

KİŞİSEL VERİLERİN KORUNMASI GENEL POLİTİKASI

1. AMAÇ

BV SAVUNMA VE HAVACILIK TİC. LTD. ŞTİ. [“ŞİRKET”] tarafından hukuka uygun bir biçimde yürütülen kişisel veri işleme faaliyeti ve kişisel verilerin korunmasına ilişkin idari ve teknik sistemler konusunda iş başvurusu yapan kişilerin, çalışanların, alt işveren çalışanlarının, şirket yöneticilerinin, ziyaretçilerin, tedarikçilerin ve müşterilerin kişisel verilerini korumak ve güvenliğini sağlamaktır.

2. KAPSAM

ŞİRKET'e iş başvurusu yapan adayları, çalışanları, alt işveren çalışanlarını, şirket yöneticilerini, ziyaretçileri, tedarikçileri ve müşterileri kapsar.

3. TANIMLAR

Kişisel Veri: Kimliği belirli ya da belirlenebilir nitelikteki gerçek bir kişiye ilişkin her türlü bilgidir. Örneğin bir gerçek kişinin; adı, soyadı, doğum tarihi ve doğum yeri, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri, müşteri şikâyet raporları, çalışan performans değerlendirme raporları, mülakat değerlendirme raporları, bordro, fatura, banka dekontları, kredi kartı ekstreleri, belgeler (nüfus cüzdanı fotokopileri, yazılar mektuplar, davet yazıları) gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler, kişisel veri olarak kabul edilmektedir.

Özel Nitelikli Kişisel Veri: İşlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına neden olma riski taşıyan verilerdir. Örneğin; Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı (her türlü tahlil sonucu, kişinin geçirdiği hastalıklar, kullandığı ilaçlar), cinsel hayatı, ceza mahkûmiyeti (sabıkası) ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verileridir.

Veri İşleyen: Veri sorumlusu adına verileri işleyen gerçek veya tüzel kişilerdir. Örneğin veri işleyen gerçek bir kişi olabileceği gibi veri sorumlusu adına faaliyet gösteren, dışarıdan hizmet alınması suretiyle hizmet sunan çağrı merkezleri, pazar araştırma şirketleri, kuryeler de olabilir.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Bu kişiler, gerçek kişiler olabileceği gibi, örneğin kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabilir.

Açık rıza: İlgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işleme sınırlı olarak verdiği onay beyanıdır.

Kişisel verinin 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 işlemidir. Örneğin, kişisel verilerin sadece bir Hard Disk'de, CD'de, Server'da depolanması, anılan verilerle başkaca hiçbir işlem yapılmısa da bir veri işleme faaliyetidir.

Veri kayıt sistemi: Veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sisteminin ifade etmektedir. Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Örneğin veri kayıt sisteminde kişisel verilerin; ad-soyad veya kimlik numarası üzerinden sınıflandırılması gibi. Otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse Kanun kapsamında değerlendirilmez.

4. SORUMLULUKLAR

Veri Sorumlusu: Kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbirleri almak zorundadır.

5. UYGULAMA

5.1. Veri Sorumlusu ve Veri İşleyen

Genel Olarak;

Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizzat kendileri "veri sorumlusu" olup, ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğacaktır. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemiştir. Bu çerçevede gerek cezai gerekse de hukuki sorumluluk bakımından, tüzel kişilerin sorumluluğuna ilişkin özel hukuk ve kamu hukukundaki genel hükümler uygulanır.

Veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiler olarak tanımlanmaktadır. Bu kişiler, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu hem de veri işleyen olabilir. Örneğin, bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

Veri işleyenin faaliyetleri veri işlemenin daha çok teknik kısımları ile sınırlıdır. Kişisel verilerin işlenmesine ilişkin kararların alınması yetkisi ise veri sorumlusuna aittir. Veri sorumlusu kişisel verilerin işleme amacını ve yöntemini belirleyen kişidir. Yani işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek kişidir.

