

1. AMAÇ

ADO Grup şirketlerinde, “**Kişisel Verilerin Korunması Kanunu**” ve buna bağlı alt yasal düzenlemelere uygun şekilde; kişisel verilerin korunması ve işlenmesinde izlenecek usul ve esasların belirlenmesi.

2. TEMEL İLKELER

- 2.1. Kişisel verilerin korunması (KVK) ve işlenmesinde işbu politika ve “**Kişisel Verilerin Korunması Kanunu**” ile bu kanuna bağlı çıkartılan diğer yasal düzenlemelerde belirtilen hükümler esas alınır.
- 2.2. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgiyi kapsar. Özel nitelikli kişisel veri; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik bilgileridir.
- 2.3. Kişisel veriler, “**Yetki Listesi**”nde belirtilen, Kurumun belirlemiş olduğu lokasyon/bölüm ve sistemlerde saklanır. Kişisel verilerin işlenmesi, verilere erişim ve bu verilerin kullanımı sadece yetkilendirilmiş kişilerce yapılır.
- 2.4. Kişisel verilerin korunması anayasal bir hak olup, Şirketimizin öncelikleri arasında yer almaktadır. Bu amaçla; kişisel verilerin korunması süreçlerinin yönetimi, gelişmelerin takibi ve analizi amacıyla Şirket bünyesinde “**Kişisel Verilerin Korunması Komitesi**” (Komite) kurulmuştur. Komite çalışma esasları ve usullerine işbu politikanın 3.1.3. başlığı altında detaylı bir şekilde yer verilmiştir.
- 2.5. İşbu politikada belirtilen hususların uygulanmasına yönelik Şirket bünyesinde gerekli prosedürler oluşturulmuş, aydınlatma metinleri düzenlenmiş, gizlilik sözleşmeleri yapılmış, görev tanımları revize edilmiş, kişisel verilerin korunması için gerekli idari ve teknik tedbirlerin tamamı alınmıştır.
- 2.6. ADO Grup çalışanları, ADO’nun iş ilişkisi içinde olduğu tedarikçiler, müşteriler, potansiyel müşteriler ve ziyaretçilere ait “**özel nitelikli kişisel veriler**”, “**Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Prosedürü**”nde belirtilen esaslar dahilinde Şirketimiz tarafından korunur ve işlenir. (PR.YNT.00.001)
- 2.7. Kişisel veriler, veri sahibinin açık rızası olmadan işlenemez, başka bir kişiye/sisteme aktarılamaz, kullanılamaz ve sunulamaz. Kişinin açık rızası; açık, bilgilendirmeye ve özgür iradeye dayalı bir biçimde alınmaktadır.
- 2.8. İşbu politikada belirtilen esaslara ve yasal mevzuata aykırı olarak kişisel verileri kaydeden, paylaşan ve/veya gerektiğinde silmeyen kişilere Türk Ceza Kanunu’nun (TCK) 135-140. maddelerinde belirtilen hususlar gereği ve ayrıca Şirket Disiplin Kurulu kararları uygulanır.
- 2.9. Tüm ADO çalışanları, kişisel verilerin korunması ve güvenliğinden bizzat sorumludur.
- 2.10. KVK Kanunu ile buna bağlı diğer yasal düzenlemelere ve işbu politikaya uyum konusunda İç Denetim Birimi tarafından “**Denetim Sistemleri Faaliyetleri Prosedürü**”nde belirtildiği şekilde periyodik olarak denetim yapılır.

3. UYGULAMA ESASLARI

3.1. KİŞİSEL VERİLERİN GİZLİLİĞİ VE GÜVENLİĞİNİN SAĞLANMASI

KVK Kanunu’na uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere erişilmesini önlemek ve verilerin doğru şekilde muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik işbu politikada 3.1.1. ve 3.1.2. alt başlıkları altında belirtilen tüm teknik ve idari tedbirleri Şirketimiz almış olup, bu kapsamda gerekli kontrol ve denetimleri yapmaktadır.

3.1.1. Teknik Tedbirler

- 3.1.1.1. Şirketimizde, kişisel verilerin korunması ve güvenli şekilde işlenmesi amacıyla her türlü teknik güvenlik önlemleri alınmış olup olası risklere karşı üst seviye koruma

Hazırlayan Kişisel Verilerin Korunması Komitesi	Kontrol Denetim Sistemleri Direktörü	Onay Yönetim Kurulu Başkanı
---	--	---------------------------------------

sağlanmaktadır. Alınan tüm teknik tedbirler Bilgi Teknolojileri Bölümü tarafından yerine getirilmektedir.

3.1.1.2. Kişisel veri içeren bilgi teknolojileri sistemlerinde hem içeriden hem de dışarıdan gelen saldırılara, siber suçlara veya kötü amaçlı yazılımlara maruz kalmamak adına aşağıda belirtilen aksiyonlar alınmaktadır:

- Tüm kullanıcıların kişisel veri içeren yazılımlardaki işlem hareket kayıtları düzenli olarak tutulur. (Log kayıtları)
- Yıllık periyotta yapılan penetrasyon testleri (sızma) ile kişisel verilerin saklandığı alanlara erişimin güvenliği kurum dışı bağımsız bir uzman kuruluşa test ettirilir ve neticesinde var ise uygunsuzluk ve/veya açıklıklar kapatılır.
- Güvenlik yazılım mesajları, erişim kontrol kayıtları ve diğer raporlama araçları sürekli kontrol edilir.
- Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olayların yaşanması halinde deliller toplanarak güvenli bir şekilde saklanır.
- Güvenlik sorunlarının tespiti halinde ivedilikle üst yönetime ve sürecin tarafı olan danışman firmaya rapor gönderilir.
- Kişisel verilerin yer aldığı serverların (sunucuların) bulunduğu fiziksel ortamlar dış tehditlere (yangın, deprem vb.) karşı uygun yöntemlerle korunur ve giriş/çıkışlar kameralar ile kayıt altına alınır.
- Personle sistem ve/veya servislerde güvenlik açıklıkları ve zafiyetleri konularında sık sık bilgilendirme e-postaları gönderilir.

3.1.1.3. Güvenlik duvarlarını içeren yazılımlar ve virüs koruma sistemleri kullanılmaktadır.

3.1.1.4. Kişisel verilerin güvenli ortamlarda saklanması için teknolojik gelişmelere uygun sistemler kullanılmaktadır. Saklanma alanlarına yönelik alınan teknik önlemlerde, risk teşkil eden hususlar periyodik olarak değerlendirilmekte ve gerekli teknolojik çözüm üretilmektedir.

3.1.1.5. Elektronik ortamda yer alan kişisel verilere erişim "**Erişim Yetkilendirme Listesi**"nde belirtildiği gibi yapılmaktadır.

3.1.1.6. Kişisel verilere erişim imkanı sağlayan sistemler üzerinde daima yetki erişim kontrolleri yapılmaktadır.

3.1.1.7. Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması riskine karşı veri sorumlularının periyodik olarak yedek alınması sağlanmaktadır.

3.1.1.8. Veri işleme konusunda yeterli teknik bilgiye sahip uzman kişiler istihdam edilmektedir.

3.1.1.9. Teknolojik gelişmeler yakından takip edilerek, akabinde mevcut sistemler güncellenmekte ve gerekli önlemler alınmaktadır.

3.1.2. İdari Tedbirler

3.1.2.1. Kişisel verilerin korunması ve en güvenli şekilde işlenmesi amacıyla Şirket bünyesinde her türlü idari tedbir alınmaktadır.

3.1.2.2. Kişisel verilerin güvenliğinin sağlanması ve korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığı ve gerçekleşmesi durumunda yol açacağı kayıplar doğru bir şekilde belirlenerek buna uygun tedbirler alınmaktadır. Risk ve tehditler belirlenirken aşağıdaki hususlar dikkate alınır:

- Kişisel verilerin özel nitelikli veri olup olmadığı,
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği,
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği.

- 3.1.2.3.** Riskler ve tehditler tanımlandıktan sonra riskleri azaltma, ortadan kaldırma vb. yönelik tüm alternatif kontrol sistemleri ve çözüm yolları maliyet, uygulanabilirlik ve yararlılık ilkeleri gözetilerek değerlendirilmekte ve "**Risk Yönetimi Prosedürü**"ne göre risk işleme seçenekleri uygulanmaktadır.
- 3.1.2.4.** Kişisel verilerin korunması ve işlenmesi hususlarında iş birimleri bazında gerekli iç kontrol sistemleri kurulmaktadır.
- 3.1.2.5.** Şirket personeline, KVK Kanunu'na uyum, kişisel verilerin hukuka aykırı erişimi vb. konularında sürekli eğitim verilmekte ve bilgilendirme çalışmaları yapılmaktadır.
- 3.1.2.6.** Şirketimiz tarafından kişisel verilerin işlenmesi, saklanması, korunması konularında idari veya teknik gereklilikler sebebiyle dışarıdan hizmet alınması söz konusu olduğunda; kişisel verilerin aktarıldığı taraf ile, verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasının sağlanacağına ilişkin hükümlere sözleşmelerde yer verilmekte ve KVK Kanunu uyarınca kişisel verilerin güvenliği ve korunması amacıyla bu sözleşme imzalanmaktadır.
- 3.1.2.7.** KVK hususlarının yer aldığı dokümanlarda (prosedür, sözleşme, taahhütname, şartname vb.) işbu politika ve KVK Kanunu dışında kişisel verileri işlememe, ifşa etmeme ve kullanmama yükümlülükleri yer almaktadır.
- 3.1.2.8.** Çalışanların dahil oldukları ve/veya öğrendikleri kişisel veriler ile 3. taraflara açıklamayacağı, işleme amacı dışında kullanmayacağı, bu yükümlülüğün işten ayrıldıktan sonra da devam edeceği ve güvenli ortamlarda saklanacağı hususlarında bilgilendirme yapılmakta ve gerekli önlemler alınmaktadır.
- 3.1.2.9.** Fiziksel ortamda yer alan kişisel verilere erişim, "**Erişim Yetkilendirme Listesi**"nde belirtildiği şekilde yapılmaktadır.

3.1.3. Kişisel Verilerin Korunması Komitesi Faaliyetleri

- 3.1.3.1.** Şirket bünyesinde kişisel verilerin korunması konusundaki çalışmalarını yönetmek üzere, "**Kişisel Verilerin Korunması Komitesi**" kurulmuştur. Komite üyeleri; Yönetim Kurulu Başkanı (YKB), Bilgi Teknolojileri Grup Başkan Yardımcısı, Başkanlık Ofisi Direktörü, Hukuk Müşaviri, İnsan Kaynakları/İdari İşler Direktörü ve Denetim Sistemleri Direktörü'nden oluşmaktadır. Komite başkanı, Bilgi Teknolojileri Grup Başkan Yardımcısıdır. Yönetim Kurulu Başkanı'nın (YKB) katıldığı toplantılarda, Komiteye YKB başkanlık eder.
- 3.1.3.2.** Komitede kararlar oy çokluğu ile alınır. Eşitlik olması halinde Komite Başkanı'nın kararı esas alınır. Denetim Sