KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

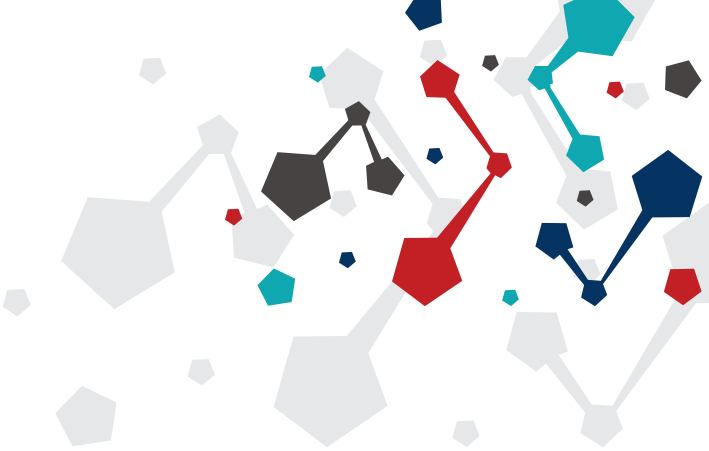
KVKK YAYINLARI NO: 114

# KAMU KURUM VE KURULUŞLARI İLE KAMU KURUMU NİTELİĞİNDEKİ MESLEK KURULUŞLARI İÇİN KİŞİSEL VERİLERİN KORUNMASI KANUNUNA UYUM REHBERİ

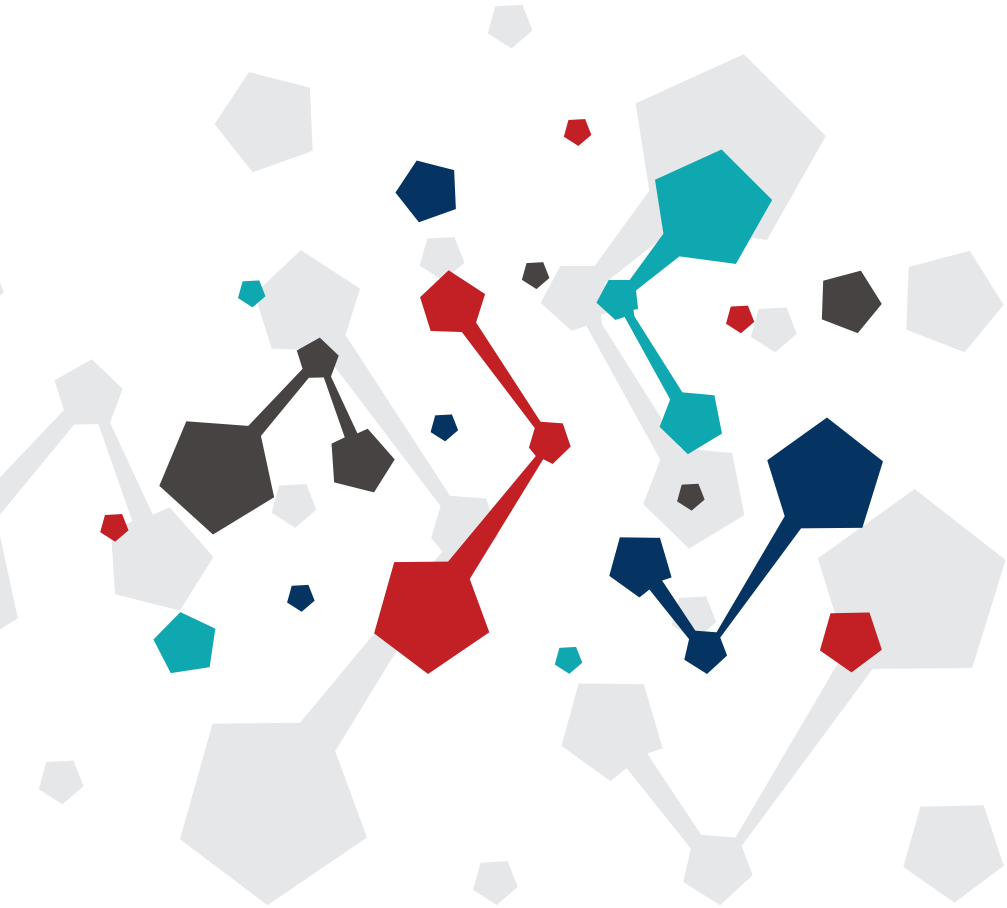
**KAMU KURUM VE KURULUŞLARI İLE KAMU KURUMU NİTELİĞİNDEKİ MESLEK KURULUŞLARI İÇİN KİŞİSEL VERİLERİN KORUNMASI KANUNUNA UYUM REHBERİ**

KVKK Yayınları No: 114
Mart 2026, Ankara

**KİŞİSEL VERİLERİ KORUMA KURUMU**
Adres: Nasuh Akar Mahallesi 1407. Sokak No: 4 Çankaya/ANKARA
Telefon: 0 312 216 50 00
Web: www.kvkk.gov.tr



KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU



# İÇİNDEKİLER


TANIMLAR ..... 9
KISALTMALAR ..... 11
GİRİŞ ..... 13

**1. KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN AMACI VE KAPSAMI ..... 15**
**2. TEMEL KAVRAMLAR ..... 17**
2.1. Kişisel Veri ve Özel Nitelikli Kişisel Veri ..... 17
2.2. Kişisel Verilerin İşlenmesi ve İşleme Şartları ..... 18
2.3. Veri Sorumlusu ve Veri İşleyen ..... 23
2.4. Veri Paylaşımı ve Veri Aktarımı ..... 26

**3. KAMU KURUMLARININ KANUN KAPSAMINDAKİ BAZI YÜKÜMLÜLÜKLERİ ..... 29**
3.1. Genel İlkelere Uyum ..... 29
3.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma ..... 29
3.1.2. Doğru ve Gerektiğinde Güncel Olma ..... 31
3.1.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme ..... 33
3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma ..... 33
3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre kadar Muhafaza Edilme ..... 34
3.2. Kişisel Veri İşleme Şartlarının Doğru Belirlenmesi ..... 35
3.3. Kişisel Verilerin Hukuka Uygun Olarak Aktarılması ..... 39
3.3.1. Kişisel Verilerin Yurt İçinde Aktarılması ..... 41
3.3.2. Kişisel Verilerin Yurt Dışına Aktarılması ..... 43
3.4. Aydınlatma Yükümlülüğü ..... 47

3.5. Veri Güvenliğine İlişkin Yükümlülükler ..... 52
3.6. İlgili Kişi Haklarının Yerine Getirilmesi ..... 63
3.6.1. Hak Arama Yöntemleri ..... 65
3.6.2. Kişisel Verilere İlişkin Düzeltme Talep Etme Hakkı ..... 66
3.6.3. Kişisel Verilerin Silinmesi veya Yok Edilmesini Talep Etme Hakkı ..... 67
3.6.4. Kişisel Verilerin İşlenmesine İtiraz Hakkı ..... 69
3.6.5. Zararın Giderilmesini Talep Etme Hakkı ..... 70
3.7. Saklama ve İmha Yükümlülükleri ..... 70
3.8. VERBİS'e Kayıt Yükümlülüğü ..... 75

**4. İNCELEME SÜREÇLERİNDE KAMU KURUM VE KURULUŞLARI İLE KAMU KURUMU NİTELİĞİNDEKİ MESLEK KURULUŞLARININ YÜKÜMLÜLÜKLERİ ..... 79**
4.1. Veri Sorumlusuna Başvuru Yolunun Tüketilmesi ve İlgili Kişiye Süresinde Cevap Verilmesi ..... 79
4.2. İlgili Kişilerin Haklarına İlişkin Talepleri Konusunda Kurula Şikâyet Hakkını Kullanması ve İnceleme Sürecinde Bilgi ve Belge Talebine İlişkin Olarak Süresinde Kurula Cevap Verilmesi ..... 84
4.3. İnceleme Süreci Neticesinde Verilen Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü ..... 85

**5. KAMU KURUM VE KURULUŞLARI ARASINDA HUKUKA UYGUN VERİ AKTARIMI ..... 91**
5.1. Aktarım Bakımından Özel Nitelikli Hukuki Düzenlemelerin Tespiti ..... 92
5.2. Aktarıma İlişkin Özel Düzenleme Bulunmaması Durumunda Aktarımın Hukuki Dayanağı ..... 98
5.2.1. Yurt İçinde Aktarım ..... 98
5.2.2. Yurt Dışına Aktarım ..... 99
5.3. Aktarımda Ölçülülük ..... 103

5.4. Güvenli Aktarım Yöntemleri ve Teknik/İdari Tedbirler ..... 107
5.5. Sık Karşılaşılan Durumlar ..... 110
5.5.1. Aktarım Süreçlerinde Özel Düzenlemelerin Kanun'un 8'inci ve 9'uncu Maddeleriyle Bütüncül Ele Alınmaması ..... 110
5.5.2. Yurt Dışına Aktarım Bakımından Yeterlilik Kararının Nihai Aktarım Yöntemi Olarak Değerlendirilmesi ..... 111
5.5.3. Aktarım Hukuka Uygun Olmakla Birlikte Kanun'un 4'üncü Maddesindeki İlkelere Uygun Davranılmaması ..... 112
5.5.4. Aktarım Taleplerinin Sistematik/Kategorik Şekilde Reddedilmesi ..... 112

**6. KAMU KURUMLARI BAKIMINDAN TAM VE KISMİ İSTİSNA HALLERİ ..... 117**
6.1. Kanun'un Uygulanmayacağı Haller (Tam İstisna Halleri) ..... 119
6.1.1. Kişisel Verilerin, Üçüncü Kişilere Verilmemek ve Veri Güvenliğine İlişkin Yükümlülüklere Uyulmak Kaydıyla Gerçek Kişiler Tarafından Tamamen Kendisiyle veya Aynı Konutta Yaşayan Aile Fertleriyle İlgili Faaliyetler Kapsamında İşlenmesi ..... 119
6.1.2. Kişisel Verilerin Resmi İstatistik ile Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla İşlenmesi ..... 120
6.1.3. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini, Ekonomik Güvenliği, Özel Hayatın Gizliliğini veya Kişilik Haklarını İhlal Etmemek ya da Suç Teşkil Etmemek Kaydıyla, Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında İşlenmesi ..... 125
6.1.4. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini veya Ekonomik Güvenliği Sağlamaya Yönelik Olarak Kanunla Görev ve Yetki Verilmiş Kamu Kurum ve Kuruluşları Tarafından Yürütülen Önleyici, Koruyucu ve İstihbarî Faaliyetler Kapsamında İşlenmesi ..... 126

6.1.5. Kişisel Verilerin Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerine İlişkin Olarak Yargı Makamları veya İnfaz Mercileri Tarafından İşlenmesi ..... 128
6.2. Kanun'un Kısmen Uygulanmayacağı Haller (Kısmen İstisna Halleri) ..... 129
6.2.1. Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması için Gerekli Olması ..... 130
6.2.2. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi ..... 131
6.2.3. Kişisel Veri İşlemenin Kanun'un Verdiği Yetkiye Dayanılarak Görevli ve Yetkili Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşlarınca, Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İçin Gerekli Olması ..... 132
6.2.4. Kişisel Veri İşlemenin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması için Gerekli Olması ..... 135

SONUÇ ..... 137

KAYNAKLAR ..... 139

# TANIMLAR

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

**Anonim hâle getirme:**
Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.

**Arızi Aktarım:**
Süreklilik arz etmeyen, olağan faaliyet akışı dışında kalan, istisnai hâller kapsamında bir veya birkaç defaya mahsus şekilde gerçekleştirilen aktarım.

**Erişim Yetki Matrisi:**
Kurum içerisinde personel veya birim bazında kişisel veriye erişim yetkisinin sistematik biçimde belirtildiği tablo veya doküman.

**Kişisel Veri:**
Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

**Kişisel Verilerin Yurt Dışına Aktarılması:**
Kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu 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.

**Kurum:**
Kişisel Verileri Koruma Kurumu

**Kurul:**
Kişisel Verileri Koruma Kurulu

**Sorumluluk Yetki Matrisi:**
Kurum içerisinde personel veya birim bazında görev, yetki ve sorumlulukların sistematik biçimde belirtildiği tablo veya doküman.

**Veri Minimizasyonu:**
Yapılacak olan işlem için gerekli olan asgari düzeyde verinin işlenmesi ilkesi.

**Veri İşleyen:**
Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.

**Veri Sorumlusu:**
Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

# KISALTMALAR

**5411 sayılı Kanun:**
5411 sayılı Bankacılık Kanunu

**5429 sayılı Kanun:**
Türkiye İstatistik Kanunu

**6458 sayılı Kanun:**
6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu

**Aktarım Yönetmeliği:**
10.07.2024 tarihli ve 32598 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

**Aydınlatma Tebliği:**
10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ

**bkz.:**
Bakınız

**İmha Yönetmeliği:**
28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

**Kanun:**
6698 sayılı Kişisel Verilerin Korunması Kanunu

**KEP:**
Kayıtlı Elektronik Posta

**Kurul:**
Kişisel Verileri Koruma Kurulu

**Kurum:**
Kişisel Verileri Koruma Kurumu

**Program:**
Resmî İstatistik Programı

**RG:**
Resmî Gazete

**sFTP:**
Secure File Transfer Protocol (Güvenli Dosya Transfer Protokolü)

**TÜİK:**
Türkiye İstatistik Kurumu

**UNHCR:**
Birleşmiş Milletler Mülteciler Yüksek Komiserliği

**vb.:**
Ve benzeri

**VERBİS:**
Veri Sorumluları Sicil Bilgi Sistemi

**Veri Sorumlusuna Başvuru Tebliği:**
10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

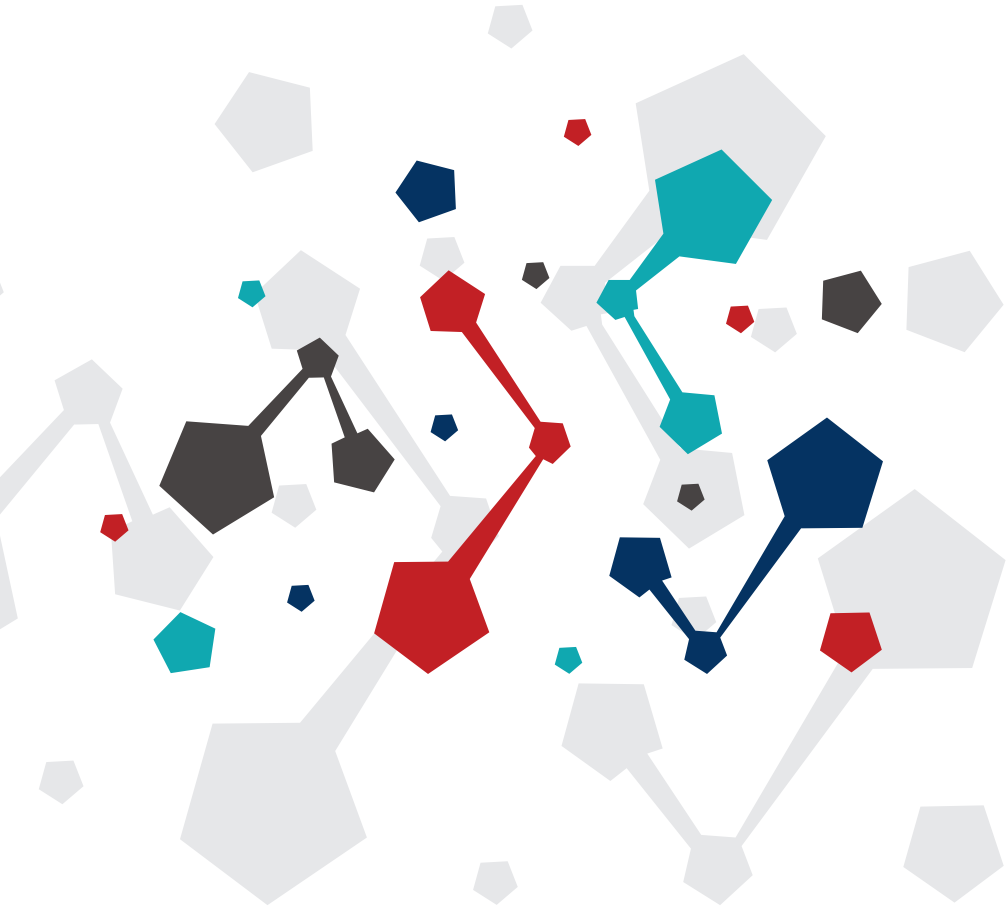
# GİRİŞ

Günümüzde bilişim teknolojilerinde yaşanan gelişmelerin etkisi ve modern iletişim araçlarının yardımıyla bireylere ait çeşitli bilgilere kolayca ulaşılabilmekte, elde edilen bu veriler kolaylıkla aktarılabilmektedir.

Bu bilgiler arasında gittikçe artan bir ölçekte kişisel verilerin de yer alıyor olması, söz konusu verilerin korunması ihtiyacını gündeme getirmiştir. Bu durum, kişisel verilerin bir kanun aracılığı ile korunmasına duyulan ihtiyacı bir hayli artırmıştır.

Türkiye Cumhuriyeti Anayasası'nda 2010 yılında yapılan değişiklikle kişisel verilerin korunmasını isteme hakkı temel hak ve özgürlük olarak anayasal güvence altına alınmıştır. Söz konusu Anayasa maddesinde, kişisel verilerin korunmasıyla ilgili detaylı düzenlemelerin ancak kanunla yapılabileceği belirtilmiştir. Bu kapsamda 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) 07.04.2016 tarihli ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

Bu rehber, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları nezdinde, Kanun'a dair farkındalık düzeyini artırmak, kamu kurum ve kuruluşlarında veri koruma kültürünü güçlendirmek, uygulamadaki tereddütleri gidermek ve Kanun'un hem ruhuna hem de güncel ihtiyaçlarına uygun bir uygulama standardı oluşturmak amacıyla hazırlanmış olup rehberde; Kanun'un amacı ve kapsamına değinilerek Kanun'da yer alan temel kavramlar, kamu kurum ve kuruluşlarının veri sorumlusu olarak Kanun kapsamında yükümlülükleri, kamu kurumları arasında hukuka uygun bir şekilde gerçekleştirilecek veri aktarımının şartları, yurt dışına veri aktarımı ve Kanun'un uygulanmayacağı istisnai haller örneklerle irdelenmiştir.

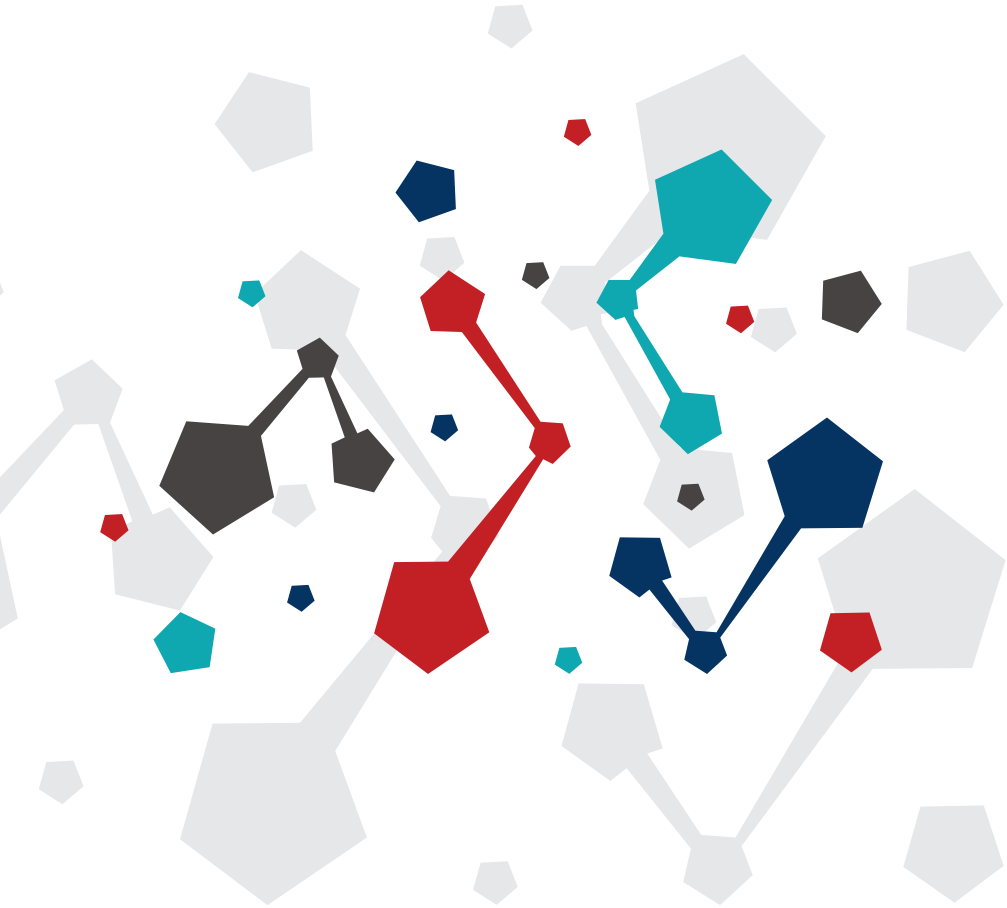


# 1. KİŞİSEL VERİLERİN KORUNMASI KANUNU'NUN AMACI VE KAPSAMI

Kanun'un amacı, kişisel verilerin işlenmesinde özel hayatın gizliliği hakkı başta olmak üzere gerçek kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Kanunla, kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, açıklanması veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmaktadır. Bunun yanında Kanun'un amacı yalnızca veri işleme süreçlerini düzenlemek değil, aynı zamanda bireyin kişisel verileri üzerinde söz sahibi olmasını sağlayan çağdaş bir veri koruma rejimi tesis etmektir.

Kanun'un kapsamı içerisinde, 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 yer almaktadır. Bu kapsam, kamu kurumlarından özel sektöre, meslek kuruluşlarından sivil toplum örgütlerine kadar geniş bir yelpazede veri işleme faaliyetini düzenlemektedir. Böylece Kanun, hem kamu hem de özel sektörün uyacağı ortak bir asgari standart belirleyerek Türkiye'de veri koruma hukukunun bütünlüğünü ve uygulama tutarlılığını sağlamaktadır.



# 2. TEMEL KAVRAMLAR

## 2.1. Kişisel Veri ve Özel Nitelikli Kişisel Veri

Kanun'un 3'üncü maddesinin birinci fıkrasının (d) bendinde kişisel veri, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. Bu tanım doğrultusunda kişisel veriden söz edebilmek için verinin bir gerçek kişiye ilişkin olması ve bu kişiyi de belirli ya da belirlenebilir kılacak nitelikte olması gerekmektedir. Bir kişinin belirli veya belirlenebilir olması ise mevcut verilerden yola çıkarak doğrudan veya mevcut verilerin başka verilerle birleştirerek dolaylı biçimde bir gerçek kişiyle ilişkilendirilmesi suretiyle o kişinin tanımlanabilir olmasını ifade etmektedir.

Kişisel veri kavramı bakımından Kanun'da sınırlı bir sayım yoluna gidilmediğinden, bir kişinin kimliği, fiziksel özellikleri, eğitim, istihdam durumu, aile hayatı, yaptığı haberleşmeler, adresi, kredi kartı bilgisi, alışveriş alışkanlıkları, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları gibi şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya yarayan her türlü bilgi kişisel veri kapsamında yer almaktadır.

Özel nitelikli kişisel veri kategorileri ise Kanun'un 6'ncı maddesinin birinci fıkrasında kanun koyucu tarafından sınırlı biçimde sayılmış olup kıyas yoluyla genişletilebilmeleri mümkün değildir. Bu

kapsamda 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[1] ve genetik verileri özel nitelikli kişisel veridir. Özel nitelikli kişisel veriler, öğrenilmesi durumunda kişileri ayrımcılıkla karşı karşıya bırakabilecek ve mağduriyete yol açabilecek nitelikteki kişisel verilerdir.

### 2.2. Kişisel Verilerin İşlenmesi ve İşleme Şartları

Kanun'un 3'üncü maddesinin birinci fıkrasının (e) bendinde 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 işlem"* olarak tanımlanmıştır. Başka bir deyişle, kişisel verilerin ilk elde edilme anından imha edilmesine kadar olan süreçte gerçekleştirilen her türlü faaliyet Kanun kapsamında kişisel verilerin işlenmesi olarak değerlendirilmektedir. Bu çerçevede kişisel verilerin otomatik yollarla (bilgisayar, telefon, saat vb. işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya

1 Ayrıntılı bilgi için bkz. Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf

donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen) veya bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla (insan müdahalesine bağlı olarak manuel veya fiziksel ortamlar aracılığıyla) işlenmesi Kanun kapsamında yer almaktadır.

***Kişisel veri işleme faaliyetinin hukuka uygun kabul edilebilmesi bakımından Kanun'da birtakım işleme şartları öngörülmüştür.*** Kişisel verilerin işleme şartlarına Kanun'un 5'inci maddesinde yer verilirken, özel nitelikli kişisel verilerin işleme şartlarına Kanun'un 6'ncı maddesinde yer verilmiştir.

Kişisel verilerin işleme şartlarının düzenlendiği Kanun'un 5'inci maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği ancak aşağıda yer alan şartlardan en az birinin mevcut olması durumunda ilgili kişinin açık rızası alınmaksızın kişisel veri işlenebilmesinin mümkün olduğu ifade edilmektedir. Buna göre;

- 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,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
- İlgili kişinin temek hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

şartlarından en az birinin varlığı halinde, kişisel verilerin ilgili kişinin açık rızası alınmaksızın işlenebilmesi mümkündür.

Kanun'un 6'ncı maddesinin üçüncü fıkrasında ise özel nitelikli kişisel verilerin işlenmesinin yasak olduğu ancak aşağıdaki durumlarda özel nitelikli kişisel verilerin işlenmesinin mümkün olduğu düzenlenmiştir. Buna göre;

- 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

şartlarından en az birinin varlığı halinde, özel nitelikli kişisel verilerin işlenmesi mümkündür.

Kişisel verilerin işlenme şartları, Kanun'da sınırlı sayma yoluyla belirlenmiş olup bu şartların genişletilebilmesi mümkün değildir.

***Kişisel veri işleme faaliyetinin Kanun'da bulunan açık rıza dışındaki şartlardan birine dayanması halinde ilgili kişiden ayrıca açık rıza alınmaması gerekmektedir.*** Zira kişisel veri işleme faaliyetinin, açık rıza dışında bir işleme şartına istinaden yürütülmesi mümkün iken ilgili kişilerden ayrıca açık rıza alınması, hakkın kötüye kullanımı

niteliğinde olacaktır. Nitekim böyle bir durumda, ilgili kişi tarafından verilen açık rızanın geri alınması halinde kişisel veri işleme faaliyetinin sona ereceği kanaatiyle hareket edileceğinden ve veri sorumlusunun diğer kişisel veri işleme şartlarından birine istinaden kişisel veri işleme faaliyetini sürdürmesi söz konusu olabileceğinden ilgili kişi yanıltılmış olacak ve böylelikle hukuka ve dürüstlük kurallarına aykırı bir durum ortaya çıkacaktır.

Bu kapsamda veri sorumlusu tarafından kişisel veri işleme faaliyetinin öncelikli olarak açık rıza dışındaki işleme şartlarından birine dayanıp dayanmadığı değerlendirilmeli, eğer işlemeye temel teşkil eden amaç Kanun'da belirtilen açık rıza dışındaki şartlardan en az birini karşılamıyorsa kişisel veri işleme faaliyetinin gerçekleştirilebilmesi için kişinin açık rızasının alınması yoluna gidilmelidir.

Öte yandan belirli bir amaç kapsamında gerçekleştirilen kişisel veri işleme faaliyeti bakımından birden fazla kişisel veri işleme şartı bulunabilmesi mümkündür. Örneğin, maaş bordrosu düzenlemek amacıyla çalışanların kişisel verilerinin işlenmesi durumunda sözleşmenin ifası ve veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesi gibi veri işleme şartları uygulama alanı bulabilecektir.

### 2.3. Veri Sorumlusu ve Veri İşleyen

Kanun'un 3'üncü maddesinin birinci fıkrasının (ı) bendinde veri sorumlusu; kişisel verilerin işleme amaç ve vasıtalarını belirleyen veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmaktadır. Bu tanım doğrultusunda veri sorumlusu, veri işleme faaliyetinin temel araçlarını ve veri işleme faaliyetinin hangi sebeple ve nasıl gerçekleştirileceği hususlarını belirleme, veri işleme sürecinin her anında serbestçe karar verme yetkilerine sahiptir. Tanımdan anlaşılacağı üzere kamu kurumu, şirket, dernek veya vakıf gibi tüzel kişilerin veri sorumlusu olabilmeleri mümkündür.

Veri sorumlusu, Kanun'un kişisel veri işleme faaliyetine ilişkin hukuki yükümlülükleri tayin etmek amacıyla belirlediği bir statü olup tanımda yer alan kriterleri karşılaması durumunda tüzel kişiliği haiz kamu kurum ve kuruluşları da bu statüde yer alacaktır. Önemle belirtilmesi gerekir ki veri sorumlusu ifadesiyle özel sektör veya kamuda faaliyet gösteren ve tüzel kişiliğe sahip olan işletme, kuruluş ve birimler bünyesinde çalışan ve kişisel veri işleme faaliyetlerinden sorumlu olan bir gerçek kişi kastedilmemektedir. Başka bir deyişle bir Bakanlığın, veri sorumlusu sıfatını taşıyan kamu kurum ve kuruluşunun veya kamu kurumu niteliğindeki meslek kuruluşunun bir veri sorumlusu belirlemesi durumu söz konusu değildir. **Tüm bu kurum ve kuruluşlarda veri sorumlusu, kurum veya kuruluşun bizzat kendisidir.**[2] Buna göre kamu

2 Bkz. 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar -1, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e-2a507e63200.pdf

kurumlarında; kamu kurumu bünyesinde bulunan daire başkanı, şube müdürü, insan kaynakları müdürlüğü, hukuk müşavirliği, strateji dairesi, bilgi işlem birimi veya kurum dışından hizmet alınan kurum/kişiler değil kamu kurumlarının bizzat kendisi veri sorumlusu sıfatını haizdir.

Öte yandan bir Bakanlığa bağlı, ilgili ve ilişkili kuruluşlar ile taşra teşkilatları kişisel veri işleme amaç ve vasıtalarını kendisi belirlemiyorsa ve kişisel verilerin işlendiği veri kayıt sisteminin kurulması ve yönetilmesinden de sorumlu değilse veri sorumlusu sayılmayacaktır. Bu birimlerin işlemekte oldukları tüm kişisel verilerle ilgili yükümlülükler, bağlı oldukları Bakanlık tarafından yerine getirilecektir. Örneğin Aile ve Sosyal Hizmetler Bakanlığının bir il müdürlüğü bünyesinde gerçekleşen kişisel veri işleme faaliyeti bakımından veri sorumlusu taşra teşkilatında yer alan il müdürlüğü değil bizzat Aile ve Sosyal Hizmetler Bakanlığıdır. Öte yandan, Dışişleri Bakanlığının yurt dışı teşkilatında yer alan bir konsolosluk bünyesinde gerçekleşen kişisel veri işleme faaliyeti bakımından da veri sorumlusu Dışişleri Bakanlığı olacaktır.

Örneğin, bir kamu kurumuna ataması gerçekleşen bir memurun kişisel verilerini içeren belgelerin insan kaynakları müdürlüğü tarafından teslim alındığı ve kaydedildiği bir durumda, veri sorumlusu söz konusu belgeleri teslim alan ve kaydeden insan kaynakları müdürlüğü veya ilgili personel değil bizzat kamu kurumunun kendisi olacaktır.

Bu doğrultuda kamu kurum ve kuruluşları nezdinde, Kanun'un uygulanmasıyla ilgili iş ve işlemleri yerine getirme konusunda kişi/birim/ekip görevlendirilse dahi bu görevlendirme neticesinde o kişi/birim/ekip veri sorumlusu olmayacaktır.

Öte yandan veri işleyen Kanun'un 3'üncü maddesi birinci fıkrasının (ğ) bendinde tanımlanmıştır. Kanun'a göre veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir. Veri işleyen kişisel veri işleme faaliyetini veri sorumlusu tarafından belirlenen temel amaç ve vasıtalar veya veri sorumlusunun verdiği talimatlar doğrultusunda gerçekleştirmektedir. Veri işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği, **veri sorumlusunun organizasyonu dışındaki ayrı bir gerçek veya tüzel kişidir**. Anılan sebeple veri işleyen olma bakımından en önemli kriterler; veri sorumlusu adına hareket edilmesi ve veri işleme faaliyeti bakımından veri işleyenin doğrudan bir menfaatinin söz konusu olmamasıdır. Ancak veri işleyenin sağladığı hizmet noktasında dolaylı bir ekonomik ediniminin olması (ücret, komisyon, vb.) bir kıstas olarak kabul edilmemektedir.

Örneğin, bir kamu kurumunun uhdesinde toplanan kişisel verilerin depolanması amacıyla özel bir şirketten hizmet alımı gerçekleştirdiği durumda, kamu kurumunun verdiği talimatlar doğrultusunda o kamu kurumu adına faaliyet gösteren şirket veri işleyen olarak nitelendirilecektir.

### 2.4. Veri Paylaşımı ve Veri Aktarımı

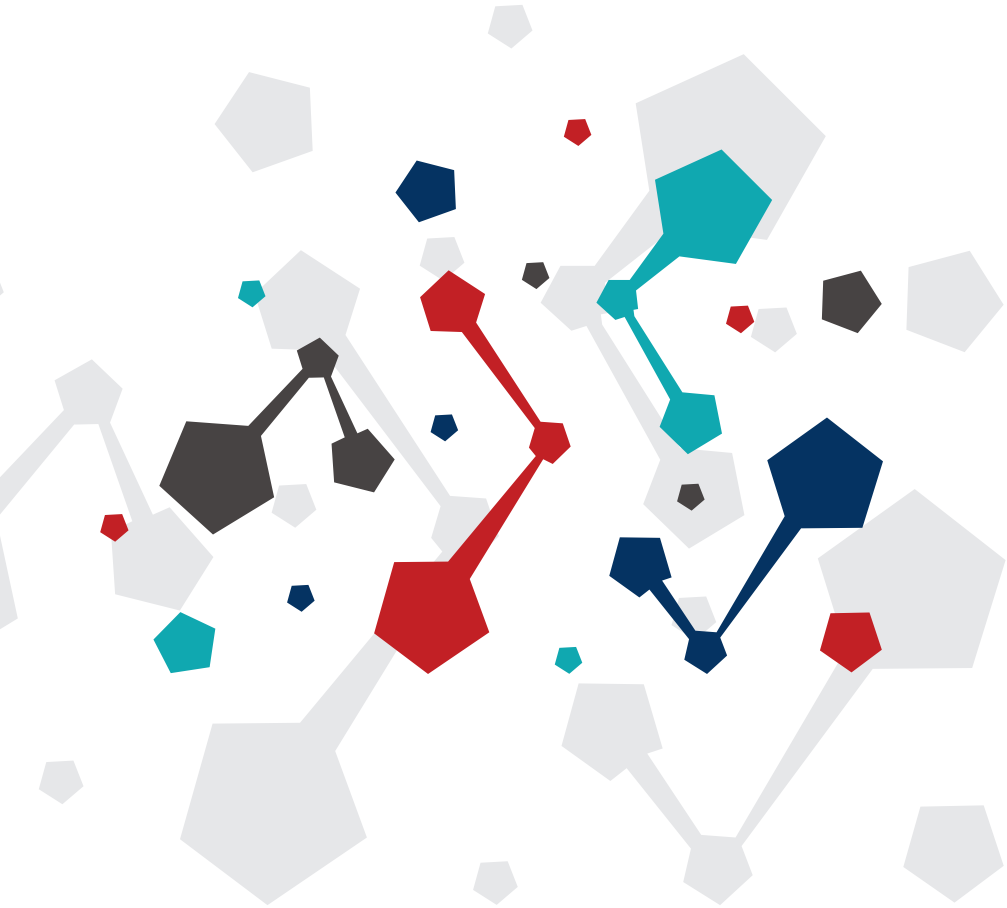
Kişisel verilerin aktarılması; veri sorumlularının uhdesinde bulunan kişisel verilerin üçüncü kişilere aktarılmasını ifade etmektedir. Kişisel verilerin aktarılması, Kanun'da iki başlık altında ele alınmıştır. Kanun'un 8'inci maddesinde kişisel verilerin yurt içinde aktarılmasına ilişkin hükümlere, 9'uncu maddesinde ise kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlere yer verilmiştir. Belirtilen maddeler kapsamında hem kişisel veriler hem özel nitelikli kişisel veriler aktarılabilmektedir.

Kanun'un 8'inci maddesi birinci fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağı, ikinci fıkrasının (a) bendinde kişisel verilerin 5'inci maddenin ikinci fıkrasında, (b) bendinde ise yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması hâlinde ilgili kişinin açık rızası alınmaksızın aktarılabileceği düzenlenmiştir.[3] Örneğin, Bakanlığın bağlı kurumları (TİKA, KGM vb.), ilgili kurumları (İŞKUR ve SGK vb.) farklı tüzel kişilikler arasında veri paylaşımı, aktarım niteliğindedir ve Kanun'un 8'inci maddesi uygulanmalıdır.

3 Ayrıntılı bilgi için bkz. 3.3. Kişisel Verilerin Hukuka Uygun Aktarılması ve 5. Kamu Kurum ve Kuruluşları Arasında Hukuka Uygun Veri Aktarımı.

Öte yandan ***veri sorumlusu sıfatını haiz bir tüzel kişiliğin bünyesi içerisinde, diğer bir ifadeyle aynı organizasyon içerisinde, kişisel verilerin paylaşımı Kanun'un 8'inci maddesi çerçevesinde bir aktarım olarak değerlendirilmemektedir. Tüzel kişiliğin bünyesinde faaliyet gösteren çalışanlar veya farklı birimler arasında kişisel verilerin paylaşılması da bu anlamda aktarım sayılmamaktadır.***

Örneğin, Sağlık Bakanlığı'na bağlı bir devlet hastanesinin ildeki il sağlık müdürlüğüne hasta kayıtlarını iletmesi durumunda verilerin paylaşılması tek bir tüzel kişilik çatısı altında gerçekleştiğinden aktarım sayılmayacaktır. Benzer şekilde Millî Eğitim Bakanlığı bünyesindeki bir okulda tutulan öğrenci devamsızlık bilgilerinin Bakanlığın merkez teşkilatındaki ilgili genel müdürlüğe gönderilmesi de kurum içi veri paylaşımı kapsamında değerlendirilecektir. Ancak bu tür kurum içi paylaşımlarda da yetki ve görev sınırları içerisinde hareket edilmesi, kişisel veri işleme şartlarına ve genel ilkelere uygunluğun sağlanması hususunda veri sorumlusunun yükümlülüklerinin devam ettiğinin göz önünde bulundurulması zorunludur.



# 3. KAMU KURUMLARININ KANUN KAPSAMINDAKİ BAZI YÜKÜMLÜLÜKLERİ

### 3.1. Genel İlkelere Uyum[4]

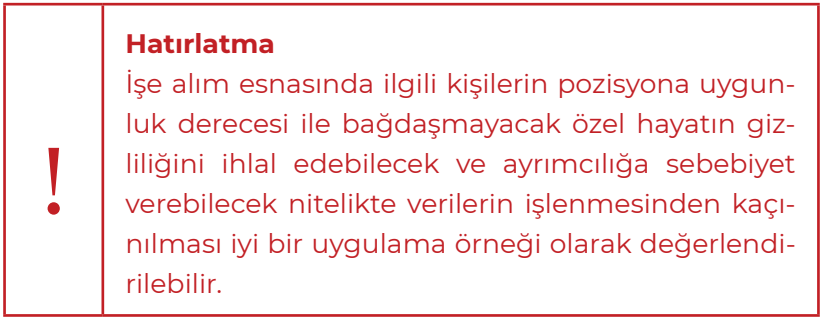
Kişisel veriler, Kanun'un 4'üncü maddesinde belirtilen genel ilkelere uygun bir şekilde işlenmelidir. Kanun'da bu ilkeler; *"a) hukuka ve dürüstlük kurallarına uygun olma b) doğru ve gerektiğinde güncel olma c) belirli, açık ve meşru amaçlar için işlenme ç) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"* şeklinde sıralanmaktadır.

#### 3.1.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma

Hukuka ve dürüstlük kuralına uygun olma, kişisel verilerin işlenmesinde hukuki düzenlemelerle getirilen ilkelere uygun hareket edilmesi ve kişisel veri işlenmesi neticesinde planlanan amaca ulaşmaya çalışırken, ilgili kişilerin çıkarları ve makul beklentilerinin dikkate alınmasını ifade etmektedir.

4 Ayrıntılı bilgi için bkz. Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf.

Bu kapsamda kişisel verilerin işlenmesi süreçlerinde ilgili kişinin makul beklentileri dışında aleyhine sonuç çıkarılmasının önüne geçilmesi, açık rıza alınmasına gerek olmayan bir hususa ilişkin açık rıza alınması suretiyle ilgili kişilerin yanıltılmasından kaçınılması ve açık rızanın bir hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemesi yerinde bir yaklaşım olacaktır.




Bununla birlikte kurumlar tarafından Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğünün[5] Kanun'a uygun bir biçimde yerine getirilmesi de hukuka ve dürüstlük kuralına uygun olma ilkesine hizmet etmektedir. Bu doğrultuda kişisel verilerin hangi amaçla neden kullanıldığı, hangi yöntemlerle elde edildiği, kimlere aktarıldığı, ilgili kişilerin muhatapları, irtibat sağlayacakları yöntemler ve sahip oldukları haklara ilişkin bilgilendirilmelerine ve bu yolla daha bilinçli tercihler yapmalarına, veri işlemenin olası sonuçlarını anlamalarına ve ilgili kişilerin haklarını etkin bir biçimde kullanmasına imkân sağlamaktadır.

5 Ayrıntılı bilgi için bkz. 3.4. Aydınlatma Yükümlülüğü.

### 3.1.2. Doğru ve Gerektiğinde Güncel Olma

Kişisel verilerin doğru ve gerektiğinde güncel olmasının sağlanması noktasında veri sorumlusunun aktif özen yükümlülüğü bulunmaktadır. Veri sorumlusu her zaman ilgili kişinin kişisel verilerinin doğru ve güncel olmasını temin edecek kanalları açık tutmalıdır. Söz konusu düzenlemede yer verilen "gerektiğinde güncel olma" ifadesi önem arz etmekte olup bu ifade, veri sorumlularınca her daim verinin güncel tutulmasına yönelik tedbirlerin alınmasından ziyade verinin ihtiyaca binaen işlenmesi durumunda güncelliğinin kontrol edilmesi anlamına gelmektedir.

Kişilerin, güncel olmayan veya yanlış kaydedilen kişisel verileri nedeniyle zarar gördüğü durumlar söz konusu olabilmektedir. Örneğin, bir kişinin veri sorumlusunun sisteminde kayıtlı telefon numarasının doğru olmaması ya da artık ilgili kişi tarafından kullanılmıyor olması, o kişiye ilişkin gerçek bir veriyi yansıtmadığından hatalı sonuçların ortaya çıkmasına neden olabilmektedir. Yine, adres bilgisi yanlış kaydedilen bir kişinin kendisine ait tebligatları zamanında alamaması veya tebligatın yanlış bir kişiye tebliğ edilmesi durumlarında ilgili kişi maddi ve manevi zarar görebilir. Bu ilke, ilgili kişinin haklarını koruduğu gibi veri sorumlusunun da menfaatlerine yönelik bir koruma sağlamaktadır.

!

**Hatırlatma**

Vatandaşa sunulan hizmetler kapsamında e-mail, cep telefonu, adres gibi verilerin belirli aralıklarla doğruluğunun teyit edilmesi, bilgilerin güncel durumu yansıtmamasından kaynaklı taleplerin dikkate alınması, personele ilişkin özlük dosyalarında yer alan bilgi ve belgelerin doğru ve güncel durumu yansıtmasında fayda bulunmaktadır.

Kişisel verilerin doğru ve gerektiğinde güncel tutulabilmesini temin etmek amacıyla; kişisel verilerin elde edildiği kaynakların belirli olması ve kişisel verilerin toplandığı kaynağın doğruluğunun tespit edilmesi ile kişisel verilerin doğru olmamasından kaynaklı ilgili kişiler açısından olumsuz sonuçlar ortaya çıkmasının önlenmesi kapsamında ilgili kişilerce beyan edilen iletişim bilgilerinin doğrulanmasına yönelik (telefon numarası ve/veya e-posta adresine doğrulama kodu/linki gönderilmesi vb.) makul önlemler alınması gerekli görülmektedir.[6]

6 Ayrıntılı bilgi için bkz. Kişisel Verileri Koruma Kurulunun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/6858/2020-966.

### 3.1.3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

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

!

**Hatırlatma**

Veri sorumluları tarafından Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğünün yerine getirilmesi esnasında amaca ilişkin genel ifadeler kullanımından kaçınılması, amacın daha spesifik ifadelerle açıklanması ve ilgili kişiye belirtilen amaçlar dışında kişisel verilerin kullanılmaması önem arz etmektedir.

### 3.1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

İşlenen kişisel veri, sadece amacın gerçekleştirilmesi için gerekli olan kadarıyla sınırlı tutulmalıdır. Bu kapsamda işlenmesi öngörülen verilere neden ihtiyaç duyulduğu net olarak belirlenmeli, yalnızca söz konusu amacı gerçekleştirmeye yönelik yeterli kişisel veri temin edilerek bunun dışındaki amaçlar için kişisel veri işlenmesinden kaçınılmalıdır. Bununla birlikte kişisel veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurularak kişisel verinin amacı gerçekleştirecek ölçüde işlenmesi gerekmektedir.

Örneğin; sunulan bir hizmet kapsamında gerekli olmayan bilgilerin işlenmesinden kaçınılması, mevcut işe alımın sınırları dışında personel adayından gerekli olmayan ek bilgi ve belge talep edilmemesi, gerçekleştirilen disiplin soruşturması kapsamında yalnız somut olay ile bağlantısı bulunan kişisel verilerin işlenmesi, yüksek güvenlik gerektirmeyen yerlerde işe giriş çıkış takibi kapsamında biyometrik verilerin işlenmesi yerine alternatif yöntemlerin tercih edilmesi gibi hususlar kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü işlenmesine ilişkin olarak veri sorumlularına yarar sağlayacaktır.

### 3.1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre kadar Muhafaza Edilme

Kişisel verilerin, işleme amacı ortaya konulduktan sonra işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir. Buna göre veri sorumluları tarafından mevzuatta öngörülmüş bir süre varsa bu süreye uyulmalı eğer mevzuatta bir süre öngörülmemişse kişisel veriler, ancak işlendikleri amaç için gerekli olan süre kadar saklanmalıdır. Kişisel verilerin işlenme amacının veya geçerli hukuki dayanağının ortadan kalktığı durumlarda veriler imha edilmelidir.

Bununla birlikte, Kanun'un 16'ncı maddesi uyarınca Veri Sorumluları Siciline (VERBİS) kayıt olma yükümlülüğü[7] bulunan veri

7 Ayrıntılı bilgi için bkz. 3.8. VERBİS'e Kayıt Yükümlülüğü.

sorumlularının saklama ve imha politikası hazırlaması zorunlu olup ilgili politikada belirtilen sürelerin ise VERBİS'te yer alan sürelerle uyuşması gerekmektedir. Saklama ve imha politikası hazırlama yükümlülüğü bulunmayan veri sorumlularının ise Kanun ve 28.10.2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in (İmha Yönetmeliği) 5'inci maddesi uyarınca kişisel verileri saklama veya imha etme yükümlülükleri devam etmektedir.

Örneğin; ilgili mevzuat kapsamında belirlenen sürelere riayet edilerek resmî belgelerin saklanması[8], mevzuatta saklama süresi belirlenmeyen işleme faaliyetleri bakımından dikkatli değerlendirmeler yapılması ve düzenli aralıklarla kontrol edilerek kişisel verilerin imha edilmesi tavsiye edilmektedir.

### 3.2. Kişisel Veri İşleme Şartlarının Doğru Belirlenmesi

Kişisel verilerin işlenmesi sürecinde, işlenecek verinin niteliğinin doğru şekilde belirlenmesi büyük önem taşımaktadır. Zira kişisel verinin niteliği, hangi işleme şartına dayanılarak veri işleme faaliyetinin gerçekleştirileceğini doğrudan etkilemektedir. Özel nitelikli kişisel verilerin işlenmesi söz konusu olduğunda Kanun'un 6'ncı maddesi, diğer kişisel veriler bakımından ise Kanun'un 5'inci maddesi esas alınmalıdır. Bu kapsamda her veri işleme faaliyeti, işlenen verinin

8 Kişisel Verileri Koruma Kurulunun 28.06.2018 tarihli ve 2018/69 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5366/2018-69.

türü, amacı ve ilgili mevzuat çerçevesinde değerlendirilerek doğru işleme şartına dayandırılmalıdır. Bu yaklaşım, ilgili kişilerin haklarının korunmasını sağlarken veri sorumlularının hukuka uygun hareket etmesine de katkıda bulunmaktadır.

Her veri işleme faaliyeti Kanun'da düzenleme altına alınan işleme şartlarından en az birine dayandırılmak zorundadır. Öte yandan kişisel veri işleme faaliyetinin amacı bakımından birden fazla kişisel veri işleme şartının dayanak olarak gösterilebilmesi de mümkündür. Hâlihazırda işlenmekte olan veriler için işleme şartlarından herhangi biri uygulama alanı bulmuyorsa veri sorumlusu kişisel veri işleme süreçlerini yeniden gözden geçirerek Kanun'a uygun hâle getirmekle yükümlüdür. Bu süreçte açık rıza dışındaki işleme şartlarının uygulanması mümkünse (örneğin, bir sözleşmenin ifası için gerekli olması ya da yasal bir yükümlülüğün yerine getirilmesi gibi durumlarda) ilgili veri işleme şartına dayalı olarak kişisel veri işlenmelidir.

Eğer açık rıza dışında herhangi bir veri işleme şartına dayanılması mümkün değilse ilgili kişilerden açık rıza alınmalı veya açık rızanın temin edilemediği durumlarda işleme faaliyeti derhal durdurularak kişisel verilerin güvenli bir şekilde imha edilmesi sağlanmalıdır. Ayrıca açık rıza bakımından veri sorumlularının daha yüksek bir özen yükümlülüğüyle hareket etmesi gerekmektedir. Açık rızanın geçerli kabul edilebilmesi için ilgili kişiye yapılacak bilgilendirmenin açık, anlaşılır ve belirli olması, rızanın özgür iradeyle ve herhangi bir şartın gerçekleşmesine bağlanmaksızın verilmesi zorunludur. Bu kapsamda

açık rıza, diğer işleme şartlarının uygulanamadığı durumlarda başvurulabilecek istisnai bir hukuki dayanak olup veri işleme faaliyetinin zorunlu bir şartı hâline getirilemez.

Örneğin, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 13'üncü maddesi uyarınca, iş kazasının meydana gelmesi hâlinde işverenler veya sigortalılar tarafından olayın yetkili kolluk kuvvetlerine ve Sosyal Güvenlik Kurumu'na belirlenen süreler içinde bildirilmesi zorunludur. Bu kapsamda SGK tarafından sigortalının kimlik bilgileri, işyeri bilgileri, olayın tarihi ve yeri, kazanın niteliği, sağlık durumu ve iş göremezlik bilgileri gibi genel ve özel nitelikli kişisel verileri işlenmektedir. Söz konusu veri işleme faaliyeti, SGK'nın kanundan doğan görev ve yetkisi kapsamında yürütülmekte olup kişisel veriler "Kanunlarda açıkça öngörülme" ve "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" şartlarına dayanarak işlenmektedir. Buna rağmen, söz konusu kişisel verilerin SGK'ya aktarılması için ilgili kişiden açık rıza alınması halinde, kanunda yer alan kişisel veri işleme şartlarına dayanarak gerçekleştirilen veri işleme faaliyeti, hukuka aykırı olarak açık rıza şartına bağlanmış olacaktır.

Ayrıca yerleşik uygulama dikkate alındığında, kamu kurum ve kuruluşlarının kamu gücüne dayalı olarak yürüttükleri faaliyetlerde meşru menfaat işleme şartının kullanılması konusunda ihtiyatlı olunmasında fayda bulunmaktadır. Kamu kurumlarının faaliyetlerinin ağırlıklı olarak kanunla verilen görevler ile idari yetkilere dayanması sebebiyle, bu işleme şartının kamu kurumlarında her zaman uygun bir hukuki temel oluşturmayabileceği göz önünde bulundurulmalıdır. Bunun yanında, kamu kurumlarında kişisel veri işleme faaliyetleri çoğu durumda Kanun'da düzenlenen kanuni zorunluluk, kamu görevinin yerine getirilmesi veya bir hakkın kullanılmasına ilişkin yürütüldüğü için, meşru menfaat şartının kullanımı dikkatli bir değerlendirmeyi gerektirir.

Ayrıca veri sorumluları yalnızca uygun işleme şartının tespitiyle yetinmemeli, aynı zamanda bu şartların doğru ve etkin şekilde uygulanmasını da sağlamalıdır. Bu çerçevede veri işleme süreçlerinin belgelenmesi, işlenen verilerin amaca uygunluğunun ve gerekliliğinin düzenli olarak denetlenmesi yerinde bir uygulama olacaktır. Kanun kapsamında bir işleme şartının varlığı altında kişisel veri işlenmesi esnasında; ilgili kişinin haklarının korunması, veri işleme amacına uygun hareket edilmesi ve veri güvenliğinin sağlanması hususlarında dikkatli olunması önem arz etmektedir. Tüm bu tedbirler, kişisel verilerin hukuka uygun şekilde işlenmesini temin ederken aynı zamanda veri sorumlularının hukuki yükümlülüklerini yerine getirmesini sağlamaktadır.

Örneğin, 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu'nun (6458 sayılı Kanun) "Kişisel veriler" başlıklı 99'uncu maddesinde yabancılar ile başvuru ve uluslararası koruma statüsü sahiplerine ait kişisel verilerin, Göç İdaresi Başkanlığı veya valiliklerce ilgili mevzuata ve taraf olunan uluslararası anlaşmalara uygun olarak alınacağı, korunacağı, saklanacağı ve kullanılacağı ifade edilmiş olup İçişleri Bakanlığı Göç İdaresi Başkanlığının yabancılara ilişkin kişisel verileri işlemesi, Kanun'un 5'inci maddesinin ikinci fıkrasının (a) bendinde ifade edilen "Kanunlarda açıkça öngörülme" işleme şartına dayanmaktadır.

### 3.3. Kişisel Verilerin Hukuka Uygun Olarak Aktarılması

Kanun'un 8'inci maddesinde kişisel verilerin yurt içinde aktarılmasına, 9'uncu maddesinde ise kişisel verilerin yurt dışına aktarılmasına ilişkin hükümlere yer verilmiştir. Kanun'un *"Kişisel verilerin aktarılması"* başlıklı 8'inci maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın aktarılamayacağı ancak 5'inci maddenin ikinci fıkrasında ve yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında yer alan şartlardan birinin varlığı hâlinde ilgili kişinin açık rızası aranmaksızın da kişisel verilerin aktarılabileceği hüküm altına alınmıştır.

Buna ek olarak Kanun'un 8'inci maddesinin üçüncü fıkrası ve 9'uncu maddesinin onuncu fıkrasında kişisel verilerin üçüncü kişilere aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlemelerine yer verilmiştir. Söz konusu hükümler aktarıma

cevaz veren hükümler olabileceği gibi aktarımı yasaklayıcı hükümler de olabilmektedir. Bu çerçevede, kişisel veri aktarım faaliyetlerinin hukuka uygun olarak gerçekleştirilmesi için kişisel veri aktarımının taraflarınca ***Kanun ve ilgili diğer mevzuat hükümleri kapsamında aktarıma dayanak oluşturan hukuki gerekçelerin ortaya konulması gerekmektedir.***

Bu kapsamda kişisel verilerin aktarılmasına ilişkin Kanunda yalnızca genel çerçeve belirlenmiş olup aktarımın hukuka uygun olup olmadığının tespit edilebilmesi için diğer kanunlarda yer alan aktarıma ilişkin düzenlemelerin dikkate alınması gerekir.

Zira diğer kanunlar kapsamında kişisel veri aktarımına cevaz veren yahut kişisel verilerin aktarımını yasaklayan nitelikte hükümler bulunması mümkündür. Bu çerçevede, kişisel verilerin aktarımı söz konusu olduğunda Kanun hükümleri ile birlikte Kanunun 8' inci maddesinin üçüncü fıkrasından ve Kanunun 9' uncu maddesinin onuncu fıkrasından atıfla diğer kanunlarda yer alan aktarım hükümlerinin de göz önünde bulundurulması gerekecektir.

Bununla birlikte kamu kurum ve kuruluşlarının kendi aralarında veya diğer gerçek kişi veya özel hukuk tüzel kişileri arasında gerçekleştirilecek veri aktarımlarında her durumda Kanun'un genel ilkelerine uyumun sağlanması gerekmekle beraber izlenecek usul ve uygulanacak şartların belirlenmesi açısından aktarımın mahiyeti, tarafların niteliği ve yurt içi ve yurt dışı aktarım hususlarının dikkatle değerlendirilmesi gerekmektedir.

### 3.3.1. Kişisel Verilerin Yurt İçinde Aktarılması

Kişisel verilerin kamu kurum ve kuruluşları tarafından yurt içinde aktarılmasına ilişkin aktarımın hukuka uygunluğunun, Kanun'un 8'inci maddesi hükümleri ile özel mevzuat düzenlemeleri çerçevesinde değerlendirilmesi gerekmektedir.

Kamu kurum ve kuruluşları ya da kamu kurum ve kuruluşları ile gerçek kişiler veya özel hukuk tüzel kişileri arasında gerçekleşecek kişisel veri aktarımları, Kanun'un 8'inci maddesi kapsamında kişisel veri aktarımı niteliğini haiz olup söz konusu aktarım faaliyetinin Kanun'a uygun olabilmesi için Kanun'un 8'inci maddesi hükümlerine uygun olarak gerçekleşmesi gerekmektedir.

Örneğin; bir Bakanlığın eski hükümlü işçi istihdamı için Ceza ve Tevkifevleri Genel Müdürlüğü'nden kişisel verileri talep etmesi durumunda kişisel verilerin kamu kurum ve kuruluşları arasında aktarımı söz konusudur. Bu kapsamda gerçekleştirilecek tüm kişisel veri aktarımlarının, Kanun'un 8'inci maddesinde belirtilen hükümlere uygun biçimde gerçekleştirilmesi zorunludur.

Örneğin; Gelir İdaresi Başkanlığı'nın vergi denetim süreçlerinde kamu kurumlarından mali veriler talep etmesi, Sağlık Bakanlığı'nın hastalıkların önlenmesi ve kamu sağlığının korunması amacıyla Sosyal Güvenlik Kurumu'ndan reçete ve tedavi verilerini talep etmesinde de yurt içi veri aktarımı söz konusudur.

Kamu kurumları arasında gerçekleştirilen veri aktarımları çoğu zaman kamu hizmetlerinin yürütülmesi amacıyla mevzuattan kaynaklanan yetkilere dayanılarak yapılmaktadır. Dolayısıyla Kanun'un 5'inci ve 6'ncı maddelerinde yer alan işleme şartlarının aktarım yetkisinin dayanağını oluşturan açık kanuni hüküm veya diğer özel mevzuat düzenlemeleri ile birlikte bütüncül bir biçimde değerlendirilmesi gerekmektedir. Zira kamu kurumlarının veri aktarımı konusundaki yetkileri mutlak olmayıp özel kanunlarla sınırlanabilmekte ya da belirli şartlara bağlanabilmektedir. Bu nedenle kişisel verilerin hangi kapsamda aktarılabileceği konusunda özel düzenlemeler içeren mevzuat hükümlerine öncelikle başvurulması, aktarımın kapsamı ile sınırlarının açıkça belirlenmesi ve hukuka uygunluk hususları açısından önem arz etmektedir. Ayrıca kişisel veri aktarımı öncesinde aktarımın hukuki dayanağının açık bir şekilde ortaya konulması ve yalnızca aktarım amacına uygun ölçüde veri aktarımı yapılması gerekmektedir.

### 3.3.2. Kişisel Verilerin Yurt Dışına Aktarılması

12.03.2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 34'üncü maddesi ile Kanun'un *"Kişisel verilerin yurt dışına aktarılması"* başlıklı 9'uncu maddesinde değişiklik yapılmış olup söz konusu değişiklikler 01.06.2024 tarihinde yürürlüğe girmiştir. Yeni düzenleme ile kişisel verilerin yurt dışına aktarılması bakımından üç basamaklı bir yapı oluşturulmuştur.

Buna göre kişisel verilerin yurt dışına aktarılabilmesi için;

- Kanun'un 5'inci ve 6'ncı maddelerinde belirtilen kişisel veri işleme şartlarından birinin varlığına ek olarak aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması,

- Yeterlilik kararının bulunmaması halinde ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla Kanun'da yer alan uygun güvencelerden birinin varlığı,

- Yeterlilik kararı veya uygun güvencenin bulunmaması durumunda arızi olmak kaydıyla Kanun'un 9'uncu maddesinin altıncı fıkrasında yer alan istisnai hallerin varlığı

gerekmektedir.

Ayrıca uluslararası sözleşme hükümleri saklı kalmak üzere Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar görme ihtimalinin söz konusu olduğu durumlarda kişisel veriler, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kişisel Verileri Koruma Kurulu'nun (Kurul) izniyle yurt dışına aktarılabilecektir.

Yurt dışına kişisel veri aktarımı planlayan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının, aktarım yapılacak yabancı ülkedeki kamu kurumları veya uluslararası kuruluşlarla yapacakları ve kişisel verilerin korunmasına yönelik hükümlere yer veren bir anlaşma aracılığıyla uygun güvence sağlamaları mümkündür.

Uluslararası sözleşme niteliğinde olmayan anlaşmalara dayalı aktarıma ilişkin usul ve esaslar, 10.07.2024 tarihli ve 32598 sayılı Resmî Gazete'de yayımlanan "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"in (Aktarım Yönetmeliği) 11'inci maddesinde düzenlenmektedir. Anlaşmada yer alan veri koruma hükümleri, taraflar arasında gerçekleştirilecek kişisel veri aktarımlarında yeterli güvenceyi sağlayan bir mekanizma işlevi görmektedir. Söz konusu anlaşma, kişisel veri aktarımı gerçekleştirecek olan taraflar arasında akdedilecek olup bu anlaşmanın müzakere süreçlerinde Kurulun görüşüne başvurulması gerekmektedir. Ayrıca bu anlaşmaya istinaden kişisel verilerin yurt dışına aktarılabilmesi için veri aktaran tarafından Kurula izin başvurusunda bulunulması ve kişisel veri aktarımına Kurul tarafından izin verildikten sonra başlanması zorunludur.

Yeterlilik kararı bulunmaması ve uygun güvencelerden herhangi birinin sağlanamaması durumunda kişisel verilerin yurt dışına aktarımı yalnızca istisnai hâllerden birinin varlığı hâlinde arızi olmak kaydıyla gerçekleştirilebilir. Söz konusu istisnai haller Kanun'un 9'uncu maddesinin altıncı fıkrasında tahdidi olarak sayılmıştır. Bu kapsamda "*a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi. b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması. c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması. ç) aktarımın üstün bir kamu yararı için zorunlu olması d) bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması e) fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması. f) kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması.*" hâllerinde kişisel verilerin yurt dışına aktarılması istisnai olarak mümkün olabilmektedir.

Örneğin, yabancı bir kamu kurumunun, Türkiye'deki bir taşınmaza ilişkin malik bilgisine mevzuata uygun bir şekilde ve yetkili kurum sıfatıyla tapu sicilinden erişim talep etmesi durumunda, kamuya açık bir sicilden, ilgili mevzuatta öngörülen yasal erişim şartlarının sağlanması koşuluyla veri temin edilmesinden söz edilebilmesi mümkündür.

Diğer taraftan Kanun'un 9'uncu maddesinin yedinci fıkrasında, ilgili hükmün altıncı fıkrasının (a), (b) ve (c) bentlerinin, kamu kurum ve kuruluşlarının **kamu hukukuna tâbi faaliyetlerine** uygulanmayacağı hüküm altına alınmıştır. Bu doğrultuda kamu kurumlarının özel hukuk ilişkisi niteliğindeki faaliyetleri (örneğin bir kamu bankasının ticari işlemleri, üniversitenin iktisadi işletmesinin faaliyetleri, belediye şirketlerinin faaliyetleri) istisnai aktarım halleri kapsamında değildir. Dolayısıyla bu faaliyetlerde Kanun'un 9'uncu maddesinin 6'ncı fıkrasında yer alan arızi aktarım hallerinin tamamı uygulanabilmektedir.

Son olarak kişisel verilerin yurt dışına aktarımına ilişkin süreçlerde Kurum tarafından yayımlanan "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"[9]nin dikkate alınması hem hukuka uygunluğun sağlanması hem uygulamada karşılaşılabilecek tereddütlerin giderilmesi açısından faydalı olacaktır.

9 Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf.

### 3.4. Aydınlatma Yükümlülüğü

Kanun'un 10'uncu maddesi uyarınca veri sorumluları her durumda ilgili kişilere karşı aydınlatma yükümlülüğünü yerine getirmelidir. Bu kapsamda kişisel verilerin ***elde edilmesi sırasında*** veri sorumlusu veya yetkilendirdiği kişi, *"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"* hususlarında ilgili kişilere bilgi vermekle yükümlüdür.

Aydınlatma yükümlüğü yerine getirilirken ilgili kişilerin yazılı, sözlü, elektronik ortamda gönderilecek e-posta, ses kaydı, web sayfası, duyuru panosu veya çağrı merkezi gibi platformlar aracılığıyla bilgilendirilmesi mümkün olmakla birlikte aydınlatma yükümlülüğünün yerine getirildiğine ilişkin ispatın veri sorumlusuna ait olduğu unutulmamalıdır. Bu kapsamda aydınlatma metinleri herhangi bir onaya/izine tabi olmamakla birlikte ispat yükümlülüğünün yerine getirildiğinin bir göstergesi olarak personele sunulan aydınlatma metinlerinin imzalatılıp özlük dosyasına kaldırılması iyi bir uygulama örneği olacaktır.

Örneğin; Kurumların ilgili kişi gruplarını ayrıştırmak suretiyle çalışanlarına ilişkin işlediği kişisel veriler bakımından "personel aydınlatma metni" hazırlaması, internet sitesinde "web sitesi aydınlatma metni"nin yer alması, Kuruma ziyaretçi giriş çıkışlarında "ziyaretçi aydınlatma metni" nin ilgililere sunulması gerekmekte olup söz konusu metinler hazırlanırken ilgili kişiye yapılacak bildirimin anlaşılır ve sade olmasına, metinlerde muğlak ifadelerden kaçınılmasına, metinlerde eksik, yanıltıcı veya yanlış bilgilere yer verilmemesine dikkat edilmelidir.

!

**Hatırlatma**

İş yerlerinde hukuki yükümlülüğün yerine getirilmesi kapsamında kameralar aracılığı ile görüntü kaydı alınabilmektedir. Bu kapsamda veri sorumluları ilgili kişileri görüntü kaydı alındığına ilişkin bilgilendirmeli, söz konusu hususlara aydınlatma metninde yer verilmelidir. Ayrıca sembol, işaret ve ikonlar kullanılmak suretiyle katmanlı aydınlatma da yapılabilir.

Uygulamada veri sorumluları tarafından görüntü ve ses kaydı alabilen kameralar aracılığı ile veri işleme faaliyeti gerçekleştirilebilmektedir. Ancak amacı gerçekleştirmeye yönelik yeterli verinin temin edilmesi, bunun dışındaki amaç için gerekli olmayan verilerin işlenmesinden kaçınılması, veri işlemenin, amacı gerçekleştirecek ölçüde olması gerekmektedir. Bu kapsamda kameralar vasıtasıyla görüntü ile birlikte ses kaydı yapılmasından kaçınılması yerinde bir uygulama örneği olacaktır.

!

**Hatırlatma**

Bakanlığa bağlı taşrada bir kamu kuruluşunun işlediği kişisel veriler bakımından Kanun'un 10' uncu maddesi kapsamında aydınlatma yükümlülüğü yerine getirilirken veri sorumlusunun Bakanlık olduğu göz önünde bulundurulmalıdır.

Ayrıca 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (Aydınlatma Tebliği) 4'üncü maddesi uyarınca kişisel verilerin elde edilmesi sırasında veri sorumluları ya da yetkilendirdiği kişilerce ilgili kişilerin bilgilendirilmesi gerekmekte olup kişisel verilerin doğrudan ilgili kişiden elde edilmemesi halinde ise Aydınlatma Tebliği'nin 6'ncı maddesi uyarınca;

- Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde,
- Kişisel veriler ilgili kişi ile iletişim amacıyla kullanılacaksa ilk iletişim kurulması esnasında,
- Kişisel veriler aktarılacaksa en geç, kişisel verilerin ilk kez aktarımının yapılacağı esnada

aydınlatma yükümlülüğü yerine getirilmelidir. Ayrıca aydınlatma metinlerinin değişen koşullar uyarınca güncellenmesi ve varsa hata ve eksiklerin giderilmesi önem arz etmektedir[10].

10 Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi,https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf.

Kurulun, öğretim görevlisi ve araştırma görevlisi kadrolarına yapılacak atamalarda adaylardan talep edilen kişisel veri niteliğindeki bilgilerin internet ortamında yayımlanması uygulaması hakkında 26.12.2019 tarihli ve 2019/389 sayılı Kararı[11] ile *"Kanun'un 10' uncu maddesinde hükme bağlanan aydınlatma yükümlülüğü kapsamında, üniversiteler tarafından söz konusu kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerin aydınlatılması gerektiğine"* karar verilmiştir.

Kurulun, bir üniversite tarafından verilen eğitimde eğitim alan kişilerin kişisel verilerini içeren yoklama listesinin diğer katılımcılar tarafından görülebilir şekilde düzenlenmesine ilişkin 02.12.2021 tarihli ve 2021/1214 sayılı Kararı[12] ile *"Kanun'un 15'inci maddesinin (5) numaralı fıkrası çerçevesinde; veri sorumlusu Üniversiteye eğitim verilirken kursiyerlere ait kişisel verilerin işlenmesi sürecinde Kanun'un "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10'uncu maddesi ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de yer verilen hükümlere uygun olacak şekilde bir uygulama geliştirmesi ve bu hususa ilişkin olarak Kurula bilgi verilmesi yönünde talimat verilmesine"* karar verilmiştir.

11 Kişisel Verileri Koruma Kurulunun 26.12.2019 tarihli ve 2019/389 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6668/2019-389.

12 Kişisel Verileri Koruma Kurulunun 02.12.2021 tarihli ve 2021/1214 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7270/2021-1214.

**Hatırlatma**

Açık rıza alınması gereken hallerde, Aydınlatma Tebliği'nin 5'inci maddesinin birinci fıkrasının (f) bendinde yer alan hüküm gözetilerek açık rıza ve aydınlatma metinleri ayrıştırılmalıdır.

Bu kapsamda kişisel verilerin elde edildiği sırada ilgili kişilere aydınlatma metni sunulmalı, söz konusu aydınlatma metninde geçen kişisel veri işleme faaliyetlerinden herhangi birinin hukuki dayanağının açık rıza olması durumunda ilgili kişiye ayrıca bir açık rıza metni sunulmalıdır.

### 3.5. Veri Güvenliğine İlişkin Yükümlülükler

Bilindiği üzere Kanun'un 12'nci maddesinde kişisel veri güvenliğine ilişkin yükümlülükler düzenlenmiştir. Kanun'un 12'nci maddesinin birinci fıkrası çerçevesinde veri sorumlusu olan kamu kurum ve kuruluşları; kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Veri sorumluları, bu tedbirleri hem kendi bünyesinde almalı hem de kendisi adına kişisel veri işleme faaliyeti yürüten başka gerçek veya tüzel kişiler bulunması durumunda bu kişilerce alınmasını sağlamalıdır. Zira Kanun'un 12'nci maddesinin ikinci fıkrası gereğince veri sorumluları, birinci fıkrada belirtilen tedbirlerin alınması

hususunda bu kişilerle birlikte müştereken sorumludur. Ayrıca veri sorumluları, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla kendi kurum veya kuruluşunda gerekli denetimleri yapmak veya yaptırmak zorundadır.

Bununla birlikte Kanun'un 12'nci maddesinin dördüncü fıkrası gereğince, 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.

Alınması gereken kişisel veri güvenliği tedbirleri ile ilgili olarak veri sorumlularına rehberlik etmek ve alınabilecek tedbirlerle ilgili örnekler sunmak amacıyla Kurum tarafından "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)[13]" hazırlanmış ve veri sorumlularının istifadesine sunulmuştur. Veri sorumluları, kişisel veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi kapsamında kendi kişisel veri işleme kapasiteleri, veri kayıt sistemlerinin yapısı ve işledikleri kişisel verilerin niteliğini de göz önünde bulundurarak veri güvenliğine ilişkin risk/tehdit analizi yapmalı ve buna uygun olarak gerekli teknik ve idari tedbirleri Rehber'den de faydalanarak almalıdır.

Kişisel veri güvenliğinin sağlanması adına öncelikle işlenen tüm kişisel veriler ile bu verilerin güvenliğini riske atabilecek hususların

13 Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc-5b-8d5cf125e3a1.pdf

neler olduğu belirlenmeli, bu risklerin gerçekleşmesi durumunda yol açacağı kayıpların neler olabileceğine ilişkin analiz yapılarak buna uygun tedbirler alınmalıdır.

Siber tehditlerin her geçen gün daha tehlikeli hale geldiği ve veri sorumlularının da gün geçtikçe daha sık siber saldırıya uğradığı hususları dikkate alındığında kamu kurum ve kuruluşlarında kişisel veri güvenliğinin sağlanması adına güçlü bir siber güvenlik altyapısının oluşturulmasının ne denli önemli olduğu anlaşılacaktır. Siber güvenliğin sağlanması adına anti-virüs ile anti-spam yazılımları, saldırı tespit ve önleme sistemleri (IDS/IPS), veri kaybı/sızıntısı önleme sistemleri (DLP), güvenlik duvarı, ağ geçidi, güvenlik bilgi ve olay yönetimi (SIEM) sistemleri, genişletilmiş tespit ve yanıt sistemi (XDR), içerik silahsızlandırma ve yeniden yapılandırma (CDR) gibi farklı çözümlerin bir arada kullanılması da dahil olmak üzere gerekli değerlendirmeler yapılmalı ve bu değerlendirmelere göre uygun çözümler hayata geçirilmelidir. Kişisel veri barındıran sistemler üzerinde düzenli olarak zafiyet taramaları yapılmalı, yapılacak sızma testleri ile güvenlik açıkları ve zafiyetler belirlenerek bu açıklar/zafiyetler giderilmelidir. Bilişim sistemlerinde kullanılan ürünlere ilişkin güncellemelerin aksatılmaması, düzenli olarak güvenlik yamalarının yapılması da yine önem arz etmektedir. Diğer taraftan, kurum içi dokümantasyon sistemlerinde güvenlik sıkılaştırması uygulanarak kritik belge ve verilerin korunması da kişisel veri güvenliğine ilişkin riskleri azaltacaktır.

Kişisel veri güvenliğini riske atabilecek durumların zamanında tespit edilebilmesi ve bunlara müdahalede bulunulabilmesi için kişisel veri güvenliğinin takip ve kontrolünün yapılması da çok önemlidir. Bilişim ağlarında anormal bir durum olup olmadığının kontrolünün yapılması, kullanıcı işlemlerine ilişkin kayıtların tutulması ve bu kayıtların düzenli olarak kontrol edilmesi gibi önlemler alınarak takip ve kontrol mekanizmaları oluşturulmalıdır. Kişisel veri işleme faaliyeti barındıran kamu hizmetlerinde, personele verilen yetkinin kötüye kullanılmasını önlemeye yönelik olarak da tedbirler alınması ve kişisel veri güvenliğinin takibinin yapılması gerekmektedir. Personel tarafından gerçekleştirilen veri işleme faaliyetleri veri sorumlusunun kontrolü ve denetimi altında yürütülmelidir. Özellikle kamu hizmetlerinin ifası kapsamında kişisel veri sorgulamalarının dahil olduğu süreçlere yönelik olarak kullanılan sorgulama sistemlerinde sorgulama limiti uygulanması, aşırı sorgulama/istek/indirme durumlarına karşı alarm sistemleri kurulması gibi etkin tedbirlerin alınması kişisel veri güvenliğinin sağlanması açısından önemlidir.

***Kişisel verilere erişimlerde çalışanlara, görev ve sorumluluklarının gerektirdiği ölçüde erişim yetkisi tanınmalıdır. Bu çerçevede sadece yetkili personelin erişebileceği şekilde kişisel verilere erişimler sınırlandırılmalı, erişim yetki ve kontrol matrisleri oluşturularak uygulamaya alınmalı ve erişimlerde uygun kimlik doğrulama sistemleri uygulanmalıdır.***

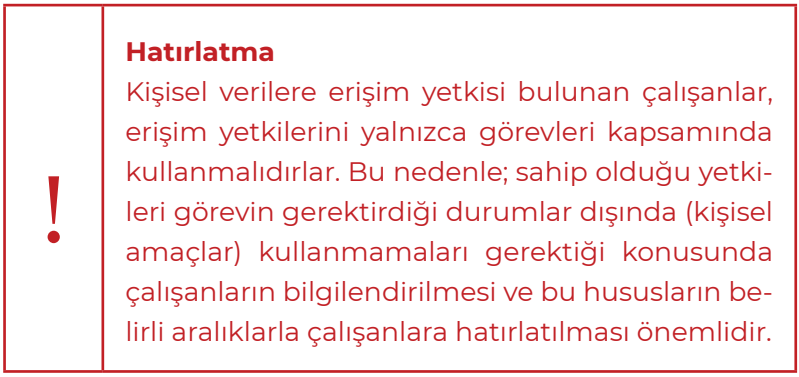
Yeni sistemlerin tedarik edilmesi/geliştirilmesi veya mevcut sistemler üzerinde iyileştirme/güncelleme/bakım yapılması gibi durumlarda da kişisel veri güvenliğine ilişkin gereksinimler mutlaka göz önünde bulundurulmalıdır.

Veri güvenliğinin sağlanması adına kişisel verilerin bulunduğu ortamların da güvenliğinin sağlanması gerekmektedir. Bu kapsamda kişisel verilerin bulunduğu fiziksel ya da dijital ortamlara göre risk ve tehditler belirlenmeli; kişisel verilerin kaybolması, çalınması, tahrip olması, şifrelenmesi, kişisel verilere yetkisiz bir şekilde erişilmesi gibi durumlara karşı bu ortamların güvenliği sağlanmalıdır.

Kişisel verilerin herhangi bir sebeple şifrelenmesi, yok edilmesi, değiştirilmesi vb. ihtimaller göz önünde bulundurularak kişisel veri kayıplarının önüne geçilmesi adına uygun yedekleme stratejileri belirlenmeli ve uygulanmalıdır.

Personelin veri güvenliği farkındalığına sahip olması da kişisel verilerin korunmasında son derece kritik öneme sahiptir. Çünkü veri güvenliğini sağlamaya yönelik en gelişmiş teknik tedbirler alınsa dahi farkındalığı düşük personelin dikkatsiz ve/veya bilinçsiz davranışları nedeniyle alınan teknik tedbirler yetersiz kalabilmektedir. Bu nedenle kişisel verilerin korunması ve bilgi güvenliği konularında personele düzenli olarak eğitim verilmesi, güncel risk ve tehditlere yönelik olarak personelin sürekli bilgilendirilmesi, bu eğitimlerin/bilgilendirmelerin veriminin ölçülmesi ve gerektiğinde güncellenmesi kişisel veri güvenliğinin sürdürülebilirliği açısından büyük önem

taşımaktadır. Kişisel veri güvenliği farkındalığı ve KVKK uyumu tek bir birim/departman sorumluluğuna indirgenmemeli; tüm birimlerin rol ve sorumluluk aldığı şekilde kurumsal ölçekte sahiplenilmelidir.




Kişisel veri içeren paylaşımların kurumun bilişim sistemleri ve kurumsal hesaplar üzerinden yapılması kişisel veri güvenliğinin sağlanması açısından önemlidir. Bu çerçevede; kişisel veri paylaşımında kurumun bilişim sistemleri ve kurumsal hesaplarının kullanımının esas olduğu konusunda çalışanların bilgilendirilmesi gerekmektedir. Ayrıca kurumsal e-posta hesaplarının işin gerektirdiği amaçlar dışında (kişisel kullanım vb.) kullanılmaması hususunda çalışanların bilgilendirilmesi de oltalama vb. siber saldırıların gerçekleşmesi ihtimalini azaltabileceği için veri güvenliğine ilişkin alınabilecek tedbirlerdendir.

Kişisel veri güvenliği politika ve prosedürlerinin hazırlanması da kişisel veri güvenliğinin sağlanmasında çok önemli bir yere sahiptir. Hazırlanan politika ve prosedürler kapsamında düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken

hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.

Kişisel verilerin işlenmesinde veri minimizasyonu ilkesi benimsenmeli, işlenen kişisel verilerin mümkün olduğunca azaltılması sağlanmalıdır. Ayrıca kişisel veriler ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Bazı veri sorumluları, kişisel verilerin yanında özel nitelikli kişisel veriler de işleyebilmektedir. Bilindiği üzere Kanun'un 6'ncı maddesinin dördüncü fıkrasında "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*" hükmü yer almaktadır. Bu çerçevede özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler, 31.01.2018 tarihli ve 2018/10 sayılı Karar[14] ile Kurul tarafından belirlenmiştir. Bu kapsamda özel nitelikli kişisel veri işleyen veri sorumlularınca, bahse konu Kurul Kararında yer alan tedbirlerin de alınması gerekmektedir.

Kişisel verilerin korunmasına yönelik olarak alınan tedbirlerin etkinliği ve yeterliliği veri sorumlusu tarafından düzenli olarak denetlenmelidir. Denetim sonucunda; tespit edilen bulgular, iyileştirme alanları ve hedeflenen tamamlanma sürelerini de içeren bir iyileştirme planı ve takvimi oluşturmak veri güvenliğinin sağlanmasında faydalı olacaktır.

14 Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10.

***Kurula intikal ettirilen kişisel veri ihlali bildirimlerine ilişkin yürütülen inceleme süreçlerinde sıkça rastlanan bazı tedbir eksiklikleri, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faydasına sunulmak üzere aşağıda örnek olarak verilmiştir.***

**Sık Karşılaşılan İdari Tedbir Eksiklikleri:**

- Organizasyon büyüklüğü, çalışan sayısı fazlalığı, bütçe ve zaman kısıtları gibi gerekçelerle kişisel veri işleme faaliyetlerinde veri güvenliğine yönelik farkındalık ve eğitim çalışmalarının hiç gerçekleştirilmemesi veya yetersiz düzeyde gerçekleştirilmesi,
- Belirli aralıklarla sosyal mühendislik/oltalama testlerinin gerçekleştirilmemesi,
- Kişisel veri güvenliğine ilişkin politika/prosedürlerin belirlenmesi ve uygulanması noktasında yetersiz kalınması, bu politika ve prosedürlerin gerektiğinde güncellenmemesi,
- Parola güvenliğine ilişkin kurumsal politikaların oluşturulmaması veya uygulanmaması, ortak kullanıcı hesaplarının kullanılmasının ve zayıf parola kullanılmasının engellenmemesi,
- İç denetim mekanizmalarının kurulmaması veya etkili işletilmemesi,
- Kişisel veri güvenliği süreçlerinde risk odaklı bir yaklaşımın benimsenmemesi, düzenli risk/tehdit analizlerinin yapılmaması ve bu analizler doğrultusunda önleyici tedbirler alınmasının planlanmaması,

- Veri minimizasyonu ilkesine uygun hareket edilmemesi,
- Test/analiz ortamlarında yapılan çalışmalarda gerçek kişilere ait kişisel verilerin kullanılması,
- Veri işleyenle yapılan sözleşmelerde kişisel veri güvenliğine ilişkin hususların detaylandırılmaması; kişisel veri güvenliğinin sağlandığından emin olunması adına veri işleyen üzerinde gerekli denetimlerin gerçekleştirilmemesi,

**Sık Karşılaşılan Teknik Tedbir Eksiklikleri:**

- Erişim kontrollerinin yetersiz olması, çalışanlara görevlerini yerine getirmek için gerekli olandan fazla yetki verilmesi,
- Gerekli dikkat ve özenin gösterilmemesi sonucu yetki matrisinin hatalı oluşturulması,
- Uygun yedekleme stratejilerinin belirlenmesi noktasında yeterli özenin gösterilmemesi,
- Ağ güvenliğine ilişkin alınması gereken tedbirler konusunda özensiz davranılması (örn. ağ segmentasyonu yapılmaması),
- Kullanılan siber güvenlik ürünlerinin doğru yapılandırılmaması,
- Yetkisiz erişim riskini azaltabilecek/engelleyebilecek kimlik doğrulama mekanizmalarının hayata geçirilmemesi,
- Yeni geliştirilen yazılımlarda kişisel verilerin korunmasına yönelik güvenlik tedbirlerinin tasarım aşamasında yeterince dikkate alınmaması, güvenli yazılım geliştirme süreçlerinin uygulanmaması ve gerekli kontrol/testlerin yapılmaması,

- Kişisel verilerin API veya web servisler üzerinden paylaşıldığı durumlarda güvenli iletişim protokollerinin kullanılmaması, erişim anahtarlarının uygun şekilde yönetilmemesi, kimlik doğrulama ve yetkilendirme süreçlerinin eksik olması,
- Güncel olmayan veya destek verilmeyen ürünlerin/yazılımların kullanılması,
- Yama/güncelleme yönetimi konusunda yetersiz kalınması,
- Kişisel veri sorgulama sistemlerinde kullanıcı sorgularına ilişkin alarm, izleme ya da sorgu limiti/kotası gibi kontrol mekanizmalarının bulunmaması,
- Kişisel veri güvenliği takibinin yapılabilmesi noktasında gerekli uyarı/alarm/engelleme mekanizmalarının kurulmaması, tespit edilen anomalilere karşı zamanında aksiyon alınmaması,
- Düzenli zafiyet taramaları/sızma testlerinin gerçekleştirilmemesi,
- Kişisel verilere erişim kayıtlarının kullanıcı müdahalesi olmayacak şekilde saklanması hususunda yeterli özenin gösterilmemesi

Bu tür tedbir eksikliklerinin önlenmesi ve zafiyetlerin giderilmesi adına veri sorumlularının; rehberler, bilgi notları, Kurul Kararları başta olmak üzere Kurum tarafından yayımlanan içerikleri dikkate alarak ve kendi iç süreçlerini gözden geçirerek veri güvenliğine ilişkin gerekli teknik ve idari tedbirleri almaları gerekmektedir.

Veri sorumlularının kişisel veri güvenliğine ilişkin yükümlülüklerinden bir diğeri de kişisel veri ihlali yaşanması durumunda bu durumun

en kısa sürede ilgili kişilere ve Kurula bildirilmesi yükümlülüğüdür. Bilindiği üzere Kanun'un 12'nci maddesinin beşinci fıkrasında *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir."* hükmü yer almaktadır. Bu çerçevede kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumun en kısa sürede ilgili kişiye ve Kurula bildirilmesi gerekir. Kişisel veri ihlali bildirimleri gerçekleştirilirken Kurulun 24.01.2019 tarihli ve 2019/10 sayılı Kararı[15] ile belirlenen kişisel veri ihlali bildirim usul ve esaslarına dikkat edilmesi gerekmektedir. Bu kapsamda veri sorumlusunun;

- Veri ihlalini öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirimde bulunması,
- Veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde bildirimde bulunması (ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle),
- İlgili kişilere yapacağı bildirimlerde Kurulun 18.09.2019 tarihli ve 2019/271 sayılı Kararı[16] ile belirlenen asgari unsurlara yer vermesi,

15 Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı Kararı,https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi.

16 Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli ve 2019/271 sayılı Kararı,https://www.kvkk.gov.tr/Icerik/5547/2019-271.

- Veri ihlali ihtimaline yönelik hazırlanan bir veri ihlali müdahale planın bulunması ve bu planın belirli aralıklarla gözden geçirilmesi

gerekmektedir.

Kamuda faaliyet gösteren veri sorumluları, kişisel veri güvenliğini sağlarken yalnızca kişisel verilerin korunmasına ilişkin mevzuata uyum göstermekle yetinmemelidir. Bu yükümlülüklerin yanında, bilgi güvenliği ve kişisel verilerin de dahil olduğu veri işleme süreçlerini düzenleyen diğer yasal düzenlemelere (7545 sayılı Siber Güvenlik Kanunu vb.) uyum sağlanarak hareket edilmelidir. Çünkü kişisel veri güvenliği, farklı yasal düzenlemelerde öngörülen teknik ve idari tedbirlerle bütüncül bir şekilde ele alındığında sürdürülebilir, kapsayıcı ve etkin olacaktır.

### 3.6. İlgili Kişi Haklarının Yerine Getirilmesi

Anayasa'nın 20'nci maddesi gereğince herkes, özel hayatına ve aile hayatına saygı gösterilmesini ve kendisiyle ilgili kişisel verilerin korunmasını isteme haklarına sahiptir. Kişisel verilerin korunmasını isteme hakkı; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsamaktadır. Kanun'un 11'inci maddesi gereğince ilgili kişiler, her zaman veri sorumlusuna başvuruda bulunarak;

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.

Kişisel verilerin korunması hukukunda ilgili kişilere tanınan haklar, veri sorumluları ve veri işleyenler tarafından gerçekleştirilen kişisel verilerin işlenmesi faaliyetlerinin mahiyeti hakkında bilgi sahibi olmak suretiyle ilgili kişilere kişisel verileri üzerinde bir denetim imkânı sağlamaktadır. Bu anlamda kişisel verilerin hukuka aykırı işlenip işlenmediğinin tespit edilebilmesi, hukuka aykırı bir işlem var ise zararın giderilebilmesi açısından önem arz etmektedir.

### 3.6.1. Hak Arama Yöntemleri

Kanun, kişisel verisi işlenen ilgili kişilerin bu haklarını kullanabilmeleri için Kurula şikâyetten önce veri sorumlusuna başvuruda bulunulmasını zorunlu kılmıştır. Bu kapsamda, Kanun'un 13'üncü ve 14'üncü maddelerinde ilgili kişilerin hak arama yöntemleri belirlenmiş olup buna göre, Kanun'un "Veri sorumlusuna başvuru" başlıklı 13'üncü maddesinin birinci fıkrasında; "İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir" hükmü yer almaktadır. Bu çerçevede, bahse konu maddeye dayanılarak hazırlanan 10.03.2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanan "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"in (Veri Sorumlusuna Başvuru Tebliği) "Başvuru usulü" başlığını taşıyan 5'inci maddesinin birinci fıkrasında "İlgili kişi, Kanunun 11'inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir" hükmüne yer verilmekte olup anılan maddenin ikinci fıkrasında ise başvuruda bulunması zorunlu unsurlar; *"ad, soyad ve başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusu"* olarak sıralanmıştır.

!

**Hatırlatma**

İlgili kişinin, Veri Sorumlusuna Başvuru Tebliği'ne uygun şekilde veri sorumlusuna başvuruda bulunabilmesi için veri sorumlusu tarafından *başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulamanın* kullanıma sunulması faydalı olacaktır.

### 3.6.2. Kişisel Verilere İlişkin Düzeltme Talep Etme Hakkı

Kişisel verilerin *"doğru ve güncel olması"*, ilgili kişilerin haklarının korunması açısından büyük önem taşımaktadır. Kanun'un 11'inci maddesi ile *"doğru ve gerektiğinde güncel olma"* ilkesine uygun olarak ilgili kişilere kişisel verilerinin eksik veya hatalı işlenmiş olması durumunda, bu verilerin düzeltilmesini talep etme imkânı sunulmaktadır.

Kanun, ilgili kişilerin eksik veya hatalı işlenen kişisel verilerin düzeltilmesini talep etme hakkına sahip olduğunu, veri sorumlularının, bu talepleri belirli süreler içinde yanıtlamak zorunda olduğunu ve bu hakkın kullanılması üzerine gerçekleştirilen düzeltmelerin, ilgili üçüncü taraflara bildirilmesi gerektiğini düzenlemiştir. Düzeltme hakkı, yalnızca ilgili kişiye ait kişisel verilerin düzeltilmesi talebini içermekte olup üçüncü bir şahsın kişisel verileri bakımından düzeltme hakkının talep edilebilmesi mümkün değildir.

### 3.6.3. Kişisel Verilerin Silinmesi veya Yok Edilmesini Talep Etme Hakkı

Kanun'da *"doğru ve gerektiğinde güncel olma"* ve *"ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"* ilkesini düzenleyen "Genel İlkeler" başlıklı 4'üncü madde, *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi"* başlıklı 7'nci madde ve *"ilgili kişilerin 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme haklarına sahip olduğunu"* düzenleyen 11'inci madde ile kişisel verilerin silinmesi, veya yok edilmesini talep etme hakkı güvence altına alınmıştır. İmha Yönetmeliği ile de söz konusu hakkın kullanılmasına ilişkin detaylı hükümlere yer verilmiştir.

Kanun'un 7'nci maddesi *"Bu Kanun ve ilgili diğer kanun hükümlerine 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."* şeklinde düzenlenme altına alınmıştır. Kanun hükümleri uyarınca silme hakkı sadece ilgili kişinin talebi ile değil aynı zamanda veri sorumlusunun etki alanında bulunan hallerde ilgili kişilerin talebi olmaksızın re'sen yerine getirilecektir. Örneğin, kişisel verilerin saklanmasını gerektiren azami sürenin geçtiği ve bu verileri saklamayı haklı kılacak herhangi bir şartın mevcut olmadığı durumlarda söz konusu kişisel veriler veri sorumlusu tarafından re'sen imha edilmelidir.

İmha Yönetmeliği, silme ve yok etme kavramlarını ayrı ayrı tanımlamıştır. Yönetmeliğin 8'inci maddesi *"Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir"*, 9'uncu maddesi "*Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir*" hükümlerini amirdir.

Geçmiş sağlık verilerinin düzeltilmesine/silinmesine yönelik şikâyetlere ilişkin olarak Kurulun 06.02.2020 tarihli ve 2020/93 sayılı Kararı ile;

- *"...İlgili kişilerin kişisel sağlık verilerinin düzeltilmesi talepleri hususunda, Kişisel Sağlık Verileri Hakkında Yönetmeliğin 13 üncü maddesi kapsamında ilgili il sağlık müdürlüklerine başvuruda bulunmaları ve il sağlık müdürlükleri tarafından başvurularına olumsuz cevap verilmesi sebebiyle Kurula yaptıkları şikâyetler kapsamında; kişisel sağlık verilerinin işlenme şartlarının "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi" şartının ortadan kalkmaması sebebiyle kaydedilen sağlık verilerinin bu amaca hizmet ettiği dikkate alındığında bahse konu şikâyetler ile ilgili olarak Kanun kapsamında yapılacak bir işlem olmadığına,*

- *İlgili kişilerin kişisel sağlık verilerinin silinmesine ilişkin talepleri hususunda kişisel sağlık verilerinin işlenme şartlarından "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi" şartının ortadan kalkmaması sebebiyle kaydedilen sağlık verilerinin bu amaca hizmet ettiği dikkate alındığında bu verilerin Bakanlık tarafından Kanun'un 6 ncı maddesinin üçüncü fıkrası kapsamında işlendiği ve söz konusu işleme şartlarının ortadan kalkmaması nedeniyle Kanun kapsamında yapılacak bir işlem olmadığına..."*

karar verilmiştir.

### 3.6.4. Kişisel Verilerin İşlenmesine İtiraz Hakkı

İlgili kişilerin itiraz hakkı Kanun'un 11'inci maddesinin birinci fıkrasının (g) bendinde *"İlgili kişiler veri sorumlusuna başvurarak işlenen kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkına sahiptir"* şeklinde düzenlenmiştir.

### 3.6.5. Zararın Giderilmesini Talep Etme Hakkı

İlgili kişiler, kişisel verilerinin hukuka aykırı şekilde işlenmesinden kaynaklı bir zararla karşılaşmaları durumunda bu zararın giderilmesini isteme hakkına sahiplerdir. Kanun'un 11'inci maddesinin birinci fıkrasının (ğ) bendi de kişisel verilerin Kanun'a uygun olmayacak şekilde işlenmesi nedeni ile ilgili kişilerin zarar görmesi durumunda zararın giderilmesini isteme hakkına sahip olduğunu düzenlemiştir.

| | |
|---|---|
| ! | **Hatırlatma**<br>Kişisel verilerin hukuka aykırı olarak işlenmesine yönelik tazminat talebinin Kanun'un 14'üncü maddesinin üçüncü fıkrası kapsamında yer alan "*Kişilik hakkı ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.*" hükmü gereğince genel hükümlere göre yargı mercileri nezdinde ileri sürülmesi gerekmektedir. |

### 3.7. Saklama ve İmha Yükümlülükleri

Kişisel verilerin işlendikleri amaç için gerekli süre kadar muhafaza edilmesi ilkesi, kişisel verilerin yalnızca işlenme amaçlarını gerçekleştirmek için gerekli olan süre boyunca saklanabileceğini ve bu sürenin sona ermesiyle birlikte verilerin güvenli bir şekilde imha edilmesi gerektiğini ifade etmektedir. İmha Yönetmeliği uyarınca veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale

getirme işlemi için dayanak yaptıkları politika kişisel veri saklama ve imha politikası olarak adlandırılmaktadır.

Saklama yükümlülüğü, kişisel verilerin hukuka uygun şekilde işlenmesini ve ilgili kişilerin haklarının korunmasını sağlamayı amaçlamaktadır. Kurumlar, hazırladıkları kişisel veri saklama ve imha politikasında saklama sürelerini işleme amacına veya mevzuatta öngörülen sürelere göre belirlemeli, bu süre zarfında kişisel verilerin güvenliğini sağlamaya yönelik teknik ve idari tedbirleri almalı ve saklama sürelerinin sonunda mevzuata uygun ve güvenli bir şekilde imha etmelidir. Bu kapsamda, saklama ve imha sürelerinin her kurumun tabi olduğu mevzuata göre farklılık gösterebileceği dikkate alınmalı; kurumlarca, kendi görev ve yetkilerini düzenleyen mevzuatta öngörülen süreler esas alınarak hareket edilmelidir.

Bazı durumlarda kişisel verinin işleme amacına göre işleme süresi sona ermiş olsa bile mevzuat gereği verilerin belirli bir süre daha saklanması gerekebilir. Örneğin, yasal zorunluluklar veya denetim yükümlülükleri gereği bazı veriler, imha edilmeden önce belirli bir süre daha muhafaza edilebilir. Böyle bir durumda, kişisel veri saklama süresinin yasal zorunluluklara uygun olarak belirlenmesi gerekmektedir.

Kişisel verilerin saklama süreleri sona erdiğinde bu verilerin hukuka ve kurumun kişisel veri saklama ve imha politikalarına uygun olarak imha edilmesi zorunludur. İmha işlemi, kişisel verinin tamamen silinmesi, yok edilmesi veya anonim hâle getirilmesi şeklinde gerçekleştirilebilir.

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Kişisel verilerin anonim hale getirilmesi ise kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekmektedir.

Veri sorumlusu kişisel verinin işleme amacını, ilgili kişinin hak ve çıkarlarını göz önünde bulundurarak en uygun imha yöntemini seçmelidir. İmha sürecinde verilerin kullanılan imha yöntemine göre imha edildiğinin belgelenmesi önem arz etmektedir. Ayrıca, kişisel verilerin hangi yöntemle imha edileceği, imha işlemlerinin sıklığı ve periyodik imha süreleri açıkça belirlenmeli ve kurum içinde kayıt altına alınmalıdır.

Kurumlar, imha sürecinde veri güvenliğini sağlamak amacıyla teknik ve idari tedbirler almalı, imha politikalarını personeline düzenli olarak duyurmalı ve eğitimler ile farkındalık oluşturmalıdır. Bu yaklaşım hem hukuka uygunluğu hem de ilgili kişilerin haklarının korunmasını güçlendirecektir.

Örneğin; Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Kararı[17] ile Devlet memurlarının, memuriyet döneminde haklarında açılmış inceleme-soruşturma dosyalarına ilişkin evrakların imha edilme talebinin veri sorumlusu kamu kurumunca yerine getirilmemesi üzerine Kuruma yapılan başvuru kapsamında; imha edilmesi talep edilen kişisel verilerin, ilgili kişinin devlet memuru olduğu dönemde hakkında açılmış inceleme-soruşturma dosyalarına ilişkin evraklar olması ve bu itibarla söz konusu evrakların, 657 sayılı Kanun gereğince özlük dosyalarında saklanması gerektiği, Kamu Personeli Genel Tebliğine (Seri No: 2) göre görevi herhangi bir şekilde sona eren memurların özlük dosyalarının kurumlarınca saklanacağı ve Devlet Arşiv Hizmetleri Hakkında Yönetmeliğe göre son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyaları içerisinde yer aldığı hususlarından hareketle, 6698 sayılı Kanunun 7'nci maddesinde belirtildiği üzere kişisel verilerin işlenmesini gerektiren sebeplerin de henüz ortadan kalkmaması dolayısıyla şikayetçinin talebinin veri sorumlusu tarafından karşılanmamasının uygun olduğuna karar verilmiştir.

17 Kişisel Verileri Koruma Kurulunun 28/06/2018 tarihli ve 2018/69 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5366/2018-69.