Veri sorumlusunun tespiti için aşağıdaki hususlara kimin karar verdiği dikkate alınmalıdır:

- Kişisel verilerin toplanması ve toplama amacı,
- Toplanacak kişisel veri türleri,
- Toplanan verilerin hangi amaçlarla kullanılacağı,
- Hangi bireylerin kişisel verilerinin toplanacağı,
- Toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı,
- Verilerin ne kadar süreyle saklanacağı,
- Veri sahiplerinin erişim hakkı ve diğer haklarının uygulanıp uygulanmayacağı.
- Veri sorumlusu yapacağı kişisel veri işleme sözleşmesi ile, aşağıda örnek olarak belirtilen hususlarda karar verme yetkisini veri işleyene bırakabilir:
- Kişisel verilerin toplanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotların kullanılacağı,
- Kişisel verilerin hangi yöntemle saklanacağı,
- Kişisel verilerin korunması için alınacak güvenlik önlemlerinin detayları,
- Kişisel verilerin aktarımının hangi yöntemle yapılacağı,
- Kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot,
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemi.

5.2 Kişisel Verilerin İşlenmesinde Genel İlkeler

Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilmelidir.

Buna göre;

- Hukuka ve dürüstlük kurallarına uygunluk,

- Doğruluk ve güncellik,
- Belirli, açık ve meşru amaçlar için işlenmek,
- İşlendikleri amaçla bağlantılık, sınırlılık ve ölçülülük,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme, ilkelerine uygun olmalıdır.

5.2.1. Kişisel verilerin işleme şartları;

Kişisel veriler ancak aşağıda sıralanan şartlardan en az birinin varlığı halinde işlenebilir:

- Veri sahibinin açık rızasının varlığı,
- 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 işlenmesinin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

5.2.2 Özel nitelikli kişisel verilerin işleme şartları;

Özel nitelikli kişisel veriler aşağıdaki durumlarda işlenebilir. Veri sahibinin açık rızası bulunmaksızın özel nitelikli kişisel verilerin işlenmesi kural olarak yasaktır. Ancak sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmüş olması halinde işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından veri sahibinin açık rızası aranmadan işlenebilir.

Açık rıza dışında kişisel verilerin işleme şartları aşağıdaki gibidir.

İşleme Şartları	Kapsamı	Örnek
Kanun Hükmüne Dayanma	İş Mevzuatı, Vergi Mevzuatı, Ticaret Mevzuatı vb.	Çalışana ait özlük bilgilerinin 4857/m.75 gereği tutulması gerekir.
Sözleşmenin Gereği Olma	İş Sözleşmesi, Satış Sözleşmesi, Taşıma Sözleşmesi, Eser Sözleşmesi vb.	Çalışanlarla 4857/m.8 gereğince iş sözleşmesi imzalanması gerekir.
Fiili İmkânsızlık Durumunda	Fiili imkânsızlık nedeniyle rıza veremeyecek olan ya da ayırt etme gücü olmayan kişi.	Bilinci kapalı kişinin iletişim veya adres bilgisi. Kaçırılan bir kişinin konum bilgisi.
Veri Sorumlusunun Hukuki Sorumluluğu	İş ve Sosyal Güvenlik Mevzuatı Gereği Denetimler, Mali Denetimler	İş ve Sosyal Güvenlik Müfettişlerinin denetimlerde bilgi paylaşımı yapılması.

Aleniyet Kazandırılması Halinde	İlgili kişilerin kendilerine ait bilgilerin umumun bilgisine sunulması.	Kurumsal internet sitesinde, çalışanların işyeri telefon numaraları ve kurumsal elektronik posta adreslerinin üçüncü kişilerin erişimine açık şekilde paylaşılması
Hakkın Tesisi, Korunması, Kullanılması Durumunda	Dava açılması, tescil işlemleri, her türlü tapu işlemi vb. işlerde kullanılması zorunlu veriler.	İşten ayrılan işçilere ait gerekli bilgilerin dava zaman aşımı boyunca saklanması. (İhbar ve kıdem tazminatı ile ücret alacaklarında 5 yıl)
Veri Sorumlusunun Meşru Menfaati Halinde	Veri sahibinin temel haklarına zarar gelmemek kaydıyla, veri sorumlusunun meşru menfaati için zorunlu olması halinde veri işlenebilir.	Çalışan bağlılığını artıran ödül ve primler uygulanması amacıyla veri işlenmesi.

5.3. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ

Kişisel verilerin silinmesi; Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar tarafından erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel verilerin yok edilmesi; kişisel verilerin yok edilmesi, bilgilerin saklandığı veri saklamaya elverişli tüm fiziksel kayıt ortamlarının tekrar geri getirilemeyecek ve kullanılamayacak hale getirilmesidir. Veri sorumluları kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel verilerin anonim hale getirilmesi; Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Bu kapsamda, veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabilirse, bu verinin anonim hale getirildiği kabul edilemez.

5.3.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinin şartları;

- Verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir. Buna göre;
- Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- Kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması, hallerinde kişisel verilerin silinmesi, yok edilmesi ya da anonim hâle getirilmesi gerekir.

5.3.2. Kişisel Verilerin Anonimleştirilmesi

- Anonim hale getirme veya anonimleştirme, verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade etmektedir. Bu kapsamda, elde kalan veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabilirse, bu verinin anonim hale getirildiği kabul edilemez.
- Bu noktada dikkat çekilmesi gereken husus, anonim veri ve anonimleştirilmiş veri arasındaki farktır. Anonim veri belirli bir kişiyle ilişkilendirilmesi mümkün olmayan veriyi ifade ederken, anonimleştirilmiş veri daha öncesinde bir kişiyle ilişkilendirilmiş ancak artık bağlantısı kalmamış veridir.
- Anonimleştirme konusunda sıkça kullanılan bazı teknikler bulunmaktadır. Anonimleştirme uygulanırken, mevcut veri kümesinde yer alan verinin büyüklüğü, verinin çeşitliliği, veriden sağlanmak istenen fayda ve işleme amacı gibi özellikler dikkate alınarak uygulanacak tekniklere karar verilebilir.

Anonimleştirmeye ilgili bazı teknikler şunlardır:

Maskleme: Kişisel verilerin belli alanlarının silinerek veya yıldızlanarak kişinin belirlenemez hale getirilmesidir. Örneğin, kişinin kredi kartı numarasının bir kısmının yıldızlanması durumunda maskeme söz konusudur. (6698 **** * 0006)

Toplulaştırma/Kümülatif Data Yaratma: Verilerin kümülatif hale getirilerek toplam değerlerinin yansıtılmasını ifade eder. Örneğin, şirkette kadın çalışan sayısının Z adet olması ve sayının %40'ının üniversite mezunu, %60'ının yüksek lisans mezunu olmasına ilişkin veriler anonim hâle getirilmiştir.

Veri Türetme: Mevcuttaki detay verilerin daha genel karşılıklarıyla değiştirilmesidir. Örneğin, doğum tarihi bilgisinin Gün/Ay/Yıl detaylarının yerine kişinin direkt yaşının yazılması durumunda veri türetmek suretiyle anonimleştirme yapılmıştır.

Veri Karması: Veri kümesi içinde değerlerin karıştırılarak toplam faydaya zarar vermeden kişilerin tespit edilebilirlik özelliğinin yok edilmesini ifade eder. Yaş ortalaması alınmak istenen bir sınıfta kişilerin yaşlarını gösteren değerlerin birbirleriyle değiştirilmesi durumunda veri karması yapılmıştır.

5.3.3. Kişisel Verilerin Aktarılması

- Kişisel veriler kural olarak veri sahibinin açık rızası olmaksızın üçüncü kişilere aktarılamaz. Veri sahibinin açık rızası olmaksızın üçüncü kişilere aktarılabilmesi için verilerin aktarılacağı üçüncü kişilerin, kanunen kişisel verileri alma veya kaydetme yetkisine sahip kişiler olması gerekir.
- Veri sorumlusu sıfatına sahip bir tüzel kişiliğin bünyesinde gerçekleşen veri aktarımları, üçüncü kişiye yapılan aktarımlar olarak değerlendirilemez. Kişiler, kişisel verilerini bir tüzel kişi ile paylaştıklarında, bahsi geçen tüzel kişilik, veri sorumlusu sıfatına sahip olur.
- Tüzel kişiliğin bünyesinde faaliyet gösteren çalışanlar veya farklı birimler arasında verilerin el değiştirmesi, bu anlamda üçüncü kişiye aktarım şeklinde değerlendirilemez.
- Bir şirketler topluluğu altında yer alan farklı şirketler arasında, veri aktarımı gerçekleştirilmesi, üçüncü kişiye veri aktarımı yapılması anlamına gelir.

