdır.

Kişisel verilerin aktarılacağı ülkelere hangilerinde yeterli korumanın bulunduğu, Kişisel Verileri Koruma Kurul tarafından ilan edilecek olup; bu konuda henüz bir belirleme yapılmamıştır.

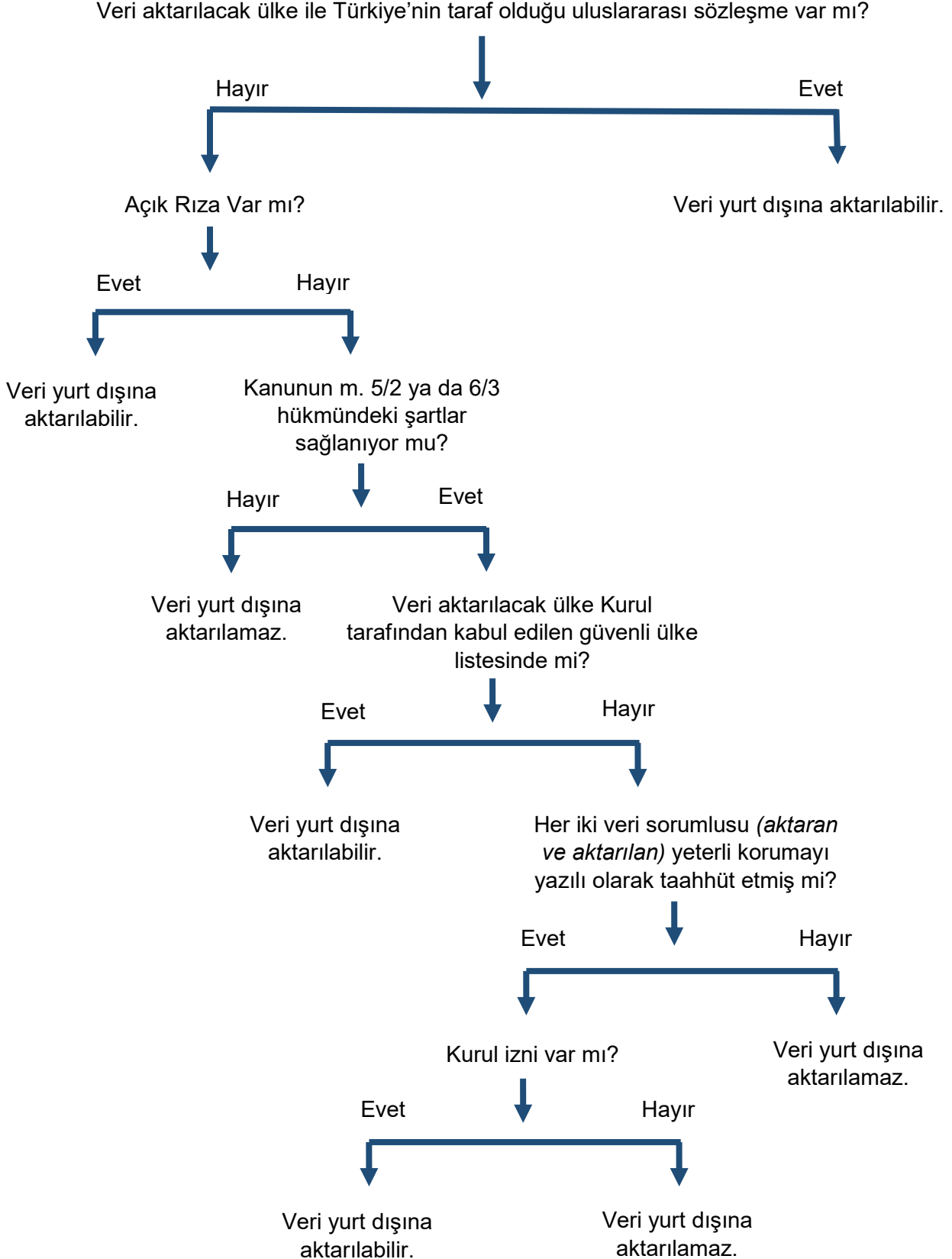
Yeterli korumanın bulunmadığı ülkelere veri aktarımının yapılabilmesi için ise, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun aktarıma izin vermesi gerekmektedir.

Bu haller dışında kişisel verilerin yurtdışına aktarılabilmesi için veri sahibinin açık rızası gerekecektir.