Kurumların kişisel veri saklama ve imha yükümlülükleri kapsamında dikkate alması gereken bir husus da Bilgi Güvenliği ve Yönetim Sistemi Politikalarıdır. Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumların sahip olduğu bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla oluşturulan, risk temelli ve sistematik bir yönetim yapısını ifade eder. BGYS kapsamında kurumlar; kişisel veriler dâhil olmak üzere tüm bilgi varlıklarına ilişkin riskleri belirler, bu risklere karşı teknik ve idari tedbirler uygular, denetim ve izleme faaliyetlerini yürütür ve bilgi güvenliği ihlallerine ilişkin olay inceleme süreçlerini işletir. Kurumların, BGYS politikalarında yer alan kayıtların saklama ve imha süreleri ile kişisel verilerin saklama ve imha süreleri, kurumun tabi olduğu mevzuatta öngörülen saklama yükümlülükleri dikkate alınarak belirlenmeli ve uyumlu olması sağlanmalıdır.

Öte yandan, Devlet Arşiv Hizmetleri Hakkında Yönetmelik ile kamu kurum ve kuruluşlarının iş ve işlemleri sonucunda oluşan belgelerin; düzenlenmesine, gerekli şartlar altında korunmalarının temine, herhangi bir sebepten dolayı kaybının engellenmesine, Devletin, gerçek ve tüzel kişilerin ve bilimin hizmetinde değerlendirilmelerine, kurum ve kuruluşlar ile şahıslar elinde bulunan arşiv belgeleri ve ileride arşiv belgesi haline gelecek arşivlik belgelerin tespit edilmesine, saklanmasına gerek görülmeyen belgelerin ayıklanmasına, imhasına ve arşiv belgelerinin Devlet Arşivleri Başkanlığına devrine ilişkin usul ve esasları düzenlenmektedir. Bu kapsamda kurumlar, ayıklama

ve imha işlemlerini yürütürken Devlet Arşiv Hizmetleri Hakkında Yönetmelik hükümleri ile bu Yönetmelik uyarınca oluşturulan saklama planlarını ve imha kurallarını dikkate alarak hareket etmelidir.

### 3.8. VERBİS'e Kayıt Yükümlülüğü

Kanun'un 16'ncı maddesinin birinci fıkrasında yer alan "*Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.*" ve ikinci fıkrasında yer alan "*Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır.*" hükmüne göre kişisel veri işleyen gerçek ve tüzel kişilerin VERBİS'e kayıt yükümlülüğü bulunmaktadır. Ayrıca, Kanun'un geçici 1'inci maddesinin ikinci fıkrasında yer alan *"Veri sorumluları, Kurul tarafından belirlenen ve ilan edilen süre içinde Veri Sorumluları Siciline kayıt yaptırmak zorundadır.*" hükmü uyarınca Kurulun 11.03.2021 tarihli ve 2021/238 sayılı Kararı[18] gereği kayıt yükümlüsü tüm veri sorumlularının 31.12.2021 tarihine kadar VERBİS'e kayıt ve bildirim yükümlülüğünü yerine getirmesi gerekmektedir.

Bu çerçevede kamu kurumları ile kamu kurumu niteliğindeki meslek kuruluşu veri sorumlularının da 31.12.2021 tarihine kadar VERBİS'e kayıt ve bildirim yükümlülüklerini tamamlamış olmaları beklenmektedir[19].

18 Kişisel Verileri Koruma Kurulunun 11.03.2021 tarihli ve 2021/238 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6905/2021-238.

19 Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Kılavuzu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c7058b41-6d7e-455a-ae96-3ebc8dabe989.pdf. Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/2f2fbcf4-932b-4dad-af8a-cd32e315d815.pdf.

VERBİS'e yapılacak bildirim, veri sorumluları açısından Kanunla düzenlenen bir yükümlülük olup bu kapsamdaki yükümlülüğe uygun davranılmaması durumunda Kanun'un 18'inci maddesinin dördüncü fıkrasında yer verildiği üzere; *"Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir."* hükmü çerçevesinde Kurul tarafından yapılacak inceleme sonrasında idari yaptırım uygulanabilecektir.

Diğer bütün veri sorumlularında olduğu gibi kamu kurumları ile kamu kurumu niteliğindeki meslek kuruluşlarının VERBİS'e yapacakları bildirim işleminden önce kişisel veri işleme envanteri hazırlamaları gerekmekte olup bu kapsamda VERBİS'e açıklanacak bilgiler kişisel veri işleme envanteri ile uyumlu olmalıdır. Benzer şekilde;

- Kanun'un 10'uncu maddesinde veri sorumluları için belirtilen aydınlatma yükümlülüğünde,
- Kanun'un 13'üncü maddesinde belirtilen ilgili kişi başvurularının yanıtlanmasında,
- İlgili kişiler tarafından açıklanacak açık rızanın kapsamının belirlenmesinde,
- Kişisel veri saklama ve imha politikası çerçevesinde kişisel verilerin işlendikleri amaç için gerekli olan azami sürelerin belirlenmesinde

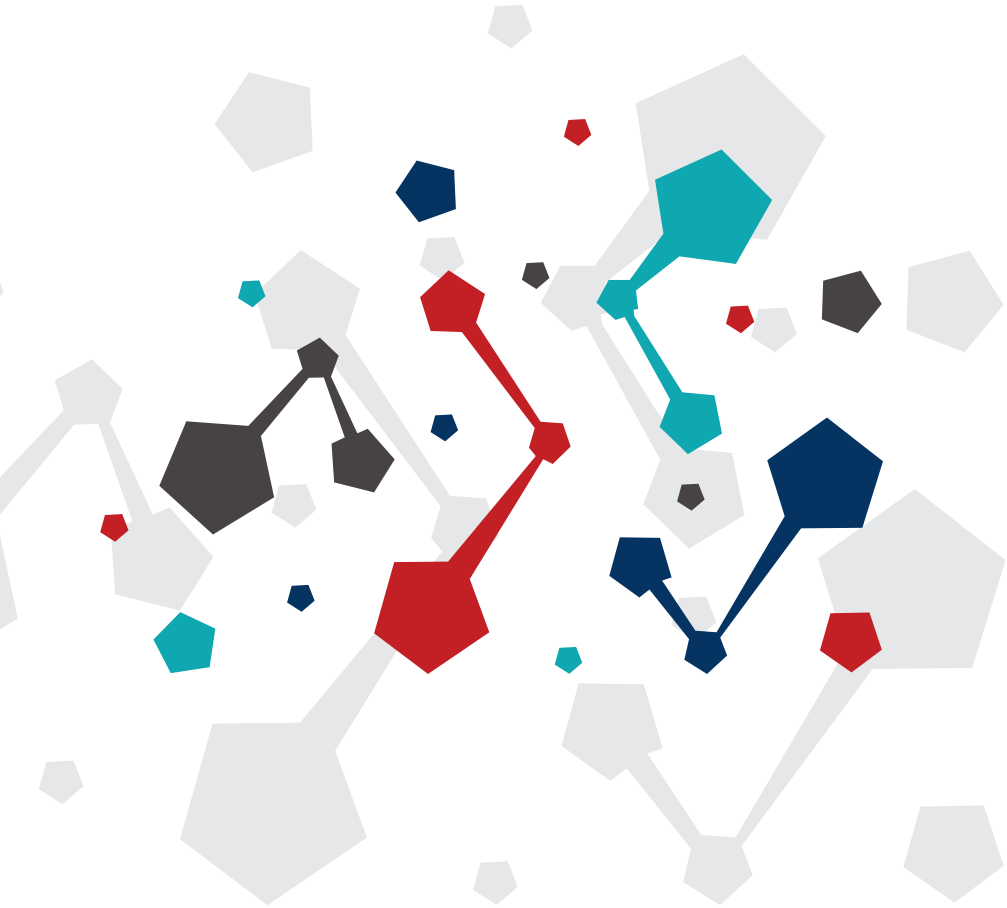
kişisel veri işleme envanterinde yer verilen bilgiler göz önünde bulundurulmalıdır.

!

**Hatırlatma**

Kanun'un geçici maddesi uyarınca Kanun'un yayımı tarihinden itibaren bir yıl içinde, kamu kurum ve kuruluşlarında bu Kanunun uygulanmasıyla ilgili koordinasyonu sağlamak üzere üst düzey bir yönetici belirlenerek Başkanlığa bildirilir.

Kamu kurum ve kuruluşlarında irtibat kişisi ise, koordinasyonu sağlayacak üst düzey yönetici tarafından Kurum ile iletişimi sağlamak amacıyla belirlenerek Sicile kaydı yapılan daire başkanı veya üstü yöneticidir.



# 4. İNCELEME SÜREÇLERİNDE KAMU KURUM VE KURULUŞLARI İLE KAMU KURUMU NİTELİĞİNDEKİ MESLEK KURULUŞLARININ YÜKÜMLÜLÜKLERİ

## 4.1. Veri Sorumlusuna Başvuru Yolunun Tüketilmesi ve İlgili Kişiye Süresinde Cevap Verilmesi

Kanun'un 13'üncü maddesinde, ilgili kişinin veri sorumlusuna başvurusuna ilişkin hususlar düzenleme altına alınmıştır. Buna göre kişisel verisi işlenen ilgili kişiler, Kanun'un 11'inci maddesinde sayılan hakları doğrultusundaki taleplerine ilişkin olarak öncelikle veri sorumlusuna başvuruda bulunmalıdır. Kişisel verisi işlenen ilgili kişilerce haklarını kullanma kapsamındaki taleplerine ilişkin olarak veri sorumlusuna başvurmadan doğrudan Kurula şikâyet yoluna gidilmemesi gerekmektedir.

İlgili kişilerin veri sorumlusuna başvurarak kendisiyle ilgili bilgi talep etmesi halinde, veri sorumlusunca talebe doğru, eksiksiz ve en geç 30 gün içinde olmak kaydı ile en kısa sürede cevap verilmesi gereklidir.

Talebi alan veri sorumlusunun talebi en kısa sürede ve en geç 30 gün içinde inceleyerek kabul etmesi ve gerekli işlemi gerçekleştirerek ilgili kişiye cevap vermesi veya gerekçesini açıklayarak reddetmesi öngörülmektedir. Veri sorumlusu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirebilecektir.

Kendisine başvuru yapılan veri sorumlusunun, kamu kurum ya da kuruluşu olması üzerinde özellikle durulması gerekmektedir. Zira kamu kurum ve kuruluşlarının yapacağı bildirimler 7201 sayılı Tebligat Kanunu ile düzenlenmektedir. Tebligat Kanunu'nun da elektronik tebligata imkân verdiği göz önüne alındığında, kamu kurum ve kuruluşu olan veri sorumlularının da ilgili mevzuata uygun bir şekilde hem yazılı hem elektronik ortamda bildirimde bulunabilmeleri mümkündür.

!

**Hatırlatma**

Kendisine Kanun'un 11'inci maddesi kapsamında başvuru yapılan veri sorumluları, başvuru yapan ilgili kişiye ait herhangi bir kişisel veriyi işlemiyor olsa dahi bu kapsamda ilgili kişiye kişisel verilerinin işlenmediğine yönelik bir cevap vermek zorundadır.

Diğer taraftan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının bünyesinde bulunan bilgi ve belgelerin paylaşılması hususunda[20] meri hukukta çeşitli özel düzenlemeler bulunmaktadır.

Bu noktada belirtmek gerekir ki; Türk Hukukunda ilk olarak, 2004'te yürürlüğe giren 4982 sayılı Bilgi Edinme Hakkı Kanunu ile düzenlenen "*bilgi edinme hakkı*", bireylerin kamu kurum ve kuruluşlarının görevlerinden dolayı sahip oldukları bilgilere erişim hakkı olup bilgi edinme başvuruları, başvurulan kurum ve kuruluşların, ellerinde bulunan veya görevleri gereği bulunması gereken bilgi veya belgelere ilişkin olmalıdır[21]. Öte yandan, 6698 sayılı Kanun ile düzenlenen "*bilgi talep etme hakkı*" ise Kanun'un 11'inci maddesi kapsamında ilgili kişilerin, veri sorumlularından kendileri ile ilgili; kişisel verilerin işlenip işlenmediğini ve işleniyor ise hangi amaçlar için işlendiğini öğrenme hakkını ifade etmektedir.

İlgili kişilere bilgi verilmesi gerekliliği Kanun'un, Aydınlatma Yükümlülüğü" başlıklı 10 uncu maddesinde veri sorumluları bakımından bir yükümlülük olarak düzenlenmiştir. Bahsi geçen madde, ilgili kişilerin haklarını kullanabilmesi ve şeffaflığın sağlanabilmesi amacına hizmet etmekte ve dürüstlük kuralının da bir sonucu olarak kabul görmektedir.

20 Access to Official Documents Guide, https://rm.coe.int/access-to-official-documents-guide/168069660c , s. 16.

21 Bilgi Edinme Değerlendirme Kurulu, 25 Soruda Bilgi Edinme Hakkı, https://bedk.adalet.gov.tr/Resimler/SayfaDokuman/233202015214925_SORUDA_BILGI_EDINME_HAKKI.pdf.

Bu kapsamda ilgili kişilerin veri sorumlusu olan kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde yer alan kişisel verilerine erişim taleplerine ilişkin olarak iç hukukta yer alan düzenlemeler göz önünde bulundurularak hukuka uygun olarak değerlendirme yapılması ve üçüncü kişilerin kişisel verilerinin de korunmasına dikkat edilmesi gerekmektedir. Bu çerçevede veri sorumluları tarafından ilgili kişilerin kişisel verilerine erişim talebi yerine getirilirken üçüncü kişilerin kişisel verilerinin korunması gerektiğine ilişkin örnek minvalinde Kurul kararlarına aşağıda yer verilmektedir:

Kurulun 29.09.2020 tarihli ve 2020/746 sayılı Kararı[22] ile; *"...Kanun'un 11 inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü kapsamında ilgili kişinin, kendisiyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme hakkının, söz konusu veriye erişim hakkını da kapsadığına ve erişim hakkının, bilgi talep etme hakkını tamamlayarak ilgili kişinin, kişisel verileri üzerindeki haklarını kullanabilmesi için, kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığı dikkate alındığında söz konusu dökümün, ilgili kişi dışında başkalarının kişisel verileri varsa bunlar çıkarılmak veya maskelenmek gibi önlemler alınarak ilgili kişiye gönderilmesi yönünde veri sorumlusunun talimatlandırılmasına..."* karar verilmiştir.

22 Kişisel Verileri Koruma Kurulunun 29.09.2020 tarihli ve 2020/746 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6954/2020-746.

Kurulun 15.06.2023 tarihli ve 2023/1050 sayılı Kararı[23] ile;
*"...5411 sayılı Bankacılık Kanunu ve ilgili mevzuatta yer verilen "sır saklama yükümlülüğü"nün, kanuni düzenlemelerin öngördüğü hukuka uygunluk hâlleri dışında, müşteri ile ilgili ticari bağlantı nedeniyle elde edilmiş olan bilgi ve olaylar hakkında üçüncü kişilere bilgi verilmemesini gerektirdiği ve diğer yandan 6698 sayılı Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (b) bendi hükmü kapsamında ilgili kişilerin, kendileriyle ilgili kişisel veriler işlenmişse buna ilişkin bilgi talep etme haklarının, söz konusu veriye erişim hakkını da kapsadığı ve erişim hakkının da bilgi talep etme hakkını tamamlayarak ilgili kişilerin kişisel verileri üzerindeki haklarını kullanabilmeleri için kişisel verilerinin ne şekilde işlendiğine dair bilgi sahibi olmalarına imkân sağladığı dikkate alındığında, tarafların görüşme sırasındaki doğrudan ifadelerini içeren söz konusu dökümün, ilgili kişi dışında başkalarının kişisel verileri varsa bunların çıkarılması/maskelenmesi gibi önlemler alınarak ilgili kişiye gönderilmesi ve buna ilişkin tesis edilen işlemler hakkında Kurula bilgi verilmesi yönünde Veri Sorumlusunun talimatlandırılmasına..."*
karar verilmiştir.

23 Kişisel Verileri Koruma Kurulu'nun 15.06.2023 tarihli ve 2023/1050 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7769/2023-1050.

### 4.2. İlgili Kişilerin Haklarına İlişkin Talepleri Konusunda Kurula Şikâyet Hakkını Kullanması ve İnceleme Sürecinde Bilgi ve Belge Talebine İlişkin Olarak Süresinde Kurula Cevap Verilmesi

Kanun'un 14'üncü maddesi gereğince 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.[24]

Kanun'un 15'inci maddesinin ikinci fıkrası uyarınca, 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'un 6'ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmamakla birlikte Kurulun bu kapsamda yayımlamış olduğu çeşitli dokümanlar da dikkate alınmalıdır[25].

İlgili kişilerin şikâyetinin ya da ihbar başvurusunun kabul edilmesi sonucunda, Kanun'un 15'inci maddesinin birinci fıkrası uyarınca Kurulun, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda re'sen, görev alanına giren konularda gerekli incelemeyi yapma yetkisi bulunmasından bahisle inceleme süreci yürütülecektir.

24 Ayrıntılı bilgi için bkz. Kişisel Verileri Koruma Kurulunun Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin 24.01.2019 tarih ve 2019/9 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu.

25 Kurula İletilen Şikâyet ve İhbarlarda Sık Yapılan Hatalar,https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7de6abf3-ea1c-4bc2-98f5-3ab90b4f5ddb.pdf.

İnceleme süreci kapsamında, Kanun'un 15'inci maddesinin üçüncü fıkrasında da belirtildiği üzere Kurul, kendisine gelen talepleri incelerken veri sorumlularından gerekli tüm bilgi ve belgeleri talep edebilme yetkisine sahiptir. Bu kapsamda veri sorumlularının, yerinde inceleme yapılmasına imkân sağlama ve talep edilen bilgiler ile belgeleri 15 gün içerisinde Kurula göndermeleri gerekmektedir. Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır.

| | |
|---|---|
| ! | **Hatırlatma**<br>Bu noktada, önemle belirtmek gerekir ki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının Kurul tarafından talep edilen bilgi ve belgeleri süresinde göndermesi inceleme sürecinin sağlıklı yürütülebilmesi için önem arz etmektedir. |

### 4.3. İnceleme Süreci Neticesinde Verilen Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü

Kanun'un 15 inci maddesinin beşinci fıkrası uyarınca şikâyet üzerine veya re'sen yapılan inceleme sonucunda ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek bu kararı ilgililere tebliğ eder.

**Hatırlatma**

Veri sorumlusu, Kurul kararını, kararın tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirmek **zorundadır**.

Örneğin; veri sorumlusu kamu kurumu tarafından, ilgili kişinin kişisel verilerinin işlenmesinin Kanun'un 5'inci maddesinde sayılan işleme şartlarından birine dayanmaksızın gerçekleştirilmesinden bahisle, ilgili kişinin kişisel verilerinin Kanun'un 7'nci maddesi ve İmha Yönetmeliği'ne uygun olarak imha edilmesi ve sonucundan Kurula bilgi verilmesi hususunda talimatlandırılmasına karar verilerek ilgili Kurul kararının veri sorumlusu kamu kurumuna tebliğ edilmesi üzerine söz konusu kişisel verilerin imha edildiğini gösterir log kaydı, imha tutanağı gibi belgelerin 30 gün içinde Kurula iletilmesi gerekecektir.

Bu kapsamda, Kanun'un 18'inci maddesinin dördüncü fıkrası uyarınca, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde hukuka aykırılık tespit edilmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacağı ve sonucunun Kurula bildirileceği düzenlenmiştir.

!

**Hatırlatma**

Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları tarafından Kurul Kararı sonucu Kanun'un 18'inci maddesinin dördüncü fıkrası uyarınca disiplin hükümlerine göre işlem tesis edilirken yalnızca o işlemi yapan ilgili personel değil veri güvenliğine ilişkin teknik ve idari tedbirleri almaktan sorumlu kişi/kişiler de **dikkate alınmalıdır.**

Söz konusu veri güvenliğine ilişkin teknik ve idari tedbirleri almaktan sorumlu kişi/kişiler tespit edilirken, Kurum bünyesinde oluşturulan Sorumluluk Yetki Matrisi ve Erişim Yetki Matrisi esas alınarak; ihlalin teknik bir eksiklikten mi yoksa idari bir süreç hatasından mı kaynaklandığı da göz önünde bulundurulmalıdır.

Veri güvenliğine ilişkin teknik ve idari tedbirleri[26] almaktan sorumlu kişi/kişiler kişisel verilerin korunmasına ilişkin eğitim ve farkındalık faaliyetlerinin yürütülmesi, gizlilik taahhütnameleri hazırlanması, kişisel veri güvenliğine ilişkin politika ve prosedürlerin oluşturulması gibi hususlarda görevli ve yetkili kişilerdir.

26 Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler).

Örneğin, ilgili kişinin kişisel verilerinin hukuka aykırı paylaşılmasından bahisle Kanun'un 12'nci maddesinin birinci fıkrasına aykırı şekilde gerekli teknik ve idari tedbirleri almayan veri sorumlusu sıfatını haiz kamu kurumu tarafından Kanun'un 18' inci maddesinin dördüncü fıkrası kapsamında sorumlular hakkında işlem tesis edilerek sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına karar verilmesi durumunda, veri sorumlusu kamu kurumu tarafından **yalnızca** ihlale konu fiili gerçekleştiren personel hakkında disiplin hükümlerine göre işlem tesis edilmesi Kurul kararının gereğinin yerine getirilmesi anlamına gelmeyecektir. Zira, Kanun'un 18'inci maddesinin dördüncü fıkrası kapsamında ihlalin önlenmesine yönelik olarak veri güvenliğine ilişkin teknik ve idari tedbirleri almaktan sorumlu kişi/kişiler hakkında disiplin hükümlerine göre işlem tesis edilmesi gerekmekte olup veri sorumlusu kamu kurumu tarafından Kanun'un 18'inci maddesinin dördüncü fıkrası kapsamında ihlalin önlenmesine yönelik olarak ***veri güvenliğine ilişkin teknik ve idari tedbirleri almaktan sorumlu kişi/kişiler hakkında*** disiplin hükümlerine göre işlem tesis edilmeli ve sonucundan Kurula bilgi verilmelidir.

Kanun'un 15'inci maddesinin altıncı fıkrası uyarınca, Kurulun yapacağı inceleme sonucunda ayrıca ilke kararı alabilme yetkisi de bulunmaktadır. İlke kararları, inceleme konusu ihlalin yaygın olduğunun tespiti halinde alınmakta ve yayımlanmaktadır. İlke kararları, Kurulun karar konusu olaya yaklaşımını ve sonraki inceleme ve şikâyetlerdeki

tutumunu göstereceği için tüm ilgililer açısından uyulması son derece önemli hukuki metinlerdir. Ayrıca ilke kararları kişisel verilerin korunmasına ilişkin mevzuatın uygulamasının yeknesaklaştırılması açısından da önem arz etmektedir. Zira ilke kararları sayesinde mevzuata ilişkin farklı yorumlar ve bunlardan doğacak farklı uygulamaların önüne geçilebilecektir[27].

| | |
|---|---|
| ! | **Hatırlatma**<br>2577 sayılı İdari Yargılama Usulü Kanunu'nun 12'nci maddesi ile 7'nci maddesinin (1) ve (2) numaralı fıkraları gereği, Kurul Kararlarına karşı yazılı bildirimin yapıldığı tarihi izleyen günden itibaren altmış gün içerisinde idare mahkemelerinde dava açılması mümkün bulunmaktadır. |

27 Kurul tarafından alınan İlke Kararları için bkz. https://www.kvkk.gov.tr/Icerik/7201/ilke-kararlari.

### İlgili Kişi Başvurusu (M.13)

- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe uygun şekilde veri sorumlusuna başvuru yapılır.

### 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.

### Kurula Şikâyet (M.14)

- 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.

### Kurul

**Kurul inceleme kararı alırsa;**

Veri Sorumlusundan Şikâyete İlişkin bilgi ve belge talep edilir.

### Veri Sorumlusu

- Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri **on beş gün içinde** göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır. **(M.15/3)**

### Kurul Kararı

**İhlalin, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde,** Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir. **(M.18/4)**

### Yargı yolu açık

# 5. KAMU KURUM VE KURULUŞLARI ARASINDA HUKUKA UYGUN VERİ AKTARIMI

Bir kamu kurumundan başka bir kamu kurumuna gerçekleştirilecek olan kişisel veri aktarımının hukuka uygun olup olmadığı hususunda çoğu zaman Kurumumuzdan görüş talep edilmektedir. Örneğin, bir kamu kurumunun belirli bir kamu görevini ifa etmek amacıyla başka bir kamu kurumundan kişisel veri talep etmesi ancak bu talebin hukuki dayanağının veriyi aktaracak kurum tarafından tespit edilememesi ya da tespit edilse dahi ilgili düzenlemenin söz konusu aktarımı açıkça mümkün kılıp kılmadığı hususunda değerlendirmeye ihtiyaç duyulması gibi durumlarla karşılaşılmaktadır. Ayrıca kişisel veri aktarım talebi reddedilen kamu kurumlarının, bu ret sebebiyle görevlerini ifa edememeleri halinde de Kurumumuzdan görüş talep edilmektedir.

Bu başlık altında, kişisel veri aktarımı talebinde bulunan kamu kurum ve kuruluşları ile kendisinden kişisel veri aktarılması talep edilen kamu kurum ve kuruluşlarının özellikle dikkat etmeleri gereken hususlara yer verilmiştir. Kamu kurum ve kuruluşlarının söz konusu yönergeleri dikkatle incelemeleri yapılacak aktarımın hukuki dayanağının doğru şekilde tespit edilebilmesi bakımından büyük önem arz etmektedir.

!