5.3.3.1. Kişisel verilerin yurt dışına aktarılması;

Kişisel veriler veri sahibinin açık rızası olmaksızın yurt dışına aktarılamaz. Ancak kişisel verilerin aktarılacağı yabancı ülkede, yeterli korumanın bulunması kaydıyla, ilgili kişinin açık rızası aranmaksızın yurt dışına aktarma yapılabilir. Şayet ilgili yabancı ülkede yeterli koruma bulunmuyorsa, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulunun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın kişisel veriler yurt dışına aktarılabilir.

Yabancı ülkelerde yeterli koruma bulunup bulunmadığı hususunda Kurul; Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle aşağıdaki ölçütlere göre karar verir.

- Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
- Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklık durumu,
- Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresi,
- Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulaması dikkate alınır.

5.4. Veri Sorumlusunun Yükümlülükleri

Veri sorumlusu "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Veri sorumlusu bir veri kayıt sistemini yöneten kişidir. Veri sorumlusu, kişisel verileri bizzat işleyebileceği gibi, veri işleme faaliyetini gerçekleştirmek üzere üçüncü bir kişiyi de yetkilendirebilir. Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen bu tür gerçek veya tüzel kişiler, "veri işleyen" olarak adlandırılır.

5.4.1. Veri Sorumlusunun Aydınlatma Yükümlülüğü

- Kanun koyucu kişisel verileri işlenen ilgili kişilere bu verilerinin kim tarafından, hangi amaçlarla ve hangi hukuki gerekçelere dayanılarak işlenebileceği, kimlere hangi amaçlarla aktarılacağı hususunda bilgi edinme hakkı tanımakta ve bu hususları, veri sorumlusunun aydınlatma yükümlülüğü kapsamında ele almaktadır. Buna göre veri sorumlusu, 6698 sayılı Kanunun 10. maddesi çerçevesinde kişisel verilerin elde edilmesi sırasında bizzat veya yetkilendirdiği kişi aracılığıyla aşağıdaki bilgileri veri sahibine sağlamakla yükümlüdür:
- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılacağı,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Veri işleme faaliyetinin ilgili kişinin açık rızasına bağlı olduğu ve faaliyetin Kanundaki başka bir şart kapsamında yürütüldüğü durumlarda da veri sorumlusunun ilgili kişiyi bilgilendirme yükümlülüğü devam etmektedir. Veri sahibi, kişisel verisinin işlendiği her durumda aydınlatılmalıdır.
- Aydınlatma yükümlülüğünü yerine getirirken ilgili kişiye verilecek bilgiler, veri sorumlusu sicilinde açıklanan bilgilerle uyumlu ve kategorik bazda olmalıdır.
- Aydınlatma yükümlülüğünün yerine getirilmesi konusu, ilgili kişinin onayına tabi değildir. Tek taraflı bir beyanla aydınlatma yükümlülüğü yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir.