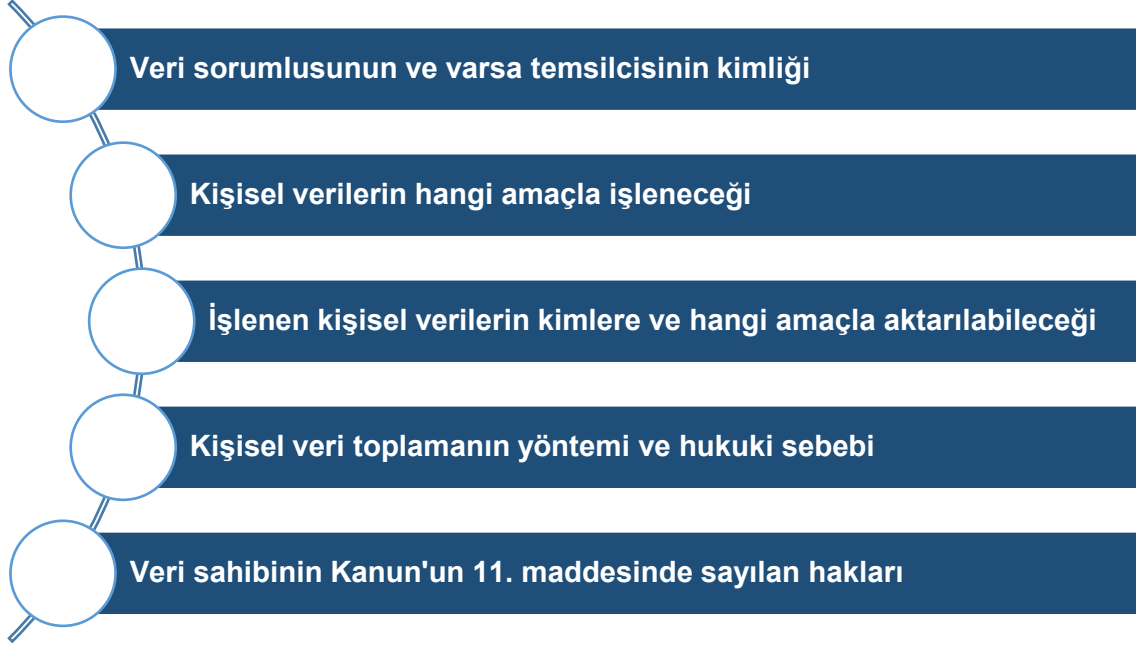
**NOT:** *Kişisel verilerin internette paylaşılması durumunda hem yurt içinde hem yurt dışına aktarımın gerçekleştiği kabul edilmektedir.*

**NOT:** *Bütün veri işleme faaliyetlerin olduğu gibi, kişisel verilerin aktarılmasında da genel ilkelere, aydınlatma yükümlülüğüne ve Kanun'da belirlenen diğer usul ve esaslara uyulması zorunludur.*

## KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI



Kanun'un 10. maddesine göre; veri sorumlusu veya yetkilendirdiği kişi, **kişisel verilerin elde edilmesi sırasında** veri sahiplerini aşağıdaki konularda bilgilendirmekle yükümlüdür:



Aydınlatma metinlerinin dilleri sade ve anlaşılır olmalı; sektöre özgü teknik terimlerin kullanılmasından kaçınılmalıdır. Aydınlatma metinlerinde kullanılan dil, bilginin hitap ettiği veri sahibi kategorisi göz önüne alınarak belirlenmelidir.

Metinlerde eksik ya da veri sahiplerini yanıltıcı bilgilere yer verilmemelidir. Veri sahibinin, kişisel verilerinin işlenmesinin sonuçlarını anlaması sağlanmalıdır.

Aydınlatma yükümlüğünün yazılı olarak yerine getirilmesi zorunlu değildir. Veri sahiplerinin elektronik olarak gönderilebilecek bir e-posta ya da sözlü olarak çağrı merkezi görüşmesi ile de bilgilendirilmeleri mümkündür. Ancak uyumsuzluk halinde ispat yükü veri sorumlusunda olduğundan aydınlatma yükümlülüğünün yerine getirildiğine ilişkin kayıtların saklanması gerekmektedir.

**NOT:** *Kişisel verilerin açık rıza dışındaki veri işleme şartlarına dayalı olarak işlendiği hallerde de aydınlatma yükümlülüğünün yerine getirilmesi zorunludur.*

Kanun'un 11. maddesine göre veri sahipleri, veri sorumlusuna yazılı olarak başvurarak;

- a. Kişisel verilerinin işlenip işlenmediğini öğrenme,
- b. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- c. Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- d. Yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme,
- e. Kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- f. Kanun'un 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
- g. Düzeltilme, silinme veya yok edilme işlemlerinin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- h. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- i. Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme

haklarına sahiptir.

**NOT:** Veri sorumlusu olarak Şirketinizin, veri sahiplerinin taleplerini talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırması gerekmektedir. Ancak, işlemin ayrıca bir maliyeti gerektirmesi halinde, Kişisel Verileri Koruma Kurulunca belirlenecek tarifedeki ücret alınabilir.

Talebin süresi içinde sonuçlandırılmaması, reddedilmesi ya da verilen cevabın yetersiz bulunması halinde veri sahibinin Kişisel Verileri Koruma Kuruluna şikayet hakkı doğmaktadır.

Veri sorumlusu olarak Şirketiniz, Veri Sorumluları Siciline kayıt yaptırmak zorundadır. Veri Sorumluları Sicili, veri sorumlularının veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri aleni bir kayıt sistemidir.

Türkiye’de yerleşik olan her şirket, Sicile kayıt ve diğer işlemler için bir irtibat kişisi atamakla yükümlüdür. Atanan bu kişi, veri sorumlusunun temsilcisi değildir. Kişisel Verileri Koruma Kurumu ve veri sahibi arasındaki iletişimin sağlanması ve yönetilmesinden sorumlu olacaktır.

Veri Sorumluları Siciline Kayıt Başvurusu esnasında aşağıdaki bilgilerin sunulması zorunludur:

- Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişisine ait kimlik ve adres bilgilerine ilişkin Kurul tarafından belirlenecek başvuru formunda yer alan bilgiler,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Kanunun 12nci maddesinde öngörülen ve Kurul tarafından belirlenen kriterlere göre alınan tedbirler,
- Kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresi.

Veri Sorumluları Siciline kayıt yükümlülüğünün yerine getirilmemesinin yaptırımı, 20.000 TL ila 1.000.000 TL arasında idari para cezasıdır.

## ŞİRKET ÇALIŞANLARI OLARAK KİŞİSEL VERİLERİN İŞLENMESİNDE NELERE DİKKAT ETMELİYİZ?

Şirket çalışanları, kişisel veriler ile asıl teması kurmakta ve şirketteki görevleri kapsamında veri işleme faaliyetinde bulunmaktadır. Bu nedenle kişisel verilerin korunması hususunda hukuka uygunluğun teminini sağlamada ana aktörlerden biri şirket çalışanlarıdır.

Şirket, insan kaynakları faaliyetleri ve diğer iç işleyiş prosedürleri kapsamında şirket çalışanlarının da kişisel verilerini işlemektedir. Şirket, çalışanlarının kişisel verilerinin güvenliği konusunda da azami özeni göstermekte, verilerin korunması için her türlü teknik ve idari tedbiri almaktadır. Bu kapsamda çalışanlara verilerinin işlenmesi ile ilgili aydınlatma metinlerini sunmakta ve gerektiğinde onların rızalarına başvurmaktadır. Şirket çalışanları olarak göreviniz gereği işlediğiniz kişisel verilere ilişkin aşağıdaki hususlara dikkat etmeniz gerekmektedir:



Veri işleme faaliyetlerinde yukarıda belirtilen genel ilkelere uymalısınız. Verileri hukuka ve dürüstlük kurallarına uygun; belirli, açık ve meşru amaçlar için işlemelisiniz. Görevinizin gerçekleştirilmesi için gerekli olmayan verileri işlemekten kaçınmalısınız.



Göreviniz kapsamında yapmakta olduğunuz işle ilgili olmayan verileri sistemden çekmemeli; kişisel verileri bireysel amaçlar için kullanmamalısınız.



Şirket işleri dolayısıyla öğrendiğiniz kişisel veriler bakımından kanunen sır saklama yükümlülüğünüz bulunmaktadır. Bu verileri üçüncü kişilerle paylaşmamalı; ifşa etmemelisiniz. Sır saklama yükümlülüğünüz şirket ile ilişkinizin kesilmesinden sonra dahi devam etmektedir.



Gerçekleştiğiniz veri işleme faaliyetinin hukuka uygunluğundan şüphe duyuyorsanız ve/veya veri sahibinin rızasının alınması gerektiğini düşünüyorsanız mutlaka Şirketinizin hukuk birimine danışmalısınız.



Kişisel verileri veri sahibinden ilk elden siz topluyorsanız, mutlaka Şirketinizin aydınlatma formunu ve gerekiyorsa açık rıza formunu veri sahibine sunmalı; verilerinin işlenmesiyle ilgili olarak onu bilgilendirmelisiniz.





Şirket içi veri koruma politikasına, Kişisel Veri Saklama ve İmha Politikasına ve konuya ilişkin diğer politikalara ve periyodik imha sürelerine uymakla yükümlüsünüz.



Şirket tarafından düzenlenen kişisel verilerin korunması ve ilgili konulardaki eğitim, konferans, seminer gibi etkinliklere katılmalısınız.



Yeni veri işleme faaliyetleri konusunda Şirketin ilgisi sorumlusunu mutlaka bilgilendirmeli, söz konusu faaliyeti Kişisel Veri İşleme Envanterine kaydettirmelisiniz.



Yazıcı, faks ve fotokopi makinelerinde, toplantı odalarında doküman unutmamalısınız.



Kişisel verileri güvenli ortamlarda (kilitli dolap, şifreli dosyalar vb.) saklanmalısınız.



Veri sahibi olarak kendini tanıtan ve kişisel verilerine erişmek isteyen kişilerin gerçekten veri sahibi olduğunu teyit etmeden önce herhangi bir bilgi paylaşmamanız gerekir.



Kişisel verilerle ilgili beklenmedik ya da tereddüde düşürecek bir olay olduğunda mutlaka Şirketin ilgili sorumlusuna müracaat etmelisiniz.