**Hatırlatma**

Muhteviyatına veya güncelliğine göre gizlilik dereceli belgeler için uygulanacak usul ve esasları belirlemek ve kamu kurum ve kuruluşlarını kapsayacak şekilde gizlilik dereceli belgelerde uygulama birliğini sağlamak amacı ile hazırlanan 13.05.1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar"ın yerine 25.04.2022 tarihli ve 5529 sayılı Cumhurbaşkanı Kararıyla "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik[28]" dikkate alınmalıdır.

### 5.1. Aktarım Bakımından Özel Nitelikli Hukuki Düzenlemelerin Tespiti

Kamu kurumları tarafından kişisel verilerin hukuka uygun olarak aktarılabilmesi için aktarımın hukuki sebebini teşkil edecek bir mevzuat hükmüne dayandırılması gerekmektedir. Kişisel verilerin yurt içinde aktarılması bakımından ilk olarak göz önünde bulundurulması gereken düzenleme Kanun'un 8'inci maddesi olup söz konusu madde;

*"... (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.*

*(2) Kişisel veriler;*

*a) 5 inci maddenin ikinci fıkrasında,*

28 Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik, RG, 26.04.2022, S.31821.

*b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.*

*(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır ...”*

hükmünü amirdir. Anılan maddenin üçüncü fıkrasında, kişisel verilerin yurt içinde aktarılmasına ilişkin olarak diğer kanunlarda yer alan hükümlerin saklı tutulmuş olması nedeniyle, kamu kurum ve kuruluşlarının öncelikle görev alanlarını ilgilendiren mevzuat hükümlerini incelemeleri, bu hükümleri benimsemeleri ve söz konusu hükümlerden hangilerinin veri aktarımına dayanak teşkil edebileceğini değerlendirmeleri gerekmektedir.

Örneğin, Kanun'un 8'inci maddesinin üçüncü fıkrasının atfıyla 213 sayılı Vergi Usul Kanunu'nun "Defter ve Belgelerle Diğer Kayıtların İbraz Mecburiyeti" başlıklı 256'ncı maddesinde yer alan; *"Geçen maddelerde yazılı gerçek ve tüzel kişiler ile mükerrer 257'nci madde ile getirilen zorunluluklara tabi olanlar, muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin mikro fiş, mikro film, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri muhafaza süresi içerisinde yetkili makam ve memurların talebi üzerine ibraz ve inceleme için arz etmek zorundadırlar."* hükmü uyarınca içinde kişisel veri ve özel nitelikli kişisel veriler ihtiva edebilecek dokümanların Vergi Denetim Kurulu Başkanlığına denetimin kapsamının gerektirdiği ölçüde ve denetim amacıyla sınırlı kalmak üzere aktarılabileceği belirtilebilir.

Kişisel verilerin yurt dışına aktarılması bakımından ise öncelikle Kanun'un 9'uncu maddesinin onuncu fıkrasının dikkate alınması zorunludur. Nitekim anılan fıkrada kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu ifade edilmektedir.

Örneğin, 6458 sayılı Kanun'un "Uluslararası koruma süreçlerinde iş birliği" kenar başlıklı 92'nci maddesinde Göç İdaresi Başkanlığı ile Birleşmiş Milletler Mülteciler Yüksek Komiserliği (UNHCR) arasında uluslararası koruma başvurusunda bulunmuş kişilerin kişisel verilerinin aktarılmasına yönelik özel hüküm bulunmaktadır. Dolayısıyla Göç İdaresi Başkanlığının UNHCR ile bu minvalde yapacağı kişisel veri aktarımları bakımından 6458 sayılı Kanun'un 92'nci maddesi uygulama alanı bulacaktır.[29]

29 Uluslararası Sözleşme Niteliğinde Olmayan Anlaşma ile Yurt Dışına Kişisel Veri Aktarımına İzin Verilmesi Hakkında Duyuru'da da yer aldığı üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9 uncu maddesinin dördüncü fıkrasının (a) bendi kapsamında; İçişleri Bakanlığı Göç İdaresi Başkanlığı ile Birleşmiş Milletler Mülteciler Yüksek Komiserliği arasında kişisel verilerin yurt dışına aktarılmasına dayanak teşkil edecek "uluslararası sözleşme niteliğinde olmayan anlaşma", Kişisel Verileri Koruma Kurulu tarafından Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 11 inci maddesi kapsamında değerlendirilmiş olup söz konusu aktarıma 21.10.2025 tarihinde izin verilmiştir. Detaylı bilgi için bkz. 10 Kasım 2025 tarihli Uluslararası Sözleşme Niteliğinde Olmayan Anlaşma ile Yurt Dışına Kişisel Veri Aktarımına İzin Verilmesi Hakkında Duyuru, https://www.kvkk.gov.tr/Icerik/8538/uluslararasi-sozlesme-niteliginde-olmayan-anlasma-ile-yurt-disina-kisisel-veri-aktarimina-izin-verilmesi-hakkinda-duyuru.

Örneğin, özel hukuk hükümlerine tâbi bankalarda olduğu gibi kamu bankaları tarafından yurt dışına yapılacak kişisel veri aktarımının 5411 sayılı Bankacılık Kanunu'nun (5411 sayılı Kanun) 73'üncü maddesinin (4) numaralı fıkrasında belirtilen sınırlar dâhilinde bulunup bulunmadığı hususunun tespit edilmesi gerektiği, şayet aktarılacak verilerin bu kapsam dışında kaldığı değerlendirilmekte ise yapılacak kişisel veri aktarımına ilişkin uygun prosedürün Banka tarafından Kanun'un 9'uncu maddesi hükümleri arasından seçilmesi suretiyle aktarımın gerçekleştirilmesi gerektiği göz önüne alınmalıdır.

İfade edilmelidir ki aktarıma esas özel düzenlemeler, uluslararası niteliği haiz anlaşmalar çerçevesinde de yer alabilmektedir. Bu bakımdan usulüne uygun yürürlüğe konulmuş milletlerarası anlaşmaların da Anayasa'nın 90'ıncı maddesinin beşinci fıkrası uyarınca kanun hükmünde olduğu unutulmamalıdır.

Örneğin, Posta ve Telgraf Teşkilatı Anonim Şirketinin yurt dışına kişisel veri aktarımı için öncelikle göz önünde bulundurulması gereken düzenleme Evrensel Posta Birliği Konvansiyonu'dur. Aktarım için mevzuat dayanağı olarak öncelikle Konvansiyon hükümlerine bakılmalı, Konvansiyonda hüküm bulunmayan hallerde Kanun hükümlerine göre hareket edilmelidir.

Örneğin, Hazine ve Maliye Bakanlığı, Mali Çerçeve Ortaklık Anlaşmasının 18'inci maddesinin ikinci fıkrası ile AB Dış Yardım Sözleşme Usulleri Uygulama Rehberi eki Özel Koşulların ilgili maddeleri çerçevesinde Kanun'un 9'uncu maddesinin onuncu fıkrasına dayanılarak kişisel veriler, yurt dışına aktarılabilecektir.

Aktarıma esas teşkil edecek düzenleme tespit edildikten sonra aktarımın ayrıntılarının taraflar arasında gerçekleştirilecek bir protokol kapsamında düzenlenmesi mümkündür. Ancak bu protokolün tek başına aktarımın dayanağı olamayacağı hususu unutulmamalıdır.

Aktarıma esas teşkil edecek hukuki düzenleme (örneğin bir kanun hükmü, bir hukuki yükümlülük veya Kanun'un 5'inci maddesinin ikinci fıkrasındaki diğer işleme şartlarından biri) belirlendikten sonra, aktarımın kapsamı, amacı, veri kategorileri, teknik ve idari güvenlik tedbirleri ile tarafların sorumluluklarının bir protokol ile ayrıntılandırılması mümkündür. Ancak bu protokol, hukuki sebebin yerine geçmez; yalnızca mevcut hukuki sebebin uygulanma usulünü düzenler. Dolayısıyla kamu kurumları arasında kişisel veri aktarımına ilişkin imzalanan bir protokol halihazırda hukuka uygunluğu tespit edilmiş kişisel veri aktarımının ne şekilde gerçekleştirileceği ve aktarımın sınırlarına ilişkin yol gösterici bir doküman olabilecektir.

## 5.2. Aktarıma İlişkin Özel Düzenleme Bulunmaması Durumunda Aktarımın Hukuki Dayanağı

### 5.2.1. Yurt İçinde Aktarım

Yurt içinde yapılacak aktarımlar bakımından Kanun'un 8'inci maddesinin üçüncü fıkrasının atfı sebebiyle kamu kurumlarının görev alanına giren hususlara ilişkin özel düzenlemelerin incelenmesi neticesinde aktarıma esas teşkil edecek (aktarıma cevaz veren) veya aktarımı yasaklayan bir hüküm bulunmaması durumunda Kanun'un 8'inci maddesinin ikinci fıkrası uyarınca Kanun'un 5'inci; özel nitelikli kişisel veriler için ise 6'ncı maddesinde yer alan işleme şartlarından en az birine dayanılmak suretiyle kişisel veri aktarılması mümkündür.

Aktarıma konu kişisel verilerin özel nitelikli kişisel veri olması yahut aktarım kapsamındaki kişisel veriler arasında özel nitelikli kişisel verilerin bulunması durumunda ise aktarım faaliyetinin Kanun'un 6'ncı maddesi kapsamında gerçekleştirilmesi gerekmektedir.

Diğer taraftan özel nitelikli kişisel veri niteliğini haiz verilerin işlenmesinde Kurulun 31.01.2018 tarihli ve 2018/10 sayılı Kararı[30] ile belirlenen "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"in alınması gerekmektedir.

30 Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı.

### 5.2.2. Yurt Dışına Aktarım

Yurt dışına yapılacak aktarımlar bakımından Kanun'un 9'uncu maddesinin onuncu fıkrasının atfı sebebiyle kamu kurumlarının görev alanına giren hususlara ilişkin özel düzenlemelerin veya uluslararası anlaşmaların incelenmesi neticesinde aktarıma esas teşkil edecek (aktarıma cevaz veren) veya aktarımı yasaklayan bir hüküm bulunmaması durumunda kişisel veriler, Kanun'un 9'uncu maddesinin birinci fıkrası uyarınca Kanun'un 5'inci; özel nitelikli kişisel veriler için ise 6'ncı maddesinde yer alan işleme şartlarından birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir. Halihazırda hakkında yeterlilik kararı verilmiş bir ülke, ülke içerisindeki sektör veya uluslararası kuruluş bulunmamaktadır. Nitekim yeterlilik kararı, Kurul tarafından alınmakla birlikte Kurul tarafından yeterli koruma bulunup bulunmadığına ilişkin yapılacak değerlendirmenin; çeşitli ve birbirinden oldukça farklı ulusal hukuk düzenlerinin varlığı, değerlendirmeye konu ülkede genel niteliğe sahip bir veri koruma düzenlemesinin bulunmaması veya yalnızca belirli alanları kapsayan düzenlemelerin bulunması ve federal devletlerde eyaletler arasındaki farklılıklar göz önünde bulundurulduğunda titizlikle yürütülmesi gereken yoğun ve uzun bir süreçtir.

Bu sebeple kişisel verilerin yurt dışına aktarılması bakımından ikinci kademe olan Kanun'un 9'uncu maddesinin dördüncü fıkrasında yer

alan uygun güvencelerden birinin sağlanması gerekmektedir. Kanun'un 9'uncu maddesinin dördüncü fıkrası uyarınca; yeterlilik kararının bulunmaması durumunda kişisel veriler, Kanun'un 5'inci ve 6'ncı maddelerinde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, anılan fıkrada tahdidi olarak sayılan uygun güvencelerden birinin sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir. Bu uygun güvencelerden biri ise *"yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi"*dir.

Söz konusu uygun güvence Aktarım Yönetmeliğinin 11'inci maddesinde düzenlenmiştir. Söz konusu düzenleme;

*"(1) Uluslararası sözleşme niteliğinde olmayan anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümler vasıtasıyla, Türkiye'deki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları ve yabancı ülkedeki kamu kurum ve kuruluşları veya uluslararası kuruluşlar arasında yapılacak kişisel veri aktarımları bakımından uygun güvence sağlanabilir. Anlaşma, kişisel veri aktarımının tarafları arasında akdedilir.*

*(2) Anlaşmanın müzakere sürecinde Kurulun görüşüne başvurulur.*

*(3) Anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümler özellikle aşağıdaki hususları içerir:*

*a) Kişisel veri aktarımının amacı, kapsamı, niteliği ve hukuki sebebi.*
*b) Kanun ve ilgili mevzuata uygun olarak temel kavramlara ilişkin tanımlar.*
*c) Kanunun 4 üncü maddesinde belirtilen genel ilkelere uyum sağlanacağına yönelik taahhüt.*
*ç) İlgili kişilerin anlaşma ve anlaşma kapsamında yapılacak kişisel veri aktarımı hakkında aydınlatılmasına ilişkin usul ve esaslar.*
*d) Kişisel verileri aktarılan ilgili kişilerin Kanunun 11 inci maddesinde belirtilen haklarının kullandırılmasına yönelik taahhüt ve bu hakların kullanımı amacıyla yapılacak başvuruya ilişkin usul ve esaslar.*
*e) Uygun veri güvenliği düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınacağına yönelik taahhüt.*
*f) Özel nitelikli kişisel verilerin aktarılması hâlinde Kurul tarafından belirlenen yeterli önlemlerin alınacağına yönelik taahhüt.*
*g) Kişisel verilerin sonraki aktarımına yönelik kısıtlamalar.*
*ğ) Anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümlerin ihlali hâlinde ilgili kişinin başvurabileceği hak arama yöntemleri.*
*h) Anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümlerin uygulanmasına ilişkin denetim mekanizması.*

*ı) Veri alıcısının, anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümlere uygunluk sağlayamaması hâlinde veri aktaranın veri aktarımını askıya alma ve anlaşmayı feshetme hakkına sahip olacağına yönelik düzenleme.*

*i) Veri alıcısının anlaşmanın feshedilmesi veya yürürlük süresinin sona ermesi hâlinde, veri aktaranın tercihine bağlı olarak, aktarıma konu kişisel verileri yedekleri ile birlikte veri aktarana geri göndereceğine ya da kişisel verileri tamamen yok edeceğine yönelik taahhüt.*

*(4) Anlaşmaya dayanılarak kişisel verilerin yurt dışına aktarılabilmesi için veri aktaran tarafından Kurula izin başvurusunda bulunulur. Yapılacak başvuru kapsamında anlaşma metninin nihai hâli ve Kurul tarafından yapılacak değerlendirme için gerekli diğer bilgi ve belgeler Kurula sunulur. Kişisel veri aktarımına, Kurul tarafından izin verilmesinden sonra başlanır."*

hükmünü amirdir.

Buna göre uluslararası sözleşme niteliğinde olmayan anlaşmada yer verilecek kişisel verilerin korunmasına yönelik hükümler vasıtasıyla Türkiye'deki kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları ve yabancı ülkedeki kamu kurum ve kuruluşları veya uluslararası kuruluşlar arasında yapılacak kişisel veri aktarımları bakımından uygun güvence sağlanabilecektir. Bu bağlamda ülkemizdeki bir kamu kurumunun yabancı ülkedeki ilgili kamu kurumuyla belirli bir alanda yapacağı iş birliği protokolü çerçevesinde Kurulun

izin vermesi koşuluyla bu iş birliği kapsamındaki faaliyetlerin gerektirdiği kişisel verilerin yurt dışındaki kamu kurumuna aktarılması mümkün hale gelecektir.

### 5.3. Aktarımda Ölçülülük

Kanun'un 4'üncü maddesinin birinci fıkrasının (ç) bendinde, kişisel verilerin *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü"* olması gerektiği hüküm altına alınmıştır. Söz konusu ilke çerçevesinde kamu kurum ve kuruluşlarının, görev ve yetki sınırları dışında, amaçla doğrudan ilgili olmayan hiçbir kişisel veriyi işlememesi veya başka kurumlara aktarmaması gerekmektedir. Bu kapsamda kişisel veri aktarımında veri minimizasyonu ilkesine azami ölçüde dikkat edilmesi ve hangi verinin hangi gerekçeyle istendiği veya aktarıldığının net biçimde ortaya konulması büyük önem arz etmektedir. Özellikle ileride doğması muhtemel ihtiyaçlar veya genel amaçlı talepler doğrultusunda veri aktarımında bulunulmamalı; veriler, yalnızca somut, güncel ve mevzuata uygun bir amaç doğrultusunda, bu amaca ulaşmayı sağlayacak derecede asgari ölçüde işlenmeli ve aktarılmalıdır. Nitekim Kurulun *"İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması"* konulu kararında[31] da veri sorumlusu tarafından gereğinden fazla kişisel veri aktarımında bulunulmasının, Kanun'un 5'inci maddesinin ikinci fıkrasının (ç) bendindeki *"hukuki*

31 Kişisel Verileri Koruma Kurulunun İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık) Konulu Kararı, https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-.

*yükümlülüğün yerine getirilmesi için zorunlu olması"* şartı kapsamında değerlendirilemeyeceği, bu durumun Kanun'un 4'üncü maddesinde belirtilen *"amaçla bağlantılı, sınırlı ve ölçülü işleme"* ilkesine açıkça aykırılık teşkil ettiği belirtilmiştir.

Ölçülülük ilkesi kişisel verilerin korunması hakkı ile diğer temel hak ve özgürlükler arasında makul bir denge kurulmasını da gerektirmektedir. Anayasa ile güvence altına alınan temel hak ve özgürlükler arasında bir çatışma yaşanması durumunda, kamu otoriteleri tarafından yapılacak değerlendirmelerde bu dengenin sağlanması anayasal bir zorunluluktur.

Örneğin, adil yargılanma hakkı kapsamında savunma hakkının kullanılması amacıyla bir kişinin sağlık verilerinin mahkemeye sunulması gerektiğinde yalnızca davaya konu olguyu açıklamaya hizmet eden asgari düzeydeki veriler aktarılmalı, kişinin tüm tıbbi geçmişine ilişkin verilerin aktarımı gibi geniş kapsamlı uygulamalardan kaçınılmalıdır.

Bir üniversite hastanesi tarafından ilgili kişinin sağlık verilerinin idari bir davaya esas teşkil etmek üzere talebine binaen davalı kamu kurumuna aktarılmasına ilişkin olarak Kurulun 04.08.2022 tarihli ve 2022/790 sayılı Kararı[32] ile;

*"...Kanun'un 8'inci maddesinin (2) numaralı fıkrasının (b) bendinde belirtilen özel nitelikli kişisel verilerin aktarılmasına ilişkin Kanun'un 6'ncı maddesinde yer alan şartlar ya da Kanun'un 8'inci maddesinin (1) numaralı fıkrasında belirtildiği üzere ilgili kişinin açık rızası mevcut olmadığı halde ilgili kişiye ilişkin özel nitelikli kişisel veri olan sağlık verilerinin Kanun'a aykırı olarak kamu kurumuna aktarıldığı, öte yandan talep edilen bilgiden daha geniş kapsamda bilgi paylaşıldığı dikkate alındığında veri sorumlusu üniversite hastanesinin Kanun'un 12'nci maddesinin (1) numaralı fıkrasına göre kişisel verilerin güvenliğine ilişkin gerekli her türlü teknik ve idari tedbiri alma yükümlülüğünü yerine getirmediği değerlendirildiğinden sorumlular hakkında Kanun'un 18'inci maddesinin (3) numaralı fıkrası çerçevesinde disiplin hükümlerine göre işlem yapılmasına ve yapılan işlem hakkında Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,*

32 Kişisel Verileri Koruma Kurulunun 04.08.2022 tarihli ve 2022/790 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7574/2022-790.

*İlgili kişinin Kanun'un 11'inci maddesinin (1) numaralı fıkrasının (d) bendi kapsamında "Anamnez Formu"nda geçen "esrar maddesi kullanıldığına ilişkin verilerin" düzeltilmesini talep etme hakkı dikkate alındığında; Kanun'un 4'üncü maddesinin (2) numaralı fıkrasının (b) bendinde yer aldığı üzere "doğru ve gerektiğinde güncel olma" ilkesine uygun olarak Kişisel Sağlık Verileri Hakkında Yönetmelik'in 13'üncü maddesi kapsamında, veri sorumlusu tarafından gerek kendi bünyesinde ve gerektiği takdirde ilgili kişiyi de yönlendirmek suretiyle İl Sağlık Müdürlüğü nezdinde gerekli işlemlerin yapılması ve sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,*

*Şikâyete konu edilen verilerin aktarıldığı kamu kurumu nezdinde de bu verilerin imha edilmesinin sağlanması hususunda gerekli işlemlerin tesis edilmesine ve yapılan işlemin sonucundan Kurula bilgi verilmesi hususunda veri sorumlusunun talimatlandırılmasına,*

*İlgili kişilerin Kanun kapsamındaki taleplerini Kanun'a ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırması gerektiğinin veri sorumlusuna hatırlatılmasına..."*

karar verilmiştir.

Sonuç olarak kamu kurumları arasında veya kamu kurumları ile üçüncü kişiler arasında gerçekleştirilecek kişisel veri aktarımlarında, amacın gerektirdiğinden fazla kişisel veri aktarımından kaçınılması, kişisel veri aktarımının sağlayacağı fayda ile temel hak ve özgürlüklerinin korunması arasındaki dengenin gözetilmesi gerekmektedir. Bu noktada aktarımı talep edilen kişisel verinin niteliği de dikkate alınarak Kurumun internet sayfasında yayımlanmış olan rehberlerin incelenmesi faydalı olacaktır.

### 5.4. Güvenli Aktarım Yöntemleri ve Teknik/İdari Tedbirler

Kamu kurum ve kuruluşları arasında veya kamu kurum ve kuruluşları ile üçüncü kişiler arasında gerçekleştirilen kişisel veri aktarımlarında, aktarımın hukuki dayanağının ve ölçülülüğünün sağlanmasına ek olarak kişisel veri aktarımının güvenli bir şekilde gerçekleştirilmesi de zorunludur. Kanun'un 12'nci maddesinde; veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve verilerin muhafazasını sağlamak amacıyla gerekli her türlü teknik ve idarî tedbiri almakla yükümlü olduğu hüküm altına alınmıştır.

Kişisel verilerin aktarılması aşamasında güvenliğin sağlanabilmesi için öncelikle hangi kişisel verilerin işlendiğinin, bu verilerin hangi yollarla (fiziksel/dijital) aktarılabileceğinin, aktarım sırasında ortaya çıkabilecek güvenlik risklerinin ve bu risklerin gerçekleşmesi durumunda oluşabilecek muhtemel zararların analiz edilmesi ve yapılan analiz doğrultusunda riski en aza indirecek önlemlerin belirlenmesi ve uygulanması gerekmektedir.

Ayrıca kişisel verilerin aktarımında güvenliğin sağlanabilmesi için kişisel verinin niteliğine veya aktarım usulüne uygun yöntemlerin kullanılması büyük önem taşımaktadır. Bu çerçevede;

- Kişisel verilerin e-posta yoluyla aktarılması halinde kişisel verilerin şifrelenmiş biçimde ve tercihen kurumsal e-posta adresi veya KEP hesabı üzerinden aktarılması, (Kişisel verilerin e-posta yoluyla aktarılması halinde mümkün olduğu durumlarda KEP gibi güvenli aktarım protokolleri kullanılarak bu imkânın bulunmaması hâlinde ise kişisel verilerin şifrelenmiş biçimde ve tercihen kurumsal e-posta adresleri üzerinden aktarılması),

- CD, DVD, USB bellek gibi fiziksel taşınabilir cihazlar kullanılarak veri aktarımı yapılması halinde kişisel verilerin kriptografik yöntemlerle şifrelenmesi ve şifre anahtarının ayrı bir ortamda muhafaza edilmesi,
- Farklı fiziksel ortamlarda bulunan sunucular arasında veri aktarımı söz konusu olduğunda ise kişisel verilerin, Virtual Private Network (Sanal Özel Ağ) üzerinden veya sFTP (Güvenli Dosya Transfer Protokolü) gibi protokoller kullanılarak aktarılması,
- Kişisel verilerin kâğıt ortamı yoluyla aktarılması durumunda evrakın çalınması, kaybolması veya yetkisiz kişilerin erişimine açılması gibi risklere karşı gerekli önlemlerin alınması; gerektiğinde evrakların "gizlilik dereceli belgeler" formatında gönderilmesi

önem arz etmektedir. Kamu kurum ve kuruluşları arasında süreklilik arz eden veri paylaşımı süreçlerinde; paylaşılacak kişisel veri türleri, paylaşım süresi, veri güvenliğine ilişkin tarafların yükümlülükleri vb. hususların düzenlendiği veri paylaşım protokollerinin yapılması veri güvenliğine ilişkin risklerin azaltılması noktasında faydalı olabilecektir. Ayrıca özel nitelikli kişisel verilerin aktarılması hâlinde Kurulun 31.01.2018 tarihli ve 2018/10 sayılı *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Alınması Gereken Yeterli Önlemler"* konulu kararında[33] yer alan önlemlere uyulmasının zorunlu olduğu hususunun tekrar hatırlatılmasında fayda görülmektedir.

33 Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı.

Son olarak kişisel verilerin kamu kurumlarınca işlenmesi ve aktarılması süreçlerinde Kurum tarafından yayımlanan *"Kişisel Veri Güvenliği Rehberi*[34]*"*nin dikkate alınması; veri güvenliği yükümlülüklerinin somutlaştırılması ve uygulamada karşılaşılabilecek risklere karşı etkili önlemler alınabilmesi açısından önem arz etmektedir.

### 5.5. Sık Karşılaşılan Durumlar

#### 5.5.1. Aktarım Süreçlerinde Özel Düzenlemelerin Kanun'un 8'inci ve 9'uncu Maddeleriyle Bütüncül Ele Alınmaması

Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının Kanun çerçevesinde yaptığı uygulamalar incelendiğinde, kişisel verilerin aktarılması/paylaşılması bakımından farklı yorumlara dayalı işlemler yapıldığı gözlemlenmektedir. Bu farklılıkların temelinde ise çoğunlukla Kanun'un 4'üncü maddesinde düzenlenen *"hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkelerinin uygulamada yeterince gözetilmemesi, Kanun'un 5'inci ve 6'ncı maddelerinde yer alan kişisel veri işleme şartlarının her somut olay bakımından ayrıntılı şekilde değerlendirilmeden genel ve kategorik bir yaklaşım sergilenmesi ve 8'inci maddesinde öngörülen hükümlerin ilgili özel mevzuat hükümleriyle birlikte bütüncül olarak ele alınmamasından kaynaklanan tereddütler bulunmaktadır. Bu tür durumlarda,

34 Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler).

kurumların ihtiyatlı davranma eğilimleri anlaşılır olmakla birlikte veri işleme ve aktarım süreçlerinde hem Kanun hükümleri hem özel kanunlardaki düzenlemelerin birlikte değerlendirilmesi, uygulamanın hukuka uygunluğunu ve vatandaşların haklarının korunmasını daha güçlü bir şekilde temin edecektir.

Bu doğrultuda öncelikle kurumların/kuruluşların kendi özel mevzuatlarında yer alan kişisel verilerin aktarımına ilişkin hükümleri iyi bilmeleri ve bu düzenlemeleri uygulamaya esas almaları gerekmektedir. Zira aktarımı açıkça öngören bir düzenlemenin bulunması halinde aktarım işlemi kural olarak hukuka uygun kabul edilecektir. Ancak böyle bir özel düzenleme mevcut değilse diğer hukuka uygunluk yollarına başvurulmalıdır. Bu bağlamda:

- Yurt içi aktarım bakımından Kanun'un 8'inci maddesinin ikinci fıkrası,
- Yurt dışına aktarım bakımından ise Kanun'un 9'uncu maddesinin dördüncü fıkrasında düzenlenen uygun güvenceler,

temel dayanak noktalarıdır.

### 5.5.2. Yurt Dışına Aktarım Bakımından Yeterlilik Kararının Nihai Aktarım Yöntemi Olarak Değerlendirilmesi

Çeşitli kamu kurumlarıyla yapılan toplantı ve yazışmalarda Kurumumuza sıklıkla "Hakkında Yeterlilik Kararı Verilmiş Olan Ülkelerin Listesi" sorusu yöneltilmektedir. Ancak yeterlilik kararının alınması, çoğu durumda devletlerarası ilişkileri ilgilendiren ve uzun süreli, karmaşık

bir süreci gerektiren bir konudur. Bu nedenle yurt dışına kişisel veri aktarımında yalnızca yeterlilik kararının beklenmesine dayalı bir yaklaşım yerine, öncelikle aktarıma dayanak teşkil edebilecek kanun ve uluslararası anlaşmaların incelenmesi; böyle bir hukuki dayanak bulunmadığı takdirde ise Kanun'un 9'uncu maddesinin dördüncü fıkrasında öngörülen uygun güvencelerden birine veya şartları bulunması halinde Kanun'un 9'uncu maddesinin altıncı fıkrasında sayılan arızi hallere dayanılarak aktarım yapılması gerekmektedir.

### 5.5.3. Aktarım Hukuka Uygun Olmakla Birlikte Kanun'un 4'üncü Maddesindeki İlkelere Uygun Davranılmaması

Her hâlükârda her tür aktarım işleminde Kanun'un 4'üncü maddesindeki ilkelerin titizlikle gözetilmesi zorunludur. Örneğin, bir kamu kurum/kuruluşuna bir kanun veya uluslararası anlaşma ile aktarım yetkisi tanınmış olsa da aktarımın kapsamına ilişkin ayrıntılı düzenleme bulunmuyorsa, bütün kişisel verilerin gereksiz şekilde paylaşılması hukuka aykırı olacaktır.

### 5.5.4. Aktarım Taleplerinin Sistematik/Kategorik Şekilde Reddedilmesi

Bazı durumlarda, kamu kurumları tarafından Kanun'a uygun şekilde belirli verilerin aktarımı talep edilmesine rağmen, bu taleplerin sistematik veya kategorik biçimde reddedildiği uygulamalara rastlanmaktadır.

Benzer şekilde kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının Kanun gerekçe gösterilmek suretiyle başvuruculara bilgi vermekten imtina ettiği gözlemlenmektedir. Bu gibi durumlarda Kanun gereği bilgi verilemediği yönünde bir cevap verilmesinden önce ilgili kurum veya kuruluşun mevzuatında verinin aktarımını yasaklayan bir hüküm bulunup bulunmadığı araştırılmalı, yasaklayıcı bir hüküm bulunmaması halinde ise aktarıma dayanak teşkil eden kişisel veri işleme şartlarından birinin bulunması halinde başvurucunun talebine olumlu yönde cevap verilmelidir.

Nitekim Kanun ve ilgili mevzuat, kişisel verilerin işlenmesini veya aktarılmasını yasaklayan değil; bu faaliyetlerin hangi şartlar altında hukuka uygun sayılacağını belirleyen çerçeve nitelikte düzenlemeler öngörmektedir.

| | |
|---|---|
| ! | **Hatırlatma**<br>Kanun, mutlak ve sınırsız bir engelleme gibi yorumlanarak özel kanunlar işlevsiz kılınmamalıdır. Kişilerin ve kurumların, kendilerine yöneltilen bilgi taleplerini doğrudan *"KVKK'ya aykırılık"* gerekçesiyle *"kategorik olarak/sistematik şekilde"* reddetmemeleri gerekir. |

Ayrıca; talep edilen bilginin kişisel veri niteliğinin yanlış belirlenmesi de uygulamada sık rastlanan bir durumdur. Bir işyerinin vergi kimlik numarasının talep edilmesi halinde, bu numaranın gerçek kişiye mi yoksa tüzel kişiye mi ait olduğunun belirlenmesi gerekir. Gerçek kişiye ait değilse ortada Kanun çerçevesinde bir kişisel veri bulunmayacaktır. Yine yalnızca kurumsal ad ve iletişim bilgilerini içeren verilerin kişisel veriymiş gibi yorumlanması da aynı şekilde Kanun'un kapsamının yanlış şekilde genişletilmesine neden olmaktadır. Oysa ad, soyad, ev adresi veya cep telefonu gibi bir gerçek kişiyi belirli kılan unsurlar bulunmadığında, kişisel veri işleme faaliyeti söz konusu olmayacaktır.

Burada önemle üzerinde durulması gereken bir diğer husus ise paylaşım faaliyetinin aktarım anlamına gelip gelmediğidir. Bu bakımdan özellikle yurt dışına aktarım meselesi önem arz etmektedir. Zira kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının uluslararası kurum ve kuruluşlarla yaptıkları iş birliği protokolleri çerçevesinde kişisel veri paylaşımı yükümlülükleri bulunabilmektedir. Türkiye'de yerleşik olmayan uluslararası kurum ve kuruluşlara kişisel veri aktarılması yurt dışına aktarım sayılacağı gibi bu kurum ve kuruluşların Türkiye'de bulunan ofisleriyle gerçekleştirilecek olan kişisel veri aktarımlarının da yurt dışına kişisel veri aktarımı sayılabileceği göz önünde bulundurulmalıdır.

Örneğin, Birleşmiş Milletler Mülteciler Yüksek Komiserliği'nin Türkiye Ofisine İçişleri Bakanlığı Göç İdaresi Başkanlığı tarafından mültecilere ait kişisel verilerin aktarılması yurt dışına kişisel veri aktarılması sayılacaktır. Böyle bir durumda yurt dışına kişisel veri aktarımına ilişkin mevzuat hükümlerine riayet edilmesi gerekmektedir.

Sonuç itibarıyla kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının Kanun'un uygulanması sırasında yaptığı bu tür farklı yorumlar, çoğu zaman kurumların aşırı ihtiyatlı davranma eğiliminden ve Kanun'u mutlak bir yasak gibi yorumlamasından kaynaklanmaktadır. Bu yaklaşım ise vatandaşların bilgiye erişim hakkını ve ihtiyaç duydukları belgeleri elde etme imkanını ayrıca kamu hizmetlerinin etkin yürütülmesini zayıflatabilmektedir.

Kanun kapsamında doğru olan her somut olayda öncelikle talep edilen bilginin gerçekten kişisel veri olup olmadığının tespit edilmesi, kişisel veri niteliği taşıyan bilgilerin söz konusu olması halinde ise Kanun'un 5'inci, 6'ncı, 8'inci ve 9'uncu maddelerinde yer alan hükümlerin dikkatle değerlendirilmesidir. Bu aşamada özel kanunların da kişisel verilerin aktarılmasına yönelik hüküm içeriyor olabileceği göz önünde bulundurularak 5'inci ve 6'ncı maddelerde yer alan veri işleme şartları aktarım yönünden ele alınmalıdır. Böyle bir bütüncül değerlendirme, kamu kurumları ile kamu kurumu niteliğindeki meslek kuruluşlarının hem hukuki yükümlülüklerini yerine getirmelerini hem de bireylerin temel hak ve menfaatlerini korumalarını mümkün kılacaktır.


Kamu Kurum ve Kuruluşları Arasında Hukuka Uygun Aktarım
Aktarım Bakımından Özel Düzenlemelerin Tespiti
Yurt İçinde Aktarım
Kanun'un 8'inci maddesinin üçüncü fıkrası uyarınca diğer kanunlarda yer alan hükümlerin saklı tutulması nedeniyle kurum/kuruluşların öncelikle görev alanlarını ilgilendiren mevzuat hükümlerinin incelenmesi gerekmektedir.
Bu hükümler "aktarıma cevaz verebilir".
Bu hükümler "aktarımı yasaklayabilir".
Yurt Dışına Aktarım
Kanun'un 9'uncu maddesinin onuncu fıkrasının atfı ile öncelikle kamu kurumlarının görev alanına giren hususlara ilişkin özel düzenlemelerin veya uluslararası anlaşmaların incelenmesi neticesinde aktarıma esas teşkil edecek (aktarıma cevaz veren) veya aktarımı yasaklayan bir hüküm bulunup bulunmadığı irdelenmelidir.
Aktarıma İlişkin Özel Düzenleme Bulunmaması Durumunda Aktarımın Hukuki Dayanağı
Yurt İçinde Aktarım
Kanun'un 8'inci maddesinin üçüncü fıkrası uyarınca aktarıma cevaz veren yahut aktarımı yasaklayan bir hüküm bulunmaması durumunda Kanun'un 8'inci maddesinin ikinci fıkrasının atfıyla Kanun'un 5 ve 6'ncı maddelerinde yer alan işleme şartlarının irdelenmesi gerekir.
Yurt Dışına Aktarım
Kanun'un 9'uncu maddesinin onuncu fıkrası uyarınca aktarıma esas teşkil eden yahut aktarımı yasaklayan bir hüküm bulunmaması durumunda;
1) Yeterlilik Kararı
2) Uygun Güvence Sağlanması
a) Uluslararası Sözleşme Niteliğinde Olmayan Olmayan
b) Bağlayıcı Şirket Kuralları
c) Standart Sözleşme
d) Taahhütname
3) Arızi Haller
Aktarımda Ölçülülük
"İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma"
Kamu Kurum ve Kuruluşlarının Görev ve Yetki Sınırları Dışında, Amaçla Doğrudan İlgili Olmayan Hiçbir Kişisel Veriyi İşlememesi veya Başka Kurumlara Aktarmaması
Güvenlik Aktarım Yöntemleri ve Teknik/İdari Tedbirler
Aktarımın Hukuki Dayanağının ve Ölçülülüğünün Sağlanmasına Ek Olarak Kişisel Veri Aktarımının Güvenli Bir Şekilde Gerçekleşmesi
Sık Karşılaşılan Durumlar
Aktarım Süreçlerin Özel Düzenlemelerin Kanun'un 8'inci ve 9'uncu Maddeleriyle Bütüncül Ele Alınmaması
Yurt Dışına Aktarım Bakımından Yeterlilik Kararının Nihai Aktarım Yöntemi Olarak Değerlendirilmesi
Aktarım Hukuka Uygun Olmakla Birlikte Kanun'un 4'üncü Maddesindeki İlkelere Uygun Davranılmaması
Aktarım Taleplerinin Sistematik/Kategorik Şekilde Reddedilmesi

# 6. KAMU KURUMLARI BAKIMINDAN TAM VE KISMİ İSTİSNA HALLERİ

Kanun'un 28'inci maddesinin birinci fıkrasında Kanun hükümlerinin bütün olarak uygulanmayacağı "tam istisna halleri", ikinci fıkrasında ise belirli koşullar altında bazı Kanun hükümlerinin uygulanmayacağı "kısmi istisna halleri", sınırlı sayma metodu ile düzenleme altına alınmıştır.

Kanun'un 3'üncü maddesinin birinci fıkrasının (e) bendinde "*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 işlem*" şeklinde tanımlanmış olup Kanun'un istisna hallerinin düzenlendiği 28'inci maddesinde yer alan "kişisel verilerin işlenmesi" ifadelerinde de anlaşılması gereken yine Kanun'un 3'üncü maddesinde sayılan kişisel veri işleme faaliyetleridir.

İstisna maddesinin birinci fıkrasında sayılan; "*a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya*

*aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi; b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi; c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi; ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi; d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi*" durumlarında Kanun hükümlerinden tamamıyla muafiyet söz konusudur. İkinci fıkrasında sayılan "*a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması; b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi; c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması; ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*" durumlarında ise Kanun'un amacına ve yine Kanun'da düzenleme altına alınan genel ilkelere uygun ve orantılı olmak kaydıyla aydınlatma yükümlülüğünün düzenlendiği 10'uncu madde, ilgili kişinin haklarının düzenleme

altına alındığı 11'inci madde (zararın giderilmesini talep etme hakkı hariç olmak üzere) ve veri sorumluları siciline kayıt yükümlülüğünün düzenlendiği 16'ncı madde uygulanmayacaktır.

### 6.1. Kanun'un Uygulanmayacağı Haller (Tam İstisna Halleri)

#### 6.1.1. Kişisel Verilerin, Üçüncü Kişilere Verilmemek ve Veri Güvenliğine İlişkin Yükümlülüklere Uyulmak Kaydıyla Gerçek Kişiler Tarafından Tamamen Kendisiyle veya Aynı Konutta Yaşayan Aile Fertleriyle İlgili Faaliyetler Kapsamında İşlenmesi

Kişisel verilerin üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak şartıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili işlenmesine ilişkin faaliyetler, Kanun'un 28'inci maddesinin birinci fıkrasının (a) bendinde düzenlenen tam istisna halleri arasında yer almaktadır.

Söz konusu düzenlemenin yalnızca kişilerin özel veya aile hayatları içerisinde gerçekleştirilen faaliyetlere ilişkin olarak bendin lafzında sayılan hususların dışında yorumlara yer verilmeden dar yorumlanması gerekmektedir.

Düzenlemede kişisel veri işleme faaliyetinin, gerçek kişi tarafından gerçekleştirilmesi, tamamen kendisiyle ilgili veya aynı konutta yaşadığı aile fertleriyle ilgili faaliyetleri kapsaması, üçüncü kişilerle paylaşılmaması ve veri güvenliğine ilişkin yükümlülüklere uyulması şartlarına bağlandığına dikkat edilmesi gerekmektedir.

Örneğin; aynı konutta yaşayan aile bireyinin doğum gününde, yine aynı konutta yaşan başka bir aile bireyi tarafından fotoğraflarının çekilerek cep telefonunda depolanması durumunda Kanun hükümleri uygulanmayacaktır. Somut olay nezdinde fotoğrafları telefonunda depolayan aile bireyinin fotoğrafları sosyal medya platformlarında paylaşması durumunda ise kişisel verilerin üçüncü kişilerle paylaşılması durumu söz konusu olacağından istisna kapsamının şartlarının sağlanmaması nedeniyle (üçüncü kişilere verilmemesi kaydı) söz konusu faaliyet Kanun kapsamı içerisinde yer alacaktır.

### 6.1.2. Kişisel Verilerin Resmi İstatistik ile Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla İşlenmesi

Kanun'un 28'inci maddesinin birinci fıkrasının (b) bendi incelendiğinde ilgili düzenlemenin çeşitli işleme amaçlarını ihtiva ettiği görülmektedir. Bunlar kişisel verilerin; resmi istatistik amacıyla işlenmesi, anonim hale getirilerek araştırma amacıyla işlenmesi, anonim hale getirilerek planlama amacıyla işlenmesi ve anonim hale getirilerek istatistik amaçlarıyla işlenmesidir.

5429 sayılı Kanun uyarınca "resmi istatistik", Türkiye İstatistik Kurumu (TÜİK) veya Resmî İstatistik Programı'nda (Program) yer alan konularda istatistik üretecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle özelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgiyi ifade etmektedir. 31 Aralık 2021'de Resmî Gazete'de yayınlanan Resmi İstatistik Programı (2022-2026) uyarınca resmi istatistik oluşturmada görevli kamu kurum ve kuruluşları "*Cumhurbaşkanlığı ve bakanlıklar ile bunların bağlı, ilgili ve ilişkili kuruluşları; Mahalli idareler*

*ve bunların bağlı ve ilgili kuruluşları ile birlik ve şirketleri; Türkiye Cumhuriyet Merkez Bankası, Borsa İstanbul ve üniversiteler de dahil olmak üzere, tüzel kişiliğe haiz enstitü, teşebbüs, teşekkül, birlik, döner sermaye, fon ve sair adlarla kurulmuş olan kurum ve kuruluşlar; Kamu kurumu niteliğindeki meslek kuruluşları*"dır.

Resmi istatistiğin idari kayıtların işlenmesi suretiyle üretilebilmesi mümkündür. İdari kayıt "*Devletin diğer kurum/kuruluşların gerek mevzuatlar çerçevesinde tutmakla zorunlu oldukları gerekse kurumsal hizmetlerin yürütülmesinde ihtiyaç duydukları konularda kişi, işletme veya olay bazında düzenlenen rapor, belge ve ölçüm türü gibi dokümanlar*" anlamına gelmektedir[35]. Çeşitli ilkeler çerçevesinde söz konusu idari kayıtların standardizasyonu neticesinde oluşturulan sistematik kayıt sistemleri, resmi istatistiksel verileri meydana getirmektedir. Mevzuatımız kapsamında 5429 sayılı Kanun'un 9'uncu maddesi gereğince TÜİK tarafından idari kayıtlara erişilebilmesi mümkündür.

5429 sayılı Kanun'un 2'nci maddesinin (g) bendi incelediğinde temelde ardışık iki faaliyet göze çarpmaktadır. Bunlar verilerin derlenmesi ve işlenmesi neticesinde bilgi elde edilmesidir. TÜİK veya veri derleme faaliyetinin gerçekleşeceği dönemi kapsayan Program tarafından belirlenen konularda istatistik üretmekle görevli kurum ve kuruluşların bünyelerindeki verilerin derlenmesi (toplanması), ardından bu verilerin kitle özelliklerinin ortaya konulması amacıyla işlenmesi ve bu işleme faaliyeti neticesinde bir bilgi elde edilmesi neticesinde resmi istatistik meydana gelmektedir. Tanımdan da anlaşılacağı üzere resmi istatistik derlenen verilerin işlenmesi suretiyle elde edilmektedir. Söz konusu Programla resmi istatistiklerde standardizasyon sağlanmakta,

35 Türkiye İstatistik Kurumu, İstatistik Üretiminde İdari Kayıtların Rolü, https://www.tuik.gov.tr/media/corporatecontent/268-İstatistik_Üretiminde_İdari_Kayıtların_Rolü.pdf.

sorumlu ve ilgili kurumlar tanımlanarak, hangi verinin hangi kurum tarafından, hangi yöntemle ve hangi dönemler için derleneceği ve ne zaman yayımlanacağı konularına açıklık getirilmektedir.

Öte yandan, 5429 sayılı Kanun'un 6'ncı maddesi "*Resmî istatistikler Türkiye İstatistik Kurumu Başkanlığı ve Programda belirtilen kurum ve kuruluşlar tarafından üretilir, dağıtılır ve yayımlanır. Kurum ve kuruluşların, görev alanları ile ilgili resmi istatistiklere ilişkin veri derleme, değerlendirme ve yayımlama görev ve yetkisi Programda açıkça belirtilir. Bu kurum ve kuruluşlar, talep edilmesi durumunda, derlenen verileri istenilen zamanda Başkanlığa vermekle yükümlüdür. ... Kurum ve kuruluşlar Programda yer almayan istatistikî konulardaki çalışmaları ile gerçek kişiler veya özel hukuk tüzel kişiliğine sahip kuruluşlarca yapılan sayım veya araştırmalara ait sonuçlar Resmî istatistik olarak kabul edilmez.*" hükmünü amirdir. Bu bakımdan, Programda yer almayan kurum veya kuruluşların ya da Programda yer alsa dahi Programda yer almayan istatistikî konularda gerçekleştirilen çalışmalar ile gerçek kişiler veya özel hukuk tüzel kişiliğine sahip kuruluşlarca yapılan sayım veya araştırmalara ait sonuçlar "resmî istatistik" kavramı kapsamında değerlendirilemeyecektir. Ancak Program dönemi için öngörülmemiş, fakat dönem içinde kurum/kuruluşlarca üretilmesine ihtiyaç duyulan istatistiklerin yıllık güncelleme tarihine kadar TÜİK ile iş birliği yapılmak suretiyle resmi istatistik niteliği kazanması sağlanabilir. İlgili konunun ilk revizyonda Programa dahil edilmesi mümkündür.

Özetle; resmi istatistikler TÜİK ve Programda belirtilen kurum ve kuruluşlar tarafından üretilir ve yayımlanır. Kurum ve kuruluşların, görev alanları ile ilgili resmi istatistiklere ilişkin veri derleme, değerlendirme ve yayımlama görevi Programda yer almaktadır. Resmi istatistiklerin

üretim ve yayımının koordinasyonundan sorumlu olan TÜİK, Programda görev verilen kurum ve kuruluşlar tarafından derlenen resmi istatistikleri de yayımlayabilir ve dağıtabilir. Bu kurum ve kuruluşlar, talep edilmesi durumunda, derlenen verileri istenilen zamanda ve istenilen içerikte TÜİK'e vermekle yükümlüdürler. Diğer yasal düzenlemelerdeki gizlilik hükümleri belirtilerek, TÜİK'e iletilen veri ve bilgilerin korunmasında ve saklanmasında söz konusu gizlilik hükümleri aynen uygulanır.

Diğer taraftan araştırma, planlama ve istatistik gibi amaçlarla işlenen kişisel verilerin anonim hale getirilmesi suretiyle kullanılması ve sonuca varılmasının mümkün olduğu durumlarda da Kanun'un 28'inci maddesinin birinci fıkrasının (b) bendi gereğince Kanun'dan tamamıyla muafiyet sağlanabilecektir. Halihazırda anonim veri söz konusu olduğunda Kanun uygulanmayacaktır. Burada ilgili bentte düzenlenen amaçla gerçekleştirilen veri işleme faaliyetinin tam istisna kapsamında yer alabilmesi için verilerin anonimleştirilmesi gerekmektedir[36].

Sonuç olarak, kamu kurum ve kuruluşları tarafından resmi istatistik üretimi amacıyla gerçekleştirilen veri işleme faaliyetleri ile kişisel verilerin anonim hale getirilmesi suretiyle araştırma, planlama ve istatistik gibi amaçlarla gerçekleştirilen veri işleme faaliyetleri Kanun'un 28'inci maddesinin birinci maddesinin (b) bendi uyarınca istisna hükmü kapsamındadır.

36 Araştırma Şirketlerinin İstatistiksel Araştırma Yapmak Amacıyla "Rastgele Numara Çevirme ile Telefon Mülakatı Yöntemi" Kullanarak Gerçekleştirdikleri Kişisel Veri İşleme Faaliyetleri Hakkında Kamuoyu Duyurusu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7989/-Arastirma-Sirketlerinin-Istatistiksel-Arastirma-Yapmak-Amaciyla-Rastgele-Numara-Cevirme-ile-Telefon-Mulakati-Yontemi-Kullanarak-Gerceklestirdikleri-Kisisel-Veri-Isleme-Faaliyetleri-Hakkinda-Kamuoyu-Duyurusu.

Örneğin; 2022-2026 Resmi İstatistik Programı'nın 1.1.1. numaralı ve "İstatistiksel İş Kayıtları" başlıklı istatistiksel altyapıya yönelik istatistik çalışması kapsamında üretilmesi planlanan istatistiklerden biri Esnaf ve Sanatkâr Bilgi Sistemi'nde (ESBİS) yer alan esnaf ve sanatkâr istatistikleri olup söz konusu istatistiki veriler ülkeye özgü ihtiyaç nedeniyle Ticaret Bakanlığı sorumluluğunda ESBİS verilerinin üretimi ile sağlanacaktır. Bu verinin üretimi esnasında çalışmadan ve temel ihtiyaçları karşılamakla sorumlu kurum Ticaret Bakanlığı'dır. Diğer taraftan bir diğer istatistiksel altyapı ögesi olan ve Resmi İstatistik Programı'nın 1.1.6. numaralı başlığında düzenlenen Eğitim İşgücü Veritabanı'nın oluşturulmasından ise TÜİK sorumludur. Söz konusu istatistiki verinin üretimine ilişkin olarak temel ihtiyaçları yani verileri karşılayacak olan kurum ve kuruluşlar ise sırası ile Yüksek Öğretim Kurumu, Millî Eğitim Bakanlığı, Sosyal Güvenlik Kurumu, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ve Muhasebat Genel Müdürlüğü'dür. Belirtilen kurumlardan idari kayıtların zamanlı ve standart bir şekilde TÜİK'e akışı sağlanacaktır. Bu kapsamda söz konusu veri akışı esnasında kişisel veri işlenmesi halinde Kanun'un 28'inci maddesi uygulama alanı bulacaktır. Söz konusu muafiyet hali hem alıcı hem de gönderici bakımından yalnızca düzenleme altına alınan veri işleme amacı ile sınırlı olarak uygulanacaktır.

Örneğin; bir kamu kurumu Program kapsamında olmasa dahi bünyesindeki kişisel verilerden amacıyla bağlantılı olarak anonim hale getirmek suretiyle istatistiki veri üretebilecektir. Kamu kurumunun kişisel verileri anonim hale getirmeden resmi istatistik üretebilmesi ise Program içerisinde yer almasına yahut sonradan TÜİK ile iş birliği yaparak ürettiği verinin Program kapsamına dahil edilmesine bağlıdır.

### 6.1.3. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini, Ekonomik Güvenliği, Özel Hayatın Gizliliğini veya Kişilik Haklarını İhlal Etmemek ya da Suç Teşkil Etmemek Kaydıyla, Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında İşlenmesi

Sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında kişisel verilerin işlenmesi Kanun'un 28'inci maddesinin birinci fıkrasının (c) bendi kapsamında tam istisna hükümleri kapsamında değerlendirilmiş olup Kanun; sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında kişisel veri işleme faaliyetinin tam istisna kapsamında değerlendirilebilmesi halini söz konusu işleme faaliyetinin gerçekleştirilmesi esnasında millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemesi ya da suç teşkil etmemesi şartına bağlanmıştır.

Kişisel verinin söz konusu amaçlarla işlenmesine ilişkin sürecin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal edip etmediği ya da suç oluşturup oluşturmadığına ilişkin kanaat, somut olay nezdinde yapılacak değerlendirme ile neticelenecektir.

Örneğin, Aile ve Sosyal Hizmetler Bakanlığı Eğitim ve Yayın Dairesi Başkanlığı tarafından sanat, tarih, edebiyat veya bilimsel amaçlarla gerçekleştirilen çalışmaların Kanun'un 28'inci maddesinin birinci fıkrasının (c) bendi kapsamında değerlendirilebilmesi mümkündür.

#### 6.1.4. Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini veya Ekonomik Güvenliği Sağlamaya Yönelik Olarak Kanunla Görev ve Yetki Verilmiş Kamu Kurum ve Kuruluşları Tarafından Yürütülen Önleyici, Koruyucu ve İstihbarî Faaliyetler Kapsamında İşlenmesi

Kişisel verilerin önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesinin tam istisna kapsamında değerlendirilebilmesi ancak kişisel veri işleme faaliyetinin; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak ve yalnızca kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından gerçekleştirilmesi durumunda söz konusu olabilecektir.

Kanun'un genel gerekçesinde söz konusu bende ilişkin olarak "*Millî İstihbarat Teşkilâtı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır. Bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği veriler de kapsam dışında tutulmaktadır*" açıklamasına yer verilmiştir.

Bu kapsamda, yürütülen önleyici, koruyucu ve istihbarî faaliyetler bakımından; söz konusu faaliyetleri yerine getirmekle görevli kurum ve kuruluşlara ilişkin olarak, ilgili hükümde belirtilen amaçlarla sınırlı kalmak koşuluyla, diğer kamu kurum ve kuruluşlarınca gerçekleştirilecek kişisel verilerin açıklanması, aktarılması, elde edilebilir hale getirilmesi, sınıflandırılması gibi kişisel verilerin işlenmesi faaliyetleri Kanun'un istisna hükümleri kapsamında değerlendirilecektir.

T.C. İçişleri Bakanlığının millî savunmayı ve millî güvenliği sağlamaya yönelik önleyici ve koruyucu faaliyetler kapsamında işlediği kişisel veriler ve Millî İstihbarat Teşkilâtı tarafından milli güvenliği sağlamak amacıyla gerçekleştirilen istihbarî faaliyet kapsamında işlenen kişisel veriler söz konusu düzenlemeye örnek olarak gösterilebilecektir.

### 6.1.5. Kişisel Verilerin Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerine İlişkin Olarak Yargı Makamları veya İnfaz Mercileri Tarafından İşlenmesi

Kişisel verilerin, yargı makamları veya infaz mercileri tarafından soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak işlenmesi de Kanun tarafından tam istisna kapsamında düzenlenmiştir. Bu noktada belirtmek gerekir ki yargı makamları veya infaz mercilerinin yalnızca soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin faaliyetleri bakımından Kanun'dan tam istisna hali iken söz konusu işlemler dışında kalan faaliyetleri Kanun kapsamında yer almakta dolayısıyla Kanun'a tâbi olmaya devam etmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 2'nci maddesinde soruşturma, kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi; kovuşturma, iddianamenin kabulüyle başlayıp hükmün kesinleşmesine kadar geçen evreyi ifade etmektedir.

Bu kapsamda kişisel verilerin yargı makamları veya infaz mercileri tarafından soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak işlenmesi istisna kapsamında değerlendirilirken kurum ve kuruluşları tarafından yargı makamlarına veya infaz mercilerine aktarılan kişisel veriler Kanun'un 5'inci maddesinin ikinci fıkrasının (ç) bendi uyarınca "*Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.*" işleme şartı kapsamında işlenebilecek, başka bir ifadeyle tam istisna hali yalnızca verinin aktarıldığı yargı makamları ve infaz mercileri bakımından söz konusu iken kamu kurum ve kuruluşlarının soruşturma, kovuşturma, yargılama veya infaz işlemleri kapsamında yargı makamlarına veya infaz mercilerine iletilmek üzere işlediği kişisel veriler bakımından Kanun ile bağlılık devam edecek, söz konusu faaliyet istisna kapsamında değerlendirilmeyecektir.

Örneğin; soruşturma sürecinde Cumhuriyet Savcılıkları tarafından işlenen kişisel veriler, kovuşturma sürecinde Mahkemeler tarafından işlenen kişisel veriler ile Ceza ve Tevkifevleri tarafından infazın yerine getirilmesine dair iş ve işlemlere ilişkin olarak işlenen kişisel veriler söz konusu istisna kapsamına dahildir.

### 6.2. Kanun'un Kısmen Uygulanmayacağı Haller (Kısmen İstisna Halleri)

Kanun'un 28'inci maddesinin ikinci fıkrasında Kanun'un amacına ve genel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10'uncu, zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarını düzenleyen 11'inci ve VER-

BİS'e kayıt yükümlülüğünü düzenleyen 16'ncı maddelerinin bazı durumlarda uygulanmayacağı düzenlenmiştir. İstisna tutulan maddeler haricinde Kanun ile getirilmiş olan diğer yükümlülükler, veri sorumluları bakımından uygulanmaya devam edecektir. Belirtmek gerekir ki sayılan maddelere ilişkin istisnalar kapsamında kişisel veri işlenmesinin ön koşulu Kanun'un amacına ve genel ilkeler ile uyumlu ve orantılı olmaktır. Dolayısıyla kısmen istisna durumu mevcut olsa dahi veri sorumluları tarafından Kanun'un amacına ve genel ilkelere uygun olarak kişisel veri işleme faaliyetinde bulunulması gerekmektedir.

### 6.2.1. Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması için Gerekli Olması.

Kişisel verilerin suç soruşturması veya suç işlenmesinin önlenmesi için gerekli olması halinde işlenmesi durumunda ilgili kişinin aydınlatılması, ilgili kişinin kişisel verilerine ilişkin bilgi talep etmesi ve veri sorumlusunun VERBİS'e kayıt yükümlülüğü söz konusu olmayacaktır. Öte yandan Kanun'un lafzı dikkate alındığında yalnızca "gerekli" olduğu ölçüde kişisel verilerin işlenmesi bakımından kısıtlamaya gidildiği görülmektedir.

Söz konusu kısmen istisna durumunda yalnızca "*suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*" durumunda kişisel verilerin işlenmesi hali düzenlenmiş olup veriyi işleyen veri sorumlusunun, "*kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları*" olması şartı aranmamıştır.

Şiddet Önleme ve İzleme Merkezi nezdinde suç işlenmesinin önlenmesi amacıyla tedbir amaçlı gerçekleştirilen kişisel veri işleme faaliyetleri bu madde kapsamında değerlendirilebilecektir.

### 6.2.2. İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi

Aleni kelime olarak "açık, ortada, meydanda, herkesin içinde yapılan"[37] anlamına gelirken; alenileşmek "herkesçe bilinir duruma gelmek."[38] olarak tanımlanmaktadır. Bu kapsamda ilgili kişinin kendisi tarafından kişisel verilerini herkesçe bilinir hale getirmesi durumunda anılan hüküm kapsamında veri sorumluları bakımından çeşitli muafiyetler söz konusu olacaktır.

İlgili kişinin kişisel verilerinin kendisi tarafından alenileştirilmesi, kişisel verilerin Kanun'un amacına ve genel ilkelerine uygun ve orantılı olarak işlenmesi gerekliliğini ortadan kaldırmayacaktır. Bunun yanında ilgili kişi tarafından alenileştirilmiş kişisel veri işlenirken ilgili kişinin alenileştirme iradesinin gözetilmesi gerekmekte olup kısmen istisna hali alenileştirilme amacı ile sınırlıdır.

37 Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/, "aleni".
38 Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/, "alenileşmek".

Örneğin; avukatlık mesleğini icra eden bir kişinin Türkiye Barolar Birliği'nin levha sorgulamasında görüntülenebilen bilgileri arasında cep telefonu numarası ve adres bilgisinin yer alması mesleki gerekçelerle tarafına ulaşılmasını isteme amacıyla alenileştirilme amacı açık olan bir durumdur. Ancak söz konusu avukatın cep telefonu numarasının vekil sıfatı ile işlem yürütmeksizin kişisel işleri dolayısıyla kamu kurumuna yapmış olduğu başvuruya ilişkin olarak bilgi verilmesi amacıyla arama yapılması suretiyle kullanılması, alenileştirme ile amaçlananın aşılması sonucunu doğuracaktır.

Alenileştirme, ilgili kişinin "Kanun'u tamamen devre dışı bıraktığı" anlamına gelmemekte; yalnızca ilgili kişinin kendi iradesiyle kamuya açık hâle getirdiği veriler bakımından amaçla sınırlı, dar kapsamlı bir istisna sağlamaktadır.

### 6.2.3. Kişisel Veri İşlemenin Kanun'un Verdiği Yetkiye Dayanılarak Görevli ve Yetkili Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşlarınca, Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması İçin Gerekli Olması

Kanun'un verdiği yetkiye dayalı olarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması durumunda kişisel verilerin işlenmesi bakımından kısmen istisna kapsamındadır.

Bu istisna yalnızca görevle doğrudan bağlantılı işlemler bakımından geçerli olup ilgili kurum veya kuruluşun görev kapsamında olmayan diğer tüm kişisel veri işleme faaliyetleri için Kanun'un hükümleri uygulanmaya devam edecektir.

Örneğin, bir kamu personeli hakkında idari soruşturma yürütülmesi bakımından ilgili kişinin verilerinin işlenmesi kısmen istisna kapsamında olup söz konusu İdare, idari soruşturma kapsamında bulunmayan hususlarda yine Kanun'a tabii olacaktır.

!

**Hatırlatma**

Mevzuat hükümleri gereğince denetleme görevi yerine getirmekte olan kamu kurum ve kuruluşunun yine tabi olunan mevzuat uyarınca gerçekleştirdiği aktarım faaliyetine ilişkin olarak Kanun'un 28'inci maddesinin ikinci fıkrasının (c) bendi kapsamında aydınlatma yükümlülüğünü yerine getirme zorunluluğu bulunmamaktadır.

T.C. Kişisel Verileri Koruma Kurumunun, Kanun'un 15'inci maddesinin üçüncü fıkrası gereğince veri sorumlusundan bilgi ve belgeler talep etmesi üzerine, veri sorumlusunun istenilen bilgi ve belgeleri Kişisel Verileri Koruma Kurumuna sunması, Kanun'un 5'inci maddesinin ikinci fıkrasının (a) bendi uyarınca "Kanunlarda açıkça öngörülmesi" ve (ç) bendinde "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" gibi işleme şartları bakımından gerçekleştirilebilecek olup bu kapsamda söz konusu kişisel verilerin Kuruma teslim edilmesine ilişkin süreçte Kanun'un 28'inci maddesinin ikinci fıkrası uyarınca, veri sorumluları bakımından ilgili kişileri aydınlatma yükümlülüğü doğmayacaktır.

T.C. Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca Kurum ve Kuruluşlardan talep edilen bilgilerin BTK'ya sunulması bakımından yine Kanun'un 28'inci maddesinin ikinci fıkrası uyarınca ilgili kişileri aydınlatma yükümlülüğü doğmayacaktır.

### 6.2.4. Kişisel Veri İşlemenin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması için Gerekli Olması

Bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için kişisel veri işlenmenin gerekli olduğu durumlar kısmen istisna kapsamında düzenlenmiştir.

Devletin ekonomik ve mali çıkarlarının korunması, kamu kurumlarının yürüttüğü bazı denetim, inceleme ve gözetim faaliyetlerinde kişisel veri işlenmesini zorunlu kılabilir. Kanun'un ilgili istisna hükmü, bu kapsamda yapılacak veri işleme faaliyetlerinin yalnızca kamu maliyesinin korunması için gerekli olduğu ölçüde ve belirli amaçla sınırlı olarak gerçekleştirilebileceğini düzenlemektedir.

Bu çerçevede, bütçe, vergi, kamu gelirleri, mali yükümlülükler ve kamu kaynaklarının yönetimiyle doğrudan ilişkili işlemlerde, görevli ve yetkili kurumların bilgi talep etmesi halinde veri paylaşımı istisna kapsamında değerlendirilebilir.

Örneğin; vergi idaresi, denetim makamları veya diğer yetkili kamu otoriteleri tarafından, mükelleflerin mali durumlarına ilişkin bilgi talep edilmesi durumunda; ilgili kurum veya finans kuruluşu yalnızca talep edilen amacın gerektirdiği kadar veri ile sınırlı olmak kaydıyla bu bilgileri paylaşabilir.

Bu istisna, kişisel verilerin mali suçların önlenmesi, vergi kayıp ve kaçaklarının tespiti, kamu kaynaklarının etkin kullanımı, bütçe disiplini ve mali denetim süreçlerinin yürütülmesi gibi kamu maliyesine ilişkin zorunlu ve meşru amaçlar doğrultusunda işlenmesini mümkün kılmaktadır. Ancak istisnanın kapsamı geniş yorumlanmamalı; veri işleme faaliyetleri ölçülülük, amaçla sınırlılık ve ilgili mevzuata uygunluk ilkelerine bağlı olarak yürütülmelidir.

# SONUÇ

6698 sayılı Kanun, kişisel verilerin işlenmesini disiplin altına alarak veri sorumlularının yükümlülükleri ile uyacakları usul ve esasları düzenlemektedir. Veri sorumlusu kavramı, Kanun'un kişisel veri işleme faaliyetine ilişkin hukuki yükümlülükleri tayin etmek amacıyla belirlediği bir statü olup Kanun'un 3'üncü maddesinin birinci fıkrasının (ı) bendinde; kişisel verilerin işleme amaç ve vasıtalarını belirleyen veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmaktadır.

Özellikle kamu kurumlarının, taşra ve yurt dışı teşkilatları ile bağlı, ilgili ve ilişkili kuruluşlarının kişisel veri işleme faaliyetleri göz önünde bulundurulduğunda veri sorumlusunun tespitinin yapılması, uyacakları hukuki yükümlülükler bakımından önem arz etmekte olup tanımda yer alan kriterleri karşılamaları durumunda kamu kurum ve kuruluşları da bu statüde yer alacaktır.

Kamu kurum ve kuruluşları nezdinde işlenen kişisel veriler, Kanun'un 4'üncü maddesinde yer alan genel ilkelere uygun işlenmeli, verinin niteliğine göre kişisel verilerin işlenmesi, Kanun'un 5'inci ve 6'ncı maddelerinde yer alan uygun hukuki şartlara dayandırılmalıdır.

Kamu kurum ve kuruluşları arasında veya kamu kurum ve kuruluşları ile gerçek kişiler ya da özel hukuk tüzel kişileri arasında yurt içinde bir kişisel veri aktarımı gerçekleşecek ise söz konusu aktarım faaliyeti, Kanun'un 8'inci maddesi hükümlerine uygun olarak gerçekleştirilmelidir. Öte yandan kişisel verilerin veri sorumlusu sıfatını haiz bir tüzel kişiliğin bünyesinde çalışanlar veya birimler arası paylaşımı, Kanun'un 8'inci maddesi çerçevesinde bir aktarım olarak değerlen-

dirilmemektedir. Kişisel verilerin yurt dışına aktarılması durumunda ise, Kanun'un 9'uncu maddesine riayet edilmesi gerekmektedir. Bununla birlikte kişisel veri aktarımlarında yalnızca aktarım amacına uygun ölçüde veri aktarımı gerçekleştirilmelidir.

Ayrıca veri sorumlusu ve yetkilendirdiği kişi tarafından kişisel verilerin elde edilmesi sırasında Kanun'un 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğü yerine getirilmeli, bu doğrultuda ilgili kişiler, kişisel verilerin hangi amaçla neden kullanıldığı, hangi yöntemlerle elde edildiği, kimlere aktarıldığı ve sahip oldukları haklara ilişkin bilgilendirilmelidir. Bu kapsamda ilgili kişilere sunulan aydınlatma metinleri açık, sade ve anlaşılır olmalı; eksik, yanıltıcı veya yanlış bilgilere yer verilmemelidir.

Veri sorumlusu olan kamu kurum ve kuruluşları Kanun'un 12'nci maddesinin birinci fıkrası çerçevesinde; kişisel verilerin hukuka aykırı olarak işlenmesini ve bu verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Kamu kurum ve kuruluşları, bu tedbirleri hem kendi bünyesinde almalı hem de kendisi adına kişisel veri işleme faaliyeti yürüten başka gerçek veya tüzel kişiler bulunması durumunda bu kişilerce alınmasını sağlamalıdır. Kanun'un 12'nci maddesinin ikinci fıkrası gereğince veri sorumlularının birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu olduğu unutulmamalıdır. Ayrıca veri sorumluları, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla kendi kurum veya kuruluşunda gerekli denetimleri yapmak veya yaptırmak zorundadır.

# KAYNAKLAR


- Access to Official Documents Guide, Erişim Adresi: https://rm.coe.int/access-to-official-documents-guide/168069660c, s. 16.
- Araştırma Şirketlerinin İstatistiksel Araştırma Yapmak Amacıyla "Rastgele Numara Çevirme ile Telefon Mülakatı Yöntemi" Kullanarak Gerçekleştirdikleri Kişisel Veri İşleme Faaliyetleri Hakkında Kamuoyu Duyurusu, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7989/-Arastirma-Sirketlerinin-Istatistiksel-Arastirma-Yapmak-Amaciyla-Rastgele-Numara-Cevirme-ile-Telefon-Mulakati-Yontemi-Kullanarak-Gerceklestirdikleri-Kisisel-Veri-Isleme-Faaliyetleri-Hakkinda-Kamuoyu-Duyurusu
- Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf.
- Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf
- Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf.
- Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf.
- Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf.

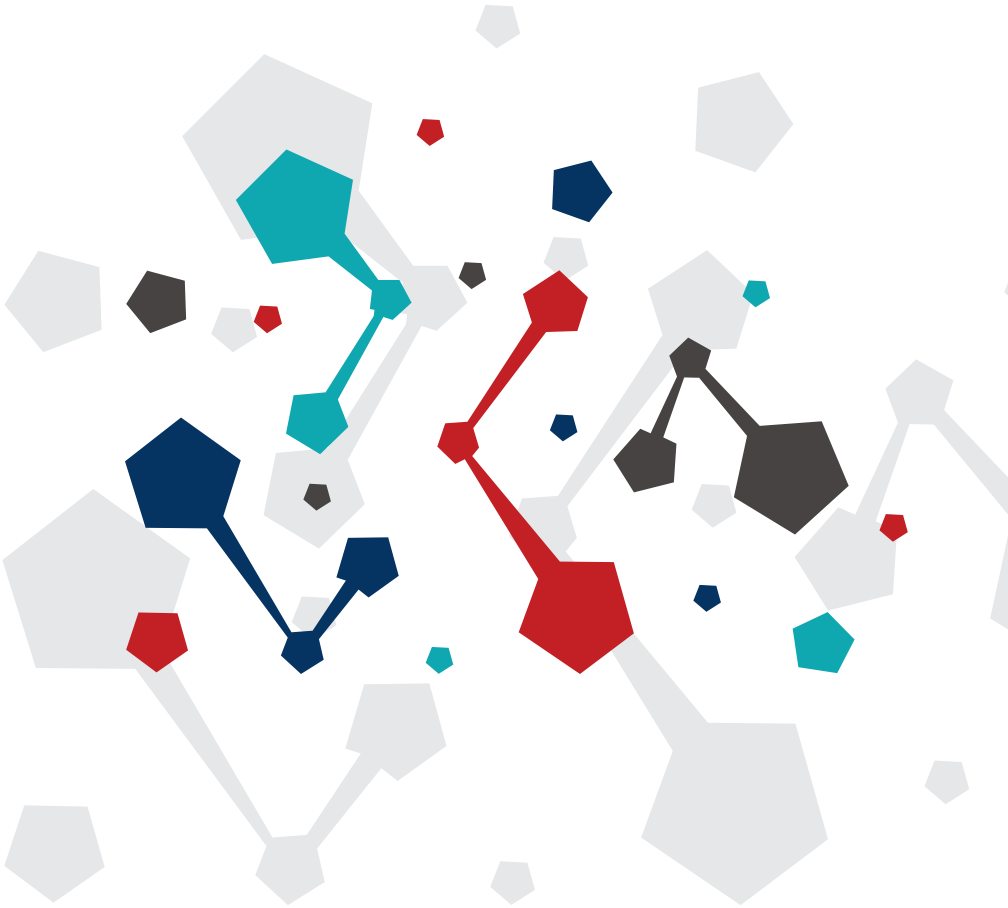
- Kişisel Verileri Koruma Kurumu, 10 Kasım 2025 tarihli Uluslararası Sözleşme Niteliğinde Olmayan Anlaşma ile Yurt Dışına Kişisel Veri Aktarımına İzin Verilmesi Hakkında Duyuru, https://www.kvkk.gov.tr/Icerik/8538/uluslararasi-sozlesme-niteliginde-olmayan-anlasma-ile-yurt-disina-kisisel-veri-aktarimina-izin-verilmesi-hakkinda-duyuru,
- Kurula İletilen Şikâyet ve İhbarlarda Sık Yapılan Hatalar, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7de6abf3-ea1c-4bc2-98f5-3ab90b4f5ddb.pdf.
- Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/2f2fbcf4-932b-4dad-af8a-cd32e315d815.pdf
- Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/, alenileşmek.
- İstatistik Üretiminde İdari Kayıtların Rolü, Türkiye İstatistik Kurumu, https://www.tuik.gov.tr/media/corporatecontent/268-İstatistik_Üretiminde_İdari_Kayıtların_Rolü.pdf.
- Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) Kılavuzu, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c7058b41-6d7e-455a-ae96-3ebc8dabe989.pdf.
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar -1, Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ca752cda-c3df-4645-8d5e-e2a507e63200.pdf
- 25 Soruda Bilgi Edinme Hakkı, Bilgi Edinme Değerlendirme Kurulu, https://bedk.adalet.gov.tr/Resimler/SayfaDokuman/233202015214925_SORUDA_BILGI_EDINME_HAKKI.pdf

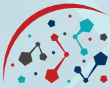

**Kurul Kararları**


- Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/4110/2018-10.

- Kişisel Verileri Koruma Kurulunun 28.06.2018 tarihli ve 2018/69 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/5366/2018-69.
- Kişisel Verileri Koruma Kurulunun Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin 24.01.2019 tarih ve 2019/9 sayılı Kararı, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu.
- Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi.
- Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli ve 2019/271 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/5547/2019-271.
- Kişisel Verileri Koruma Kurulunun 26.12.2019 tarihli ve 2019/389 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/6668/2019-389.
- Kişisel Verileri Koruma Kurulunun 29.09.2020 tarihli ve 2020/746 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/6954/2020-746.
- Kişisel Verileri Koruma Kurulunun 22/12/2020 tarihli ve 2020/966 sayılı İlke Kararı https://www.kvkk.gov.tr/Icerik/6858/2020-966
- Kişisel Verileri Koruma Kurulunun 11.03.2021 tarihli ve 2021/238 sayılı kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/6905/2021-238.
- Kişisel Verileri Koruma Kurulunun 02.12.2021 tarihli ve 2021/1214 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7270/2021-1214.

- Kişisel Verileri Koruma Kurulunun 04.08.2022 tarihli ve 2022/790 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7574/2022-790.
- Kişisel Verileri Koruma Kurulunun 15.06.2023 tarihli ve 2023/1050 sayılı Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7769/2023-1050.
- Kişisel Verileri Koruma Kurulu'nun İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık) Konulu Kararı, Kişisel Verileri Koruma Kurumu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-.
- İlke Kararları, Kişisel Verileri Koruma Kurulu, Erişim Adresi: https://www.kvkk.gov.tr/Icerik/7201/ilke-kararlari






Adres: Nasuh Akar Mahallesi
1407. Sokak No: 4
Çankaya/ANKARA
Telefon: 0 312 216 50 00
Web: www.kvkk.gov.tr

kvkkurumu