5.4.2. Veri Sorumlusunun Veri Güvenliğine İlişkin Yükümlülükleri

- Kanun koyucu kişisel verilerin hukuka aykırı olarak işlenmesini önleme, bu verilere hukuka aykırı olarak erişilmesini önleme ve bunların hukuka uygun olarak muhafazasını sağlama yükümlülüklerinin tamamını kapsayan veri güvenliğini sağlama ödevi, veri sorumlusuna aittir.
- Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
- Veri sorumlusu, "niçin" kişisel veri işliyoruz ve kişisel verileri "nasıl" işleyeceğiz sorularını cevaplamakla yetkili olan gerçek veya tüzel kişidir.
- Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi halinde, 6698 sayılı Kanun 15.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası öngörmektedir.
- Veri güvenliğine ilişkin alınacak önlemlerin her bir veri sorumlusunun yapısına, faaliyetlerine ve tabi olduğu risklere uygun olması gerekir.
- Veri sorumlusunun denetim yükümlülüğünün ve veri sorumlusu organizasyonu içerisinde veri işleme konusunda görevlendirilen kişilerin sır saklama yükümlülüğü vardır.
- Verilerin yasal olmayan yollarla ifşası veya ele geçirilmesi noktasında veri sorumlusunun hem Kişisel Verileri Koruma Kurumuna hem de veri sahibine karşı yükümlülükleri vardır.
- Veri sorumlusu; Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

- Kişisel verilerin muhafazasını sağlamakla yükümlüdür.
- Veri sorumlusu bu yükümlülüklerini yerine getirmek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

5.4.3. Veri Güvenliğinin Sağlanmasında Müşterek Sorumluluk

- 6698 sayılı Kanuna göre, verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, gerekli tedbirlerin alınması hususunda veri sorumlusu, bu kişilerle birlikte müştereken sorumludur.
- Veri sorumlusu, veri işleyenler de veri güvenliğinin sağlanması için tedbir alma yükümlülüğü altındadır. Örneğin veri sorumlusunun şirketine ilişkin kayıtlar bir muhasebe şirketi tarafından tutuluyorsa, verilerin işlenmesine ilişkin birinci fıkrada belirtilen tedbirlerin alınması hususunda veri sorumlusu muhasebe şirketiyle birlikte müştereken sorumlu olacaktır.

5.4.4. Veri Sorumlusunun Denetim Yapma veya Yaptırma Yükümlülüğü

- 6698 sayılı Kanuna göre, veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlama ve kişisel verilerin Kanunda öngörülen usul ve esaslara uygun olarak işlenmesi amacıyla gerekli denetimleri yapma veya yaptırma yükümlülüğü vardır.
- 6698 sayılı Kanun, denetimin veri sorumlusu tarafından yapılması gerektiğini öngörmektedir. Veri sorumlusu bu denetimi kendisi gerçekleştirebileceği gibi, bir üçüncü kişi vasıtasıyla da gerçekleştirebilir.

5.4.5. Veri Sorumlusunun Sır Saklama Yükümlülüğü

- 6698 sayılı Kanuna göre, veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğü bulunmaktadır.
- Veri sorumluları ile veri işleyenlerin öğrendikleri kişisel verileri, Kanuna aykırı olarak başkalarına açıklamaları veya işleme amacı dışında kullanmaları yasaktır.
- Bu yükümlülük veri sorumluları ve veri işleyenlerin görevlerinden ayrılmalarından sonra da devam etmektedir.

5.4.6. Veri Sorumlusunun İhlal Halinde Bildirim Yükümlülüğü

- 6698 sayılı Kanuna göre, işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirmekle yükümlüdür.
- Veri ihlali, işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesidir. Örneğin; hizmet sağlayıcısının bilgisayar sisteminde bulunan müşterilere ait kişisel verilere, güvenlik ihlalleri nedeniyle internet aracılığıyla üçüncü kişiler tarafından erişilmesi, veri sorumlusunun veya veri işleyeninin müşterilerine ait kişisel verilerin bulunduğu USB anahtarı veya CD-ROM'unun çalınması, özel nitelikli kişisel verilerin yer aldığı sabit diskin silinmeden internet üzerinden satılması gibi.

5.4.7. Veri Sorumlusunun İlgili Kişiler Tarafından Yapılan Başvuruları Cevaplaması ve Kurul Kararlarını Yerine Getirmesi Yükümlülüğü

- 6698 sayılı Kanuna göre veri sorumluları, veri sahipleri tarafından yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle kendisine iletilen Kanunun uygulanmasıyla ilgili talepleri, niteliklerine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırmalıdır.
- Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, veri sorumlusu, Kurulca belirlenen tarifedeki ücretleri başvuruda bulunan veri sahibinden isteyebilir. Veri sorumlusu, talebi kabul eder ise veya gerekçesini açıklayarak reddeder ise bu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusu tarafından bu talebin gereği yerine getirilir. Başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde ise alınan ücret ilgiliye iade edilir.
- Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetinde bulunabilir.

- Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda yapacağı inceleme sonucunda bir ihlalin varlığını tespit ederse, hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek, kararı ilgililere tebliğ eder. Veri sorumlusu, bu kararı, tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirmek zorundadır.

5.4.8. Veri Sorumluları Siciline Kaydolma Yükümlülüğü

- 6698 sayılı Kanuna göre, Kişisel Verileri Koruma Kurumu tarafından kamuya açık olacak şekilde bir Veri Sorumluları Sicili tutulacaktır.
- Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce bu Sicile kaydolmak zorundadır.
- Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından Veri Sorumluları Siciline kayıt zorunluluğuna istisnalar getirilebilecektir.

5.5. VERİ İŞLEYENİN YÜKÜMLÜLÜKLERİ

- Veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir. Bu kişiler, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişidir. Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu hem de veri işleyen olabilir.
- Veri işleyen kişilerin temel yükümlülüğü; öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklamama ve işleme amacı dışında kullanmamadır. Bu yükümlülük, veri işleyen görevinden ayrılmasından sonra da devam etmektedir.
- Ayrıca, kişisel verilerin veri sorumlusu adına veri işleyen tarafından işlenmesi hâlinde, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınması hususunda veri işleyen veri sorumlusu ile birlikte müştereken sorumludur.

5.6. VERİ SAHİBİNİN VERİYE ERİŞİM HAKKI

- 6698 sayılı Kanununun 11 inci maddesine göre ilgili kişilerin, veri sorumlusuna başvurarak; kendileriyle ilgili kişisel verilerin işlenip işlenmediğini öğrenmek, işlenmişse bunları talep etmek, verinin muhtevasının eksik veya yanlış olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini ve verilerin kanuna aykırı olarak işlenmesi sebebiyle zararlarının giderilmesini talep etme hakları bulunmaktadır.
- Bu kapsamda ilgili kişilerin, Kanunun uygulanmasıyla ilgili taleplerini, öncelikle veri sorumlusuna iletmeleri zorunludur. Kanun, kişisel verilerin korunması kapsamındaki başvurular için kademeli bir başvuru usulü öngörmüştür. İlgili kişilerin, sahip oldukları hakları kullanabilmeleri için öncelikle veri sorumlusuna başvurmaları zorunludur. Bu yol tüketilmeden Kurula şikâyet yoluna gidilemez. İlgili kişinin talebinin 30 gün içerisinde veri sorumlusu tarafından cevaplandırılması gerekmektedir. Başvurusu reddedilen veya verilen cevabı yetersiz bulan yahut süresinde başvurusuna cevap verilmeyen ilgililer Kurula şikâyet hakkını kullanabilir.
- Kişilik hakları ihlal edilen ilgililerin genel hükümlere göre tazminat hakları saklıdır. Başvuru yoluna gitmenin zorunlu, şikâyet yoluna gitmenin ise ihtiyari olması sebebiyle, başvurusu zımnen veya açıkça reddedilen ilgili kişinin bir yandan Kurula şikâyette bulunabilmesi, diğer yandan doğrudan adli veya idari yargı yoluna gidebilmesi mümkün olacaktır. Ancak bu noktada belirtmek gerekir ki, ilgili kişilerin hak ihlallerine yönelik olarak doğrudan yargı organlarına başvurularının önünde herhangi bir engel bulunmamaktadır. Konunun yargıya intikal ettirilmesinden önce, veri sorumlusuna başvuru zorunluluğu bulunmamaktadır. Veri sorumlusuna doğrudan başvurma zorunluluğu, konunun Kurula iletilmesinden önce uyulması gereken bir zorunluluktur.

5.7. KİŞİSEL VERİLERİN KORUNMASINDA İNSAN KAYNAKLARI DEPARTMANI TARAFINDAN YERİNE GETİRİLMESİ GEREKEN HUSUSLAR

- İşyerinde Kişisel Veri Kayıt Sistemi kurulmalı,
- Kişisel verilerin korunmasıyla ilgili politika oluşturulmalı,
- Veri sorumlusu görevlisi ile irtibat kişisi şirket yönetim kurulunca görevlendirilmeli,
- Veri Sorumlusu, Veri Sorumluları Siciline kaydolmalı,
- Veri Envanteri hazırlanmalı,
- Veriler tanımlanmalı ve sınıflandırılmalı,
- Veri işleyen birimler belirlenmeli,
- Veri işleyen kişiler belirlenmeli ve konuyla ilgili eğitilmeli,
- Veri işleyenlerin her biri ile gizlilik sözleşmesi imzalanmalı,
- Verilerin saklama süreleri ve imha politikası belirlenmeli,
- Kamera İzleme Politika Belgesi Hazırlanmalı.
- Manuel ya da elektronik ortamdaki kaydedilen ve saklama süresi dolan verilerin, silinmesi, yok edilmesi veya anonim hale getirilmesi sağlanmalı,
- İnsan Kaynakları Departmanına giriş/çıkışlar kontrol altına alınmalı,
- İşçi özlük dosyaları yeniden gözden geçirilerek gereksiz belgeler çıkarılmalı,
- Özlük dosyaları kilit altında tutulmalı,
- İş başvuru formları işyeri güvenlik noktasında alınıyorsa, kapalı bir kutuya bırakılması sağlanmalı ve insan kaynakları işe alım sorumlusu tarafından her gün kilitli kutudan formlar alınmalı,
- İş sözleşmesi, İş başvuru formu, oryantasyon, işyeri iç yönetmeliği, disiplin yönetmeliği incelenerek kişisel verilerin korunması kapsamında revize edilmeli,
- İşe alım ve eleme sürecinde yer alan çalışanların eğitimi sağlanmalı,
- İşe alım sürecinde adaylar kişisel bilgilerini kime ilettiklerini bilmeli, bu yüzden işe başvuru ilanında kurum adı açıkça belirtilmeli,
- Elde edilen kişisel veriler yalnızca işe alım ve eleme amacıyla kullanılmalı,
- Adaylardan ihtiyaçtan fazla bilgi talep edilmemeli,
- Belli pozisyonlar için talep edilmesi gereken kişisel veri diğer pozisyonlara başvuran adaylardan talep edilmemeli,
- Elde edilen kişisel veriler güvende tutulmalı ve paylaşılmamalı,
- Elde edilen kişisel veriler ihtiyaç olduğu sürece saklanmalı,
- Arşiv bölümü yeniden düzenlenmeli ve arşiv yetkilisi dışında girişler engellenmeli,
- Arşive giriş ve çıkışlar kartlı sistem ile yapılmalı,
- İşyerinin tüm tedarikçileri ve müşterileriyle gizlilik sözleşmesi imzalanmalı, imzalanan sözleşmeler kişisel verilerin korunması kanunu yönünden revize edilmeli,
- Güvenlik girişinde elde edilen kimlik bilgilerinin güvenliğini sağlayacak idari ve teknik tedbirler alınmalı,
- Güvenlik personeli kişisel verilerin korunması kanunu kapsamında eğitilmeli,
- Güvenlik girişinde kimlik bilgisi alınan kişiler, kişisel verilerinin güvende olduğu ve hukuka aykırı olarak başkalarıyla paylaşılmayacağı yönünde bilgilendirilmeli,

5.8. İNSAN KAYNAKLARI DEPARTMANINDA ÖZLÜK DOSYASINDA BULUNMASI GEREKEN BELGELER

- İş Sözleşmesi, İşe giriş-ayrılış bildireleri,
- Kimlik fotokopisi, Adres bilgileri, Aile durum bildirimleri,
- Sağlık raporu, Öğrenim belgesi,
- Varsa özel sağlık durumunu gösteren belge,
- Askerlik durumunu gösterir belge,
- Fazla çalışma onayı, Çalışma belgesi,
- İşçiye yapılan bildirimler, savunma yazıları, disiplin kurulu kararları,
- Yıllık izin defteri düzenlenmiyorsa, izin kartları ya da formları,
- İş sözleşmesinin feshinde tazminat bordroları ve diğer ödeme belgeleri
- İşçilerin İSG Eğitimine ilişkin belgeleri,
- Performans değerlendirmeleri,
- Engelli çalışanların sağlık raporları ve İş Kurumu yazışmaları

5.9. İŞYERİNDE BİLGİ GÜVENLİK YÖNETİM SİSTEMİNİN OLUŞTURULMASI İÇİN BİLGİ İŞLEM DEPARTMANI TARAFINDAN YERİNE GETİRİLMESİ GEREKEN HUSUSLAR

- İşyerindeki kişisel bilgisayarlar 5 dakika içinde müdahale edilmezse otomatik kilitlenir hale getirilmeli,
- Kullanıcı şifreleri belirli periyodlarla değiştirilmeli,
- Kişisel bilgisayarlar ve donanımları ilgili kullanıcılara zimmetlenmeli,
- Bilgisayarlara şahsi USB takılması engellenmeli,
- Şirkete kişisel bilgisayar getirilmesi ya da şirketten dışarı çıkarılması özel izne tabi tutulmalı.
- Şirkete ait bilgisayarların dışarı çıkarılması halinde internet bağlantı güvenliği sağlanmalı,
- Uzaktan bağlantı yapan kullanıcıların kontrolleri sağlanmalı,
- Dışarıdan gelen bilgisayar, tablet, cep telefonu, USB flash disk gibi virüs taşıyabilecek elektronik cihazlar taranmalı ve güvenilirliği sağlanmalı,
- Veriler sınıflandırılmalı ve sınıflandırılan verilerin şirket içi ve şirket dışına gönderilmesi engellenmeli/sınırlandırılmalı,
- Kişisel verileri görebilecek kişilerin yetki sınırları belirlenmeli,
- Ekran görüntüleri saklanmalı ve kullanıcı risk seviyesi belirlenmeli,
- Veri erişimleri şirket içinde ve dışında kısıtlanmalı ve belirli süre erişimli dosyalar oluşturulmalı,
- Sistem ve Network Kırılganlık ve Zafiyet Analizi yapılmalı,
- Sızma Testi Yapılmalı,
- Veriler güvenli bir biçimde yedeklenmeli,
- Bilgi sızmaları ve Güvenlik Önlemleri için LOG Yönetimi sağlanmalı,
- Şirket bilgisayarlarında iş dışında internet erişimi sınırlandırılmalı,
- Şirket bilgisayarında özel mail kullanımının sınırlandırılması
- İşyerinde iş süreleri içinde cep telefonu kullanımı yasaklanmalı,
- İşyerinde elektronik gözetleme sonucu elde ettiği bilgilerin belirli bir süre sonra silinmesi sağlanmalı,
- Elektronik cihazların işyerinde yerleştirildiği yerler ile ilgili çalışanlar bilgilendirilmeli,
- Elektronik cihazların yerleştirildiği yerlere bilgilendirme levhalarının asılması,
- Elektronik gözetleme doğrudan çalışanlara değil işyerine yönelik olarak yapılmalı,
- Çalışanlar elektronik gözetlemeyle ilgili gözetlemenin amacı, kapsamı, zamanı, çeşidi ve metodu hakkında bilgilendirilmeli,
- Çalışanların telefon konuşmaları ve e-mail üzerinden denetimleri yapılırken kişisel verilerin korunması kanunu gözetilmeli,
- İşverenin çalışanı gözetlemesinde gözetleme amacı iş sözleşmesi ya da iş ilişkisi ile ilgili olmalı,
- İşyerine giren çıkan müşteriler, tedarikçiler, alt işverenler ve ziyaretçilerin kimlik bilgilerinin ayrı bir modülde kontrol altına alınmalıdır.

6698 Sayılı Kişisel Verilerin Korunması Kanun'u kapsamındaki haklarınızdan yararlanmak ve detaylı bilgi almak amacıyla internet sitemizde yer alan Veri Sahibi Başvuru Formu'nu doldurarak bizlerle paylaşabilirsiniz.