HARVEY
ARASAN

Kişisel Verilerin Korunması Rehberi

(KVKK) Pratik Bilgiler ve Örnek Uygulamalar

Giriş

Kişisel veriler, dijitalleşen dünyada bireylerin kimliklerinden davranışlarına kadar pek çok alanı etkileyen temel unsurlardan biri hâline gelmiştir. Bu rehber, **6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK")** kapsamında, kişisel verilerin korunmasına ilişkin temel kavramları, yükümlülükleri ve hak arama yollarını hem kurumlara hem de veri sahibi ilgili kişilere açık ve anlaşılır şekilde sunmak amacıyla hazırlanmıştır.

Rehberin temel amacı veri sorumluları ve veri işleyenlerin veri işlerken uymaları gereken kurallar ve yerine getirmeleri gereken yükümlülükler, kişisel verileri işlenen kişilerin ise KVKK kapsamında sahip oldukları hakları konusunda farkındalıklarını artırmak ve uygulamada karşılaşılan sorunlara pratik bir başvuru kaynağı oluşturmaktır.

Bu çalışma, yalnızca hukukçulara değil; veri işleyen tüm gerçek ve tüzel kişilere, kamu kurumlarına, özel sektöre ve bireylere hitap etmektedir.

Rehberde:

- Kişisel verilerin işlenme şartları,
- Açık rıza ve aydınlatma yükümlülüğü,
- Yurt dışına veri aktarımı,
- Veri güvenliği için alınması gereken teknik ve idari tedbirler,
- VERBİS yükümlülüğü ve istisnalar,
- İlgili kişilerin hakları ve başvuru yolları

gibi pek çok konu sade bir dille, örnek kararlar ve Kişisel Verileri Koruma Kurumu Uygulama Rehberleriyle uyumlu şekilde açıklanmıştır.

Kurumlar için bu rehber, KVKK uyum süreçlerini başlatmak veya güncellemek adına fikir verme işlevi görürken; bireyler için, kendi verileri üzerindeki hakları tanımak ve kullanmak açısından farkındalık kazandıran bir kaynak olacaktır.

Tanımlar

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Arızi aktarım: Düzenli olmayan, tek veya birkaç seferde gerçekleşen, süreklilik arz etmeyen ve olağan faaliyet akışı içinde bulunmayan veri aktarımını,

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

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,

Anonimleştirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

Bağlayıcı şirket kuralları: Yurt dışına veri aktarımı şartlarından biri olan ve bir teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü olduğu bağlayıcı kuralları,

EDPB: Avrupa Veri Koruma Kurulu'nu,

GDPR *(General Data Protection Regulation)***:** Avrupa Birliği'nin Genel Veri Koruma Tüzüğü'nü,

Kurul: Kişisel Verileri Koruma Kurulu'nu,

Kurum: Kişisel Verileri Koruma Kurumu'nu,

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 verilerini,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

İçindekiler

Temel İlkeler ve Kişisel Verilerin İşlenme Şartları

Kişisel Verilerin İşlenme Şartları

Özel Nitelikli Kişisel Verilerin İşlenme Şartları

İlgili Kişinin Açık Rızası

Veri Sorumlusu ve Veri İşleyen

Temel İlkeler ve Kişisel Verilerin İşlenme Şartları

Temel İlkeler

KVKK Madde 4 uyarınca kişisel veri faaliyetleri aşağıda belirtilen temel ilkelere uygun şekilde yapılmalıdır.

- ***Hukuka ve dürüstlük kurallarına uygun olma:***
  Kişisel verileri işleme faaliyeti kanunlara ve yasal düzenlemelere uygun yapılmalı, ilgili kişiye karşı şeffaf olmalı ve işleme amacına uygun olmalıdır.

- ***Doğru ve gerektiğinde güncel olma:***
  Kişisel verilerin toplandığı kaynakların doğruluğu tespit edilmeli ve ilgili kişinin kişisel verilerinin düzeltilmesine ilişkin taleplerin yerine getirilmesi sağlanmalıdır.

- ***Belirli, açık ve meşru amaçlar için işlenme:***
  Veri işleme faaliyetinin dayandığı işlenme şartı ve işleme amacı ilgili kişinin de anlayabileceği şekilde şeffaf ve belirli olmalıdır. Kişisel veriler, belirtilen amaçlar dışında başka amaçlar için işlenmemelidir.

- ***Amaçla bağlantılı, sınırlı ve ölçülü olma:***
  Bu ilke GDPR'da düzenlenen veri minimizasyonu *(data minimisation)* ilkesi ile de uyumludur. Veri işleme amacı için gerekli olmayan hiçbir kişisel veri işleme faaliyetine tabi tutulmamalıdır.

- ***Gerekli olan süre kadar saklanma:***
  Amaçla sınırlı olma ilkesinin bir uzantısı olarak kişisel veriler işlendikleri amaç için gerekli olan süreden daha uzun süre işlenmemelidir.

Kurul'un 3 Ağustos 2023 tarih ve 2023/1327 sayılı kararı:
İlgili kişinin kişisel verilerinin, konakladığı otel çalışanı tarafından üçüncü kişilerle paylaşılması ile ilgili:

> *Kat görevlilerinin temel faaliyet alanı bakım ve temizlik hizmetleridir ve bu hizmetlerin yürütülmesi konaklayan kişinin adının-soyadının bilinmesini gerektirmez. Veri sorumlusu, konaklayanları özel hissettirmek amacından yola çıkarak kişisel verilerin korunması hakkını göz ardı etmemeli, bu anlamda ilgili kişilere seçim hakkı verilmelidir. Veri minimizasyonu ilkesi doğrultusunda, Housekeeping Task Sheet (Temizlik Görev Kağıdı) belgesinde müşterilere ait isim ve soy isme yer verilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyeti, Kanun'un 4'üncü maddesi kapsamında ölçüsüz bir veri işleme faaliyetidir.*

Kurul'un 2 Mayıs 2023 tarih ve 2023/692 sayılı kararı:

> *Özel bir sağlık kuruluşu olan veri sorumlusu, tanıtım faaliyetleri kapsamında, randevu kayıt sayfasında, kişisel veri işleme faaliyetine açık rıza verilmeksizin randevu işleminin tamamlanmaması uygulamasına gitmiştir. Bu durum, açık rızanın unsurlarından "özgür irade ile verilme" unsurunu sakatlamakta olup Kanun'un 4'üncü maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık teşkil etmektedir.*

Kişisel Verilerin İşlenme Şartları

Kişisel veriler ancak KVKK Madde 5'te sayılan aşağıdaki işlenme şartlarından birinin varlığında işlenebilir.

- ***İlgili kişinin işleme faaliyeti için açık rızasının olması***
  Veri sorumlusu ilgili kişinin kişisel verisini işlemeye başlamadan önce uygun bir veri işleme şartının olup olmadığını kontrol etmeli ve işleme faaliyetini ancak diğer işleme şartlarından hiçbirinin mevcut olmaması halinde ilgili kişinin açık rızasına dayandırmalıdır. *Diğer işleme şartlarından birinin mevcut olması halinde ilgili kişinin açık rızasına başvurulmamalıdır.*

  İlgili kişi açık rızasını her zaman geri çekebilmelidir. Başka bir veri işleme şartına dayandırılması gerekirken, açık rızaya dayandırılmış bir veri işleme faaliyetine, ilgili kişi açık rızasını geri çektikten sonra diğer işleme şartına dayanılarak devam edilmesi hukuk ve dürüstlük ilkelerine aykırıdır. Açık rızaya ilişkin detaylı bilgileri "*İlgili Kişinin Açık Rızası*" başlığı altında okuyabilirsiniz.

  İlgili kişinin açık rızasını vermiş olması tek başına kişisel veri işleme faaliyetinin KVKK'ya uygun olduğu anlamına gelmez.

- ***İşleme faaliyetinin kanunlarda açıkça öngörülmesi***
  Veri işleme faaliyetinin kanunlarda açıkça öngörülmesi veri işleme şartlarından birisidir. Örneğin, 4857 sayılı İş Kanunu Madde 75 uyarınca işveren her bir çalışanı için özlük dosyası düzenlemeli ve çalışanın kimlik bilgilerini ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kaydı saklamak ve talep edildiği takdirde yetkili memur ve mercilere göstermek zorundadır.

  Bir işveren çalışanlarının özlük dosyalarını oluşturmak için kişisel verilerini işlediğinde işleme faaliyetinin dayandığı şart kanunlarda açıkça öngörülmesidir.

- ***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***
  Kişisel Verilerin İşlenme Şartları Rehberi'ne göre özgürlüğü kısıtlanan bir kişinin kurtarılması için üzerinde bulunan telefonuna ilişkin veriler kişinin yerinin tespit edilmesi için fiili imkansızlık şartına dayanarak işlenebilir.

  GDPR'ın 46 sayılı gerekçesi fiili imkansızlık şartının salgınların izlenmesinde ve afet müdahalesinde kullanabileceğini öngörür.

- ***Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması,***
  Sözleşme taraflarına ait kişisel verilerin işlenmesinin, bir sözleşmenin kurulması veya ifası için zorunlu olması halinde işlenebilir. Örneğin, bir satın alma sözleşmesinde satıcının malı teslim etmek için sözleşmenin tarafı alıcının adresini işlemesi gerekir. Alıcı da satın alım bedelini ödemek için satıcının banka hesap bilgisini işleyebilir.

- ***Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması***
  Veri sorumlusu, faaliyette bulunduğu sektörün tabi olduğu mevzuat uyarınca işlemesi gereken kişisel veriler olması halinde bu işleme şartına dayanabilecektir. Örneğin bankalar mevzuat gereği müşterileri ve yapılan işlemlere dair çeşitli verileri saklama yükümlülüğünü yerine getirmek için kişisel verileri işleyebilirler.

- ***İlgili kişinin kendisi tarafından alenileştirilmiş olması***
  İlgili kişinin kişisel verisini kendisinin alenileştirmiş olması halinde söz konusu kişisel veri alenileştirme amacı dışında işlenemez. Örneğin, arabasını satmak için yayınladığı ilan içinde iletişim bilgisini alenileştiren bir kişinin iletişim bilgisi sadece ilan ile ilgili iletişime geçmek için kullanılabilir.

- ***Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması***
  Yasal takipler ve davalarla ilgili ispat niteliğindeki kişisel verilerin zaman aşımı süresi boyunca saklanması bu işlem şartına dayanılarak mümkündür. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun **meşru menfaatleri** için veri işlenmesinin zorunlu olması halinde kişisel veriler işlenebilir.

  Kişisel Verilerin İşlenme Şartları Rehberi'ne göre *"veri sorumlusunun elde edeceği fayda; meşru, ilgili kişinin temel hak ve özgürlüğü ile yarışabilecek düzeyde etkin, belirli ve halihazırda mevcut olan bir menfaatine ilişkin olmalıdır"*. Rehber örnek olarak veri sorumlularının çalışan bağlılığını artıran ödül ve prim uygulamaları için çalışanlarının verilerini işlemesini öngörmüştür.

Özel Nitelikli Kişisel Veriler

Özel nitelikli kişiler veriler, işlenmesi halinde ilgili kişi ayrımcılığa maruz kalabileceği veya başka şekillerde zarar görebileceği için diğer kişisel verilere göre daha hassas kabul edilen ve daha koruyucu hükümlere tabi olan verilerdir. Özel nitelikli kişisel verilerin işlenmesi genel kural olarak yasaktır ve sadece KVKK'da düzenlenmiş sınırlı hallerde veya ilgili kişinin açık rızası ile işlenebilirler.

KVKK hangi verilerin özel nitelikli kişi veri sayılacağını ve özel nitelikli kişisel verilerin hangi şartlarda işlenebileceğini düzenler.

Özel nitelikli kişisel veriler aşağıdaki kategorilere giren verilerdir:

- Irk,
- Etnik köken,
- Siyasi düşünce,
- Felsefi inanç,
- Din, mezhep veya diğer inançlar,
- Kılık, kıyafet,
- Dernek, vakıf veya sendika üyeliği,
- Sağlık,
- Cinsel hayat,
- Ceza mahkumiyeti ve güvenlik tedbirleri,
- Biyometrik veriler,
- Genetik veriler.

Özel Nitelikli Kişisel Verilerin İşlenme Şartları

KVKK Madde 6(3) uyarınca özel nitelikli kişisel veriler ancak aşağıdaki işlenme şartlarından birinin varlığı halinde işlenebilir.

- *İlgili kişinin açık rızasının olması,*
- *Kanunlarda açıkça öngörülmesi,*
- *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,*
- *İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,*
- *Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,*
- *Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,*
- *İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,*
- *Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması.*

İlgili Kişinin Açık Rızası

KVKK'da yer alan tanıma göre açık rıza aşağıdaki şartlara uygun olarak verilmiş olmalıdır:

- Belirli bir konuya ilişkin verilmiş olmalı
- Bilgilendirilmeye dayanmalı
- Özgür iradeyle açıklanmış olmalı.

Avrupa Birliği'nin kişisel veri koruma mevzuatı GDPR'a göre açık rıza "*kişinin **bir beyan veya açık eylemi ile özgürce, belirli ve bilgiye dayalı** şekilde verilmiş, belirsizliğe yer vermeyen ve kendisine ilişkin kişisel verilerin işlenmesini kabul ettiği anlamına gelen dileğinin göstergesi*"dir.

Güç Dengesi ve Özgür İrade

Açık rızanın özgürce açıklanabilmesi için veri sorumlusu ve ilgili kişi arasında bir güç dengesi bulunması gerekir. Açık Rıza Rehberi'nde "*Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi (..)*" gerektiğinin altı çizilmiştir.

Rızanın özgürce açıklandığından söz edebilmek için taraflar arasındaki güç dengesi veya dengesizliğini de dikkate almak gerekir. İlgili kişinin, reddetmesi halinde bir zarar göreceğinden çekindiği için verdiği rıza veya müzakereye açık olmayan bir sözleşme içinde verilen rıza KVKK kapsamında geçerli kabul edilmez.

Veri sorumlusu oldukları zaman ilgili kişiye karşı güçlü durumda olabileceğini göz ardı edemeyeceğimiz taraflara örnek olarak işverenleri ve kamu kurumlarını verebiliriz.

Açık Rıza Rehberi'nde de bu durumun altı çizilir ve şöyle denir: *"Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkanının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez"*.

Avrupa Veri Koruma Kurulu ("**EDPB**") da 4 Mayıs 2020 tarihinde kabul edilen 05/2020 sayılı açık rızaya ilişkin rehberinde iş ilişkisinin doğası gereği çalışanın işverenine kişisel verilerinin işlenmesine ilişkin özgür iradesiyle açık rızasını vermesinden bahsetmenin oldukça güç olduğuna değinmiştir. Çalışanın işini kaybetme korkusu duymadan verilerinin işlenmesine itiraz edebileceği bir senaryo hayatın olağan akışına uygun değildir.

Madde 29 Veri Koruma Çalışma Grubu'nun 13 Eylül 2001 tarihli ve 8/2001 sayılı istihdam bağlamında kişisel verilerin işlenmesi üzerine görüşünde ise işveren ve çalışan arasındaki ilişkide işverenin iş ilişkisinin gerekli ve kaçınılamaz bir sonucu olarak kişisel veri işlemesi gerektiği durumlarda, bu veri işlemeyi çalışanın rızası ile meşru kılmaya çalışmasının yanıltıcı olduğu ve rızaya sadece çalışanın gerçek anlamda özgür bir seçim hakkı olduğu ve hiçbir zarar görmeden rızasını daha sonra geri çekebileceği durumlarda başvurulabileceği belirtilmiştir.

Çalışanların özlük dosyalarında tutulan kişisel verileri, maaşları, maaşlarının ödendiği banka hesapları gibi verilerini işlemek için dayanak veri sorumlusunun yasal yükümlülüklerini yerine getirmesi veya iş sözleşmesinin ifası gibi veri işleme şartlarına dayandırmak mümkünken, çalışanın açık rızasına başvurulması kişisel verilerin korunması anlamında yeterli olmaz.

Kurul'un 10 Ağustos 2023 tarih ve 2023/1356 sayılı kararı:
Bir işveren tarafından işe iade davasında, ilgili kişinin mescitte ibadet etme görüntülerinin ibraz edilmesi ile ilgili:

> *"Söz konusu olayda, ilgili kişiye veri sorumlusu çalışanı tarafından gönderilen elektronik posta içeriğinden anlaşılacağı üzere açık rızanın özgür irade ile verilmediği ve ilgili kişinin işten çıkarılma korkusu ile geriye dönük olarak kişisel verilerin işlenmesiyle ilgili diğer belgeleri de rızası olmadan imzalamak zorunda bırakıldığı, (...)"* değerlendirilmiştir.

Kurul'un 8 Temmuz 2019 tarih ve 2019/206 sayılı kararı:

> *"Veri işleme faaliyeti, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde"* dir.

Kurul'un 31 Ağustos 2023 tarih ve 2023/1509 sayılı kararı:

> Kişisel veriler, ilgili kişinin açık rızası veya Kanun'un 5. maddesinin 2. fıkrasındaki diğer işleme şartları bulunmadan işlenmez. Kişisel veri işleme faaliyeti Kanun'da bulunan açık rıza dışındaki şartlardan birine dayanıyorsa ilgili kişiden açık rıza alınması ilgili kişiyi yanıltıcı olacağı için, ilgili kişinin açık rızası aranmaz. Bu durumda ilgili kişinin açık rızasının bulunmamasının veya açık rızasını geri aldığı itiraz ve beyanlarının da hukuken bir geçerliliği yoktur.

Açık Rıza ve Aydınlatma Yükümlülüğü Arasındaki İlişki

İlgili kişinin açık rızasının alınması ve ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi birbirinden bağımsız iki işlemdir. Aynı işlem altında hem aydınlatma yükümlülüğünün ifa edilmesi hem de ilgili kişinin açık rızasının alınması yanlış bir uygulamadır.

Aydınlatma yükümlülüğü ile beraber açık rızanın da talep edilmesi ilgili kişinin gerekli bilgilere erişmesi ile eş zamanlı olarak açık rızasını vermesi sonucunu doğurur. Oysa, aydınlatma metnini okuyan ilgili kişinin açık rıza vermemeyi seçebileceği unutulmamalıdır.

Kurul'un 26 Temmuz 2018 tarih ve 2018/90 sayılı kararı:

"Aydınlatma yükümlülüğünün yerine getirilmesindeki amaç kişisel verilerin işlenmesi noktasında ilgili kişinin bilgi sahibi olmasının temin edilmesidir. Açık rıza alınmasında amaç ise, veri sorumlusu tarafından kişisel verilerinin işlenmesinin hukuki bir gerekçeye dayandırılmasıdır. Bu sebeple, ilgili kişi aydınlatma metni sayesinde kişisel veri işleme faaliyeti ile ilgili olarak bilgi edinmiş olmakla birlikte, söz konusu metinde yazılanlara açık rıza vermek zorunda değildir".

"Aydınlatma metninin okunduğuna ilişkin geri bildirim alınması ile ilgili kişilerin kişisel verilerinin işlenmesi hususunda gerekli seçimlik haklarının da tanındığı açık rıza metninin onaylandığının ispatını sağlayacak mekanizmaların ayrıştırılması" gerekir.

→ Açık rıza alınması ve aydınlatma yükümlülüğünün yerine getirilmesi birbirinden bağımsız iki işlemdir. Aynı işlem altında hem aydınlatma yükümlülüğünün ifa edilmesi hem de ilgili kişinin açık rızasının alınması yanlıştır.

Veri Sorumlusu ve Veri İşleyen

Kişisel veri güvenliğinin sağlanması kapsamında işleme faaliyetinin tarafları arasında sorumlulukların paylaştırılması, hazırlanacak yasal belgelerin içeriği, ilgili kişilerin haklarını nasıl kullanacağı gibi soruların cevaplandırılması için veri sorumlusu ve veri işleyen tanımlarının doğru yapılması büyük önem taşır. KVKK, *"veri sorumlusu"* ve *"veri işleyen"* ifadelerini aşağıdaki gibi tanımlanmıştır:

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Veri Sorumlusu ve Veri İşleyen Rehberi'nde veri sorumlusunun *"kişisel verilerin işlenme amacını ve yöntemini belirleyen kişi"*, bir başka deyişle *"işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek kişi"* olduğu belirtilmiştir.

Rehber, ayrıca veri sorumlusunun tespitinde aşağıdaki konulara kimin karar verdiğinin dikkate alınması gerektiğini söyler:

- Kişisel verilerin toplanması ve toplama yöntemi,
- Toplanacak kişisel veri türleri,
- Toplanan verilerin hangi amaçlarla kullanılacağı,
- Hangi bireylerin kişisel verilerinin toplanacağı,
- Toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı,
- Verilerin ne kadar süreyle saklanacağı.

Bir gerçek veya tüzel kişinin veri işleyen olması için veri sorumlusundan bağımsız, ayrı bir kişi olması ve veri sorumlusu adına veri işliyor olması gereklidir. Aynı kişinin, bazı veri işleme faaliyetleri için veri işleyen ve diğer veri işleme faaliyetleri için de veri sorumlusu olabileceğini unutmamak gerekir.

Veri işleme amaçlarını ve vasıtalarını belirleyen kişi veri sorumlusudur.

Veri sorumlusu kabul edilmek için, veri işleme amacı ve vasıtalarını ne derecede belirlemek gerekir sorusunu sormak önemlidir. Bununla beraber, veri güvenliğine ilişkin alınacak idari ve teknik tedbirlerin belirlenmesinde veri işleyene yetki verilebileceğini de dikkate almamız gerekir.

Rehber bu konuda veri sorumlusunun aşağıda belirtilen hususlarda veri işleyene karar verme yetkisi verebileceğini belirtir:

- Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılan metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri.

Ancak hangi verilerin işleneceği, ne kadar süre tutulacağı, kimlerin bu verilere erişimi olacağı gibi konuların belirlenmesindeki yetki, veri sorumlusunda olmalıdır.

→ Bir sözleşmede bir tarafın veri işleyen veya veri sorumlusu olarak tayin edilmiş olması her zaman gerçek rolünün tespit edilmesinde yeterli ve tek kriter olmayabilir. Somut durumun koşullarının da incelenmesi gerekir.

Veri Sorumlusunun Yükümlülükleri

Veri Sorumlusunun Aydınlatma Yükümlülüğü

VERBİS - Veri Sorumluları Siciline Kayıt Yükümlülüğü

Veri Güvenliği için Teknik ve İdari Tedbirler

Veri Sorumlusunun Yükümlülükleri

Veri Sorumlusunun Aydınlatma Yükümlülüğü

Aydınlatma yükümlülüğü ne zaman doğar?
Kişisel veri işlenen her durumda aydınlatma yükümlülüğü doğar. İlgili kişinin kişisel verisi işlenmeden önce veri sorumlusu aydınlatma yükümlülüğünü yerine getirmelidir.

Daha önce belli bir amaç ve veri işleme şartına dayanılarak işlenmiş olan bir kişisel veri farklı bir amaç ve farklı bir veri işleme şartına dayanılarak işlenmeden önce ilgili kişi yeni veri işleme faaliyeti ile ilgili aydınlatılmalıdır.

Aydınlatma metninde hangi bilgilere yer verilmelidir?
Aydınlatma metninde asgari olarak aşağıdaki bilgilere yer verilmelidir.

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin hangi alıcı gruplarına ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- İlgili kişinin kanunda sayılan hakları.

Yukarıda belirtilenler aydınlatma metninde bulunması gereken asgari unsurlardır. Aydınlatma yükümlülüğünün amacının ilgili kişilerin işleme faaliyeti ile ilgili bilgilendirilmesi olduğu unutulmamalı ve gerektiğinde daha detaylı bilgi verilmelidir.

Örneğin, veri sorumlusunun veya temsilcisinin kimliği açıklanırken, iletişim bilgilerinin de verilmesi gerekir.

Kurul'un 1 Haziran 2023 tarih ve 2023/938 sayılı kararı:

Öğrencilere kurumsal elektronik posta adresinden üniversite hakkında duyurular gönderileceğine ilişkin bilgilendirmeye aydınlatma metninde yer verilmelidir.

→ En çok dikkat edilmesi gereken nokta aydınlatma yükümlülüğü yerine getirilirken ilgili metinde genel nitelikli ve muğlak ifadelerin kullanılmamasıdır. Örneğin, kişisel veri işlenmesi amacı olarak *"size daha iyi hizmet verebilmek için"* veya *"yeni hizmetler geliştirmek için"* gibi geniş açıklamalar kullanılması aydınlatma yükümlülüğünün amacına aykırıdır.

Aydınlatma metninin onaylanması açık rıza yerine geçer mi?
Kişisel veri işlemenin dayandığı veri işleme şartı ilgili kişinin açık rızası ise ilgili kişinin aydınlatma metnini okuduğuna dair onayı ve açık rıza verdiğine dair onayının ayrı ayrı alınması gerekir.

İlgili kişi için yanıltıcı olmaması için aydınlatma metninin okunup, anlaşıldığına dair alınan onay metninde "*aydınlatma metnini onaylıyorum*" veya "*aydınlatma metnini kabul ediyorum*" gibi ifadelerden kaçınılmalı; "*aydınlatma metnini okudum ve anladım*" gibi ifadelere yer verilmelidir.

Kurul'un 28 Eylül 2023 tarih ve 2023/1653 sayılı kararı:

Alışveriş esnasında ticari elektronik ileti gönderilmesi suretiyle kişisel verilerin işlenmesine ilişkin açık rızanın alınması, ilgili kişilerde alışverişin bir parçası olarak bu rızanın verilmesi gerektiği izlenimi oluşturacağından açık rızanın özgür irade ile açıklanma unsurunu zedeleyebilir.

Mağazalarda gerçekleştirilen alışverişlerde; kişilerin telefonuna gönderilecek olan SMS'in amacının ne olduğu ve bu SMS ile iletilen kodun verilmesi halinde ne gibi sonuçlar doğuracağı hususunun, katmanlı aydınlatmanın bir gereği olarak ilk aşamada veri sorumlusunun mağazalarda yetkilendirdiği kişiler tarafından ilgili kişilere açık ve anlaşılır bir biçimde aktarılması gerekmektedir. Bu nedenle, aydınlatma ve açık rıza onay kodu aynı kısa mesaj içerisinde sunulmamalıdır.

Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı kime aittir?
Aydınlatma yükümlülüğünün olması gerektiği gibi yerine getirildiğinin ispat yükü veri sorumlusuna aittir. Bu sebeple aydınlatma metinlerinin yazılı olarak sunulması ve ilgili kişiden metni okuduğuna ve anladığına dair yazılı bir onay alınması tavsiye edilir.

VERBİS - Veri Sorumluları Siciline Kayıt Yükümlülüğü

KVKK ve Veri Sorumluları Sicili Hakkında Yönetmelik uyarınca istisna tutulanlar hariç olmak üzere veri sorumluları kişisel veri işlemeye başlamadan önce VERBİS üzerinden Veri Sorumluları Sicili'ne kaydolmak zorundadır.

Veri sorumluları sicile kayıt yükümlülüğü altına girdikleri tarihten itibaren 30 gün içinde sicile kaydolmalıdır. Herhangi bir fiili, teknik ya da hukuki imkânsızlık nedeniyle kayıt yükümlülüğünü yerine getirmeyen veri sorumlusu, en geç 7 iş günü içinde Kurum'a yazılı olarak başvurarak ek süre talep etmelidir. Kurum bir seferliğine 30 günü aşmamak üzere ek süre verebilir. Sicil kaydında aşağıdaki bilgilere yer verilir:

- Veri sorumlusu, varsa veri sorumlusu temsilcisi ve irtibat kişisine ait kimlik ve adres bilgileri,
- Kişisel verilerin işlenme amaçları,
- Veri konusu kişi grupları ile veri kategorileri,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Kişisel veri güvenliğine ilişkin tedbirler,
- Kişisel verilerin saklanma süresi.

Sicilde kayıtlı bilgilerde değişiklik olması halinde veri sorumlusu değişiklikleri yedi gün içerisinde VERBİS üzerinden Kuruma bildirmelidir.

Sicile kayıtla yükümlü olan veri sorumluları aynı zamanda Kişisel Veri İşleme Envanteri hazırlamakla da yükümlüdür.

Aşağıdaki veri sorumluları sicile kayıt yükümlülüğünden istisna tutulmuştur:

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler,
- Noterler,
- Dernekler, vakıflar ve sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler,
- Siyasi partiler,
- Avukatlar,
- Gümrük müşavirleri,
- Arabulucular,
- Serbest muhasebeci mali müşavirler ve yeminli mali müşavirler,
- Yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 100 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar,
- Köy tüzel kişilikleri.

Veri Güvenliği için Teknik ve İdari Tedbirler

KVKK uyarınca veri sorumlusu, kişisel verilerin veri güvenliği için her türlü teknik ve idari tedbirleri almalıdır.

Madde 12: "*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."

Veri sorumlusu kendi organizasyonu için alınması gereken idari ve teknik tedbirleri belirlemek için veri işleme faaliyetlerinin farkında olmalı ve her bir faaliyet için veri ihlali risklerini değerlendirmelidir.

Kurul'un 3 Ağustos 2023 tarih ve 2023/1327 sayılı kararı:
İlgili kişinin kişisel verilerinin, konakladığı otel çalışanı tarafından üçüncü kişilerle paylaşılması ile ilgili:

> *Housekeeping Task Sheet belgesinde yer alan kişisel verilerin üçüncü kişiler tarafından elde edilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyeti, yalnızca veri sorumlusu tarafından idari ve teknik tedbirlerin alınmamış olması dolayısıyla gerçekleşebilir.*

Veri güvenliğinin sağlanması için alınacak tedbirler sadece bilgi sistemlerinin saldırılardan korunmasına yönelik teknik tedbirler ile sınırlı olmayıp aynı zamanda organizasyonel ve fiziki önlemler de alınmalıdır.

Veri sorumlusunun faaliyet gösterdiği sektörü düzenleyen özel mevzuat veya düzenleyici kurumların çıkardığı yönetmelikler veya kılavuzlarda belirlenen teknik ve idari tedbirler olabilir. Bu durumda veri sorumlusu bu tedbirleri de uygulamalıdır.

İzin verilmedikçe her şey yasaktır.

Kişisel Veri Güvenliği Rehberi, veri güvenliğinin temini için "*Yasaklanmadıkça Her Şey Serbesttir*" ilkesi yerine, "*İzin Verilmedikçe Her Şey Yasaktır*" ilkesinin benimsenmesi gerektiğinin altını çizer.

Kurum kültürünün oluşması ve çalışanların uyması gereken kuralların belirlenmesi için kişisel verilerin işlenmesi korunması ile ilgili şirket politikalarının oluşturulması önemlidir.

Kişisel verilere erişim
Kişisel verilere erişim sadece görevi gereği ilgili kişisel veriyi bilmesi gereken kişilere verilmelidir. Organizasyon içinde kişisel verileri bilmesi gerekmeyen kişilerin bu verilere erişimini engellemek için şirket içi erişim yetki ve kontrol matrisi oluşturulması tavsiye edilir.

Kurul'un 6 Temmuz 2023 tarihli ve 2023/1130 sayılı kararı:
İlgili kişinin rapor ve ilaç kayıtlarının eczane tarafından eski eşi ile paylaşılması ile ilgili:

> *"Eczacı, diğer yükümlülüklerde olduğu gibi sır saklama yükümlülüğünde de yanında çalıştırdığı kimselerden Türk Borçlar Kanunu'nun 116. maddesi gereğince sorumludur. Çalıştırdığı personelin seçimi, bilgilendirilmesi, denetimi ve talimat verilmesinde gerekli objektif özen ve dikkati gösterdiğini ya da bunu göstermiş olsa bile zararın doğumuna engel olamayacağını kanıtlar nitelikte bir bilgi ve belge sunamayan ve ilgili kişinin sağlık verilerinin üçüncü bir kişi ile paylaşılmasına sebep verecek şekilde özen yükümlülüğüne aykırı olarak hareket ettiği değerlendirilen eczacı, (veri sorumlusu) Kanun'nun 12. maddesinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmemiştir."*

Kurul'un 24 Ağustos 2023 tarihi ve 2023/1465 sayılı kararı:
Veri sorumlusuna ait araç kiralama platformuna kullanıcı girişi yapılırken farklı kullanıcılara ait kişisel verilerin görüntülenmesi ile ilgili:

> *Araç kiralama platformundaki veri kayıt sistemindeki algoritmanın yanlış çalışması nedeniyle bir platform kullanıcısı tarafından sisteme giriş yapılmaya çalışıldığı esnada farklı kullanıcıların kişisel verilerine hukuka aykırı olarak erişim sağlanması, veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini yerine getirmediğini gösterir.*

Veri sorumlusunun veri güvenliğini sağlama yükümlülüğü içinde kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde en kısa sürede Kurul'a bildirme yükümlülüğü de vardır.

Kurul'un 1 Haziran 2023 tarihli ve 2023/928 sayılı kararı:
Bir üniversite tarafından ilgili kişilerin kişisel verilerinin yer aldığı belgenin e-posta ekinde üçüncü kişilerle paylaşılması ile ilgili:

> *Şikayete konu veri işleme faaliyetinin veri ihlali niteliği taşıdığı ancak veri sorumlusu tarafından Kurul'a bir veri ihlal bildiriminde bulunulmaması, Kanun'un 12. maddesinde düzenlenen Kurul'a bildirimde bulunma yükümlülüğüne aykırılık teşkil eder.*

Veri işleyenlere yönelik tedbirler

Veri sorumlusu, kendisi adına veri işleyecek olan veri işleyeni seçerken KVKK ile uyumlu olarak yeterli güvenlik tedbirlerini uygulayıp uygulamadığını kontrol etmeli ve veri işleyenin söz konusu tedbirleri uygulayacağı taahhüdünü veri işleme sözleşmesine eklemelidir.

Veri Güvenliği Rehberi, veri işleme sözleşmesinin veri sorumlusu adına kişisel veri işleyen veri işleyenin kişisel verilere ilişkin sır saklama yükümlülüğünün süresiz olarak geçerli olacağının düzenlenmesi gerektiğini belirtir. Veri sorumlusunun ayrıca kişisel veri içeren sistem üzerinde gerekli denetimleri yapma veya kendi adına üçüncü kişilere yaptırma yetkisi olmalıdır.

Kişisel Veri Güvenliği Rehberi, veri güvenliğinin takibi için veri sorumlusunun aşağıdaki önlemleri alması gerektiğini belirtir.

- Bilişim ağlarında hangi yazılım ve servislerin çalıştığını kontrolü,
- Bilişim ağlarında sızma olup olmadığını tespit etmek,
- Kullanıcıların işlem hareketlerinin kaydının düzenli olarak tutulması *(log kayıtları gibi)*,
- Güvenlik sorunlarının hızlı bir şekilde raporlanması,
- Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini bildirmesi için resmi bir raporlama prosedürü oluşturulması.

Kişisel Verilerin Yurt Dışına Aktarımı

Yeterlilik Kararı

Uygun Güvenceler

Yurt Dışına İstisnai Veri Aktarımları

Kişisel Verilerin Yurt Dışına Aktarımı

Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, kişisel verilerin yurt dışına aktarılmasını "*kişisel verilerin 6698 sayılı Kanun kapsamındaki bir veri sorumlusu veya veri işleyen tarafından yurt dışındaki bir veri sorumlusu veya veri işleyene iletilmesi ya da başka bir suretle erişilebilir hâle getirilmesi*" olarak tanımlamaktadır.

Kişisel veriler, KVKK'da düzenlenen diğer işlenme şartlarına ilaveten ancak aşağıdaki şartlardan birinin varlığı halinde yurt dışına aktarılabilir:

Yeterlilik kararı:
Aktarımın yapılacağı ülke veya ilgili sektör veya uluslararası kuruşular hakkında bir yeterlilik kararı olması,

Uygun güvenceler:

i. Yurt dışındaki kamu kurum ve kuruluşları ile Türkiye'deki kamu kurum ve kuruluşları arasında bir anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmiş olması,
ii. Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı,
iii. Kurul tarafından ilan edilen standart sözleşmenin varlığı,
iv. Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi.

Bu şartlardan hiçbirinin sağlanamaması halinde kişisel veriler ancak istisnai olarak ve arızi olmak kaydıyla yurt dışına aktarılabilir.

Yeterlilik Kararı

Kurul tarafından kişisel veri aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında verilmiş bir yeterlilik kararı bulunması halinde, kişisel veriler yurt dışına aktarılabilir.

Kurul, yeterlilik kararı vermeyi değerlendirirken aşağıdaki konuları dikkate alır:

i. İlgili ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu.
ii. İlgili ülkenin kişisel verilerin korunmasına ilişkin mevzuatı ve uluslararası kuruluşun tâbi olduğu kurallar.
iii. İlgili ülkede bağımsız ve etkin bir veri koruma kurumunun varlığı ile idari ve adli başvuru yollarının bulunması.
iv. İlgili ülke veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu.
v. İlgili ülke veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu.
vi. Türkiye'nin taraf olduğu uluslararası sözleşmeler.

→ Bu rehberin yayınlandığı tarihte Kurul tarafından verilmiş bir yeterlilik kararı bulunmamaktadır.

Uygun Güvenceler

1) Uluslararası sözleşme niteliğinde olmayan anlaşma

Kişisel veri aktarımında bulunacak Türkiye'deki kamu kurum ve kuruluşları ile yabancı ülkedeki kamu kuruluşları arasında yapılan bir anlaşma ile uygun güvence sağlanması mümkündür.

Anlaşma imzalanmadan önce müzakere aşamasında Kurul'un görüşüne sunulur. Kişisel veriler, anlaşma metninin nihai halinin Kurul'a sunulması ve Kurul'un aktarıma izin vermesi sonrasında yurt dışına aktarılabilir.

Anlaşmanın uygun güvence sağlaması için içeriğinde aşağıdakilerin düzenlenmiş olması gerekir:

- Veri aktarımının amacı, kapsamı, niteliği ve hukuki sebebi,
- Temel kavramlara ilişkin tanımlar,
- KVKK'da düzenlenen temel ilkelere uyum ile ilgili taahhüt,
- İlgili kişilerin veri aktarımı hakkında aydınlatılmasına ilişkin düzenlemeler,
- İlgili kişilerin KVKK'dan kaynaklanan haklarının kullandırılmasına yönelik taahhüt ve başvuruya ilişkin düzenlemeler,
- Veri güvenliğine yönelik teknik ve idari tedbirlere ilişkin düzenlemeler,
- Özel nitelikli kişisel verilerin aktarımı halinde gerekli önemlerin alınacağına yönelik düzenlemeler,
- Sonraki aktarımlara ilişkin kısıtlamalar,
- İlgili kişinin başvurabileceği hak arama yöntemleri,
- Denetim mekanizması,
- Veri alıcısının, anlaşma hükümlerine uygunluk sağlayamaması hâlinde veri aktaranın aktarımı askıya alma ve anlaşmayı feshetme hakkına yönelik düzenlemeler,
- Veri alıcısının anlaşmanın feshedilmesi veya süresinin sona ermesi hâlinde, aktarıma konu kişisel verileri yedekleri ile birlikte veri aktarana geri göndereceğine ya da tamamen yok edeceğine yönelik taahhüdü.

2) Bağlayıcı Şirket Kuralları

Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketler bağlayıcı şirket kuralları ile uygun güvence sağlayabilirler. Bağlayıcı şirket kurallarına dayanılarak kişisel verilerin yurt dışına aktarılabilmesi için Kurul'un onayının alınması gereklidir. Kurul, başvuru sırasında sunulan bağlayıcı kuralların yabancı dilde de mevcut olması halinde Türkçe metni dikkate alır ve kararını ona göre verir.

Bağlayıcı şirket kuralları aşağıdaki hususları içermelidir.

- Ortak ekonomik faaliyette bulunan teşebbüs grubunun her üyesinin organizasyon yapısı ve irtibat bilgileri.
- Kişisel veri kategorileri, işleme faaliyeti ve amaçları, ilgili kişi grubu veya grupları ve aktarımın yapılacağı ülke ve gerçekleştirilecek aktarımlara ilişkin hususlar.
- Bağlayıcı şirket kurallarının hukuken bağlayıcı olduğuna yönelik taahhüt.
- KVKK'da düzenlenen temel ilkelere uyum,
- Kişisel verilerin işlenme şartları ve özel nitelikli kişisel verilerin işlenme şartları,
- Veri güvenliğinin sağlanmasına yönelik teknik ve idari tedbirler,
- Sonraki aktarımlara yönelik kısıtlamalar,
- Diğer veri koruma önlemleri,
- İlgili kişilerin KVKK'dan kaynaklanan haklarının kullandırılmasına yönelik taahhüt ve kullanıma ve Kurul'a şikayete ilişkin düzenlemeler,
- Teşebbüs grubunun Türkiye'de yerleşik olmayan bir üyesi tarafından bağlayıcı şirket kurallarının ihlalinde Türkiye'de yerleşik bir veri sorumlusu ve/veya veri işleyenin ihlalden sorumluluğu üstleneceğine dair taahhüt.
- İlgili kişilerin veri aktarımı ve bağlayıcı şirket kuralları hakkında aydınlatılmasına ilişkin düzenlemeler,
- Çalışanlara kişisel verilerin korunması konusunda verilecek eğitime ilişkin açıklamalar.
- İlgili kişi başvurularının sonuçlandırılması ve bağlayıcı şirket kurallarına uyumunun takibinden sorumlu kişi veya birimlerin görevleri.
- Denetim mekanizmaları
- Bağlayıcı şirket kurallarına ilişkin değişikliklerin raporlanması ve Kurula bildirilmesine ilişkin mekanizmalar.
- Kurum ile iş birliği yükümlülüğünü
- Teşebbüs grubu üyelerinin aktarımın yapılacağı ülkede bağlayıcı şirket kurallarının sağladığı güvencelere aykırı herhangi bir ulusal düzenleme olmadığına dair taahhüt ve söz konusu güvenceler üzerinde olumsuz

bir etki yaratması muhtemel bir mevzuat değişikliği yapılması hâlinde durumu Kurula bildirmeye yönelik mekanizmalar.

- Kişisel verilere sürekli veya düzenli olarak erişimi bulunan personele yönelik uygun veri koruma eğitimlerinin verileceğine dair taahhüt.

3) Standart Sözleşme

Veri aktaran ve yurt dışında bulunan veri alıcısı arasında Kurul tarafından ilan edilen standart sözleşmenin imzalanması ile uygun güvence sağlanabilir.

Taraflar, Kurul tarafından ilan edilen standart sözleşmeyi üzerinde herhangi bir değişikilk yapmadan imzalamalıdırlar. Yabancı ülkede bulunan şirketlerle imza aşamasını kolaylaştırmak üzere Kurul, ilan ettiği standar sözleşmelerin İngilizce tercümelerini de Kurul'un web sitesinde yayınlamıştır. Standart sözleşmeyi Türkçe ve İngilizce çift dilli imzalamak mümkün olsa da sözleşmenin Türkçe metni esas alınır.

Standart sözleşme, imzaların tamamlanmasından itibaren beş iş günü içinde fiziki olarak veya kayıtlı elektronik posta (KEP) adresi üzerinden veya https://standartsozlesme.kvkk.gov.tr sayfasında bulunan Standart Sözleşme Bildirim Modülü kullanılarak Kurum'a bildirilir. Aktarım tarafları standart sözleşmede, bildirim yükümlülüğünün kimin tarafından yerine getirileceğini belirleyebilir. Eğer bu konuda bir belirleme yapılmamışsa standart sözleşme veri aktaran tarafından Kuruma bildirilir.

Standart sözleşme taraflarında veya veri aktarımı ile ilgili verilen bilgilerde değişiklik olması veya standart sözleşmenin sona ermesi halinde bu durumun Kurum'a bildirilmesi zorunludur.

4) Taahhütname

Veri aktaran ve veri alıcısı arasında bir taahhütname imzalanması yoluyla uygun güvence sağlanabilir.

Taahhütnameye dayanılarak kişisel verilerin yurt dışına aktarılabilmesi için Kurul'un onayının alınması gereklidir. Kurul, başvuru sırasında sunulan taahhütnamenin yabancı dilde de mevcut olması halinde Türkçe metni dikkate alır ve kararını ona göre verir.

Taahhütname uygun güvence sağlamak için kişisel verilerin korunmasına yönelik aşağıdaki düzenlemeleri içermelidir:

- Kişisel veri aktarımının amacı, kapsamı, niteliği ve hukuki sebebi.
- Temel kavramlara ilişkin tanımlar
- KVKK'da düzenlenen temel ilkelere uyum taahhüdü
- İlgili kişilerin veri aktarımı ve taahhütname hakkında aydınlatılmasına ilişkin düzenlemeler
- İlgili kişilerin KVKK'dan kaynaklanan haklarının kullandırılmasına yönelik taahhüt,
- Veri güvenliğine yönelik teknik ve idari tedbirlere yönelik taahhüt,
- Sonraki aktarımlara yönelik kısıtlamalar
- Taahhütnamenin ihlali hâlinde ilgili kişinin başvurabileceği hak arama yöntemleri.
- Veri alıcısının aktarıma konu kişisel verilerin işlenmesi hususunda Kurul'un karar ve görüşlerine uyacağına yönelik taahhüt.
- Veri alıcısının taahhütnameye uygunluk sağlayamamasına neden olacak ulusal düzenlemenin bulunmadığına ve buna yol açabilecek muhtemel bir mevzuat değişikliğini veri aktarana en kısa sürede bildireceğine dair taahhüt ile bu durumda veri aktaranın veri aktarımını askıya alma ve taahhütnameyi feshetme hakkına sahip olacağına yönelik düzenleme.
- Veri alıcısının taahhütnameye uygunluk sağlayamaması hâlinde veri aktaranın veri aktarımını askıya alma ve taahhütnameyi feshetme hakkına sahip olacağına yönelik düzenleme.
- Veri alıcısının taahhütnamenin feshedilmesi veya süresinin sona ermesi hâlinde aktarıma konu kişisel verileri yedekleri ile birlikte veri aktarana geri göndereceğine ya da kişisel verileri tamamen yok edeceğine yönelik taahhüt.
- Taahhütnamenin Türk hukukuna tabi olduğuna ve bir uyuşmazlık hâlinde Türk mahkemelerinin görevli ve yetkili olduğuna yönelik düzenleme ile veri alıcısının Türk mahkemelerinin yargı yetkisini tanımayı kabul ettiğine yönelik taahhüt.

Yurt Dışına İstisnai Veri Aktarımları

Kişisel veriler, arızi olmak kaydıyla ve aşağıda istisnai aktarım hâllerinden birinin varlığı hâlinde yeterlilik kararı veya uygun güvencelerden biri olmadan yurt dışına aktarılabilir.

- Arızi kabul edilmesi için aktarım:
- düzenli olmamalı,
- tek veya birkaç sefer gerçekleşmeli,
- süreklilik arz etmemeli
- olağan faaliyet akışı içinde bulunmamalıdır.

İstisnai aktarım hâlleri:

- İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi şartıyla, aktarıma açık rıza vermesi.
- Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.
- Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.
- Aktarımın üstün bir kamu yararı için zorunlu olması.
- Bir hakkın tesisi, kullanılması veya korunması için aktarılmasının zorunlu olması.
- 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.
- Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden aktarım yapılması.

→ Muhtemel riskler hakkında bilgilendirilme şartının yerine getirilmesi için ilgili kişinin kişisel verilerinin yeterli koruma sağlamayan bir ülkeye aktarılacağı ve bu ülkede verileri korumaya yönelik yeterli güvenlik önlemlerinin olmamasından kaynaklanabilecek riskler hakkında bilgilendirilmesi gerekir.

İlgili Kişilerin Hakları ve Hak Arama Yöntemleri

İlgili Kişilerin Hakları ve Hak Arama Yöntemleri

İlgili kişilerin hakları

KVKK uyarınca ilgili kişiler aşağıdaki haklara sahiptirler:

- Kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
- Kişisel verilerin silinmesini veya yok edilmesini isteme,
- Bu işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Veri sorumlusuna başvuru

İlgili kişiler kişisel verilerini işleyen veri sorumlularına başvurarak KVKK'da düzenlenen ve yukarıda "İlgili Kişilerin Hakları" başlığı altında belirtilen haklarını kullanabilirler. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ uyarınca başvurular Türkçe yapılmalı ve ilgili kişinin adı, soyadı, imzası (başvuru yazılı ise), T.C. kimlik numarası, yabancılar için pasaport numarası, adres, bildirime esas elektronik posta adresi, telefon, faks numarası ve başvurunun konusu. İlgili kişi başvuru konusuna ilişkin bilgi ve belgeleri başvurusuna ekleyebilir.

Veri sorumlusuna başvurular aşağıdaki yollardan biri ile yapılabilir.

- Yazılı,
- Kayıtlı elektronik posta (KEP) adresi,
- Güvenli elektronik imza,
- Mobil imza,
- İlgili kişi tarafından veri sorumlusuna daha önce bildirilen elektronik posta adresini kullanarak,
- Veri sorumlusuna başvuru için geliştirilmiş bir yazılım ya da uygulama vasıtasıyla.

Veri sorumlusu ilgili kişinin başvurusunu kabul edebilir veya gerekçesini açıklayarak reddedebilir. Veri sorumlusu ilgili kişinin talebini en geç 30 *(otuz)* gün içinde sonuçlandırmalıdır.

Kurula şikayet

KVKK, veri sorumlusuna başvurmadan doğrudan Kurul'a şikayet yapılmasına izin vermemektedir. İlgili kişi, veri sorumlusuna yukarıda sayılan usullerden biri ile başvurusunu yaptıktan sonra, veri sorumlusunun başvurusunu reddetmesi veya verilen cevabı yetersiz bulması veya veri sorumlusunun başvurusuna hiç cevap vermemesi halinde Kurul'a şikayette bulunabilir. İlgili kişi şikayetini veri sorumlusunun cevabını öğrendikten sonra 30 gün içinde ve her halde başvuru tarihinden itibaren 60 gün içinde Kurul'a bildirmelidir.

Kurul incelemesi

Kurul, ilgili kişinin şikayeti üzerine veya kişisel veri ihlalinden haberdar olması halinde resen inceleme yapmaya yetkilidir. Veri sorumlusu Kurul'un inceleme kapsamında talep ettiği bilgi ve belgeleri Kurul'a sağlamalı ve gerekmesi halinde yerince inceleme yapılmasına müsaade etmelidir.

Kurul şikayet tarihinden itibaren 60 gün içinde cevap verir. Bu süre içinde Kurul'un cevap vermemesi halinde talep reddedilmiş kabul edilir. Veri ihlaline ilişkin şikayeti üzerine Kurul'dan cevap alamamış başvuru sahibi idare mahkemesinde Kurul'un kararına karşı iptal davası açabilir.

Kurul'un bir veri ihlali olduğuna karar vermesi halinde veri sorumlusu Kurul tarafından tespit edilen aykırılıkları en geç 30 gün içinde gidermelidir. Kurul, kendisine iletilen şikayetler üzerine yaptığı incelemelerde, Kanun'a aykırılık tespit etmesi halinde ilgili veri sorumlusu hakkında çeşitli işlemler tesis edebilir. Bunlar arasında idari para cezaları, veri işleme faaliyetlerinin durdurulması, kişisel verilerin silinmesi veya anonim hale getirilmesi gibi kararlar yer alır.

Kurul'un söz konusu işlemleri, ihlalin oluşmadığı kanaatinde olan ve cezaya, amaç, sebep, neden ve ölçülülük yönünden bir itirazda bulunmak isteyen veri sorumluları tarafından İdari Yargılama Usulü Kanunu uyarınca idare mahkemelerinde iptal davasına konu edilebilir.

İptal davaları Kurul'un bulunduğu yer olan Ankara'daki idare mahkemelerinde 60 gün içinde açılabilir.

İlgili kişinin tazminat hakları

KVKK'nın 14. Maddesinin üçüncü bendi uyarınca "*Kişilik hakları ihlal edilen ilgililerin genel hükümlere göre tazminat hakkı saklıdır*". İlgili Kişilerin Hak Arama Yöntemleri Rehberi'ne göre ilgili kişilerin veri sorumlusuna başvuruda bulunmadan veya başvuru sonrası Kurul'a şikayet yoluna gitmeden doğrudan yargı organlarına başvurmaları mümkündür. Kurul'a şikayette bulunmak için öncesinde veri sorumlusuna başvuruda bulunmak şart olmakla beraber, bu yolların hiçbirine başvurmadan da yargı organlarına başvurulabilir.

Yargıtay 4. Hukuk Dairesi'nin 08/05/2019 tarihli ve 2019/979 E. – 2019/2679 K. Sayılı kararı:

Davacının rızası dışında kimlik bilgilerinin kullanılarak adına telefon hattı açıldığı, borcun ödenmemesi sebebiyle icra takibi başlatıldığı ve bu süreçte menfi tespit davası açmak zorunda kaldığı bir olayda; iletişim şirketinin bayisini seçme ve denetleme yükümlülüğüne aykırı hareket ettiği ve bu nedenle kişilik haklarına saldırının gerçekleştiği tespit edilmiştir. Yargıtay hem maddi hem de manevi tazminat taleplerini kabul etmiş ve iletişim şirketi ile bayiyi birlikte sorumlu tutmuştur. Kararda açıkça, kişisel verilerin ilgili kişinin rızası dışında kullanılması suretiyle kişilik haklarının ihlal edildiği ve ***bu durumun manevi tazminat gerektirdiği ifade edilmiştir.***

AB Adalet Divanı'nın C-687/21 sayılı kararı:

Bir kişinin kişisel verisinin üçüncü kişiler tarafından haksız biçimde kullanılacağı yönündeki endişesinin dahi manevi tazminata konu olabileceği açıkça belirtilmiştir sağladığını. Bu karar, ***kişisel verilerin ihlalinin yalnızca fiili zarara değil, soyut etkilerine karşı da*** *koruma göstermektedir.*

İlgili Mevzuat

6609 sayılı Kişisel Verilerin Korunması Kanunu

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

Veri Sorumluları Sicili Hakkında Yönetmelik

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

Kişisel Verileri Koruma Kurumu Rehberleri

1. Açık Rıza
2. Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi
3. İlgili Kişinin Hak Arama Yöntemleri
4. Kişisel Verilerin İşlenme Şartları
5. Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler
6. Kişisel Verilerin silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi
7. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber
8. Kişisel Verilerin Yurt Dışına Aktarılması Rehberi
9. Kişisel Veri Güvenliği Rehberi *(Teknik ve İdari Tedbirler)*
10. Veri Sorumlusu ve Veri İşleyen Rehberi

İletişim

Deniz Eray Harvey

→ deniz@harveyarasan.com
linkedin.com/in/denizeray/

Tayla Kesgün
→ tayla@harveyarasan.com
linkedin.com/in/tayla-merve-k-60905b151/

Harvey Arasan
İstanbul: Şakayık Sok. No.32 D.10 K.7 Teşvikiye, Şişli, 34365
Paris: 11 Boulevard de Sébastopol 75001 Paris
Tel: +90 212 931 77 48
www.harveyarasan.com
info@harveyarasan.com
www.linkedin.com/company/harveyarasan/

2025

HARVEY
ARASAN

Bu Rehber hakkında detaylı bilgi almak ya da görüşlerinizi paylaşmak isterseniz bize aşağıdaki iletişim kanallarından ulaşabilirsiniz: info@harveyarasan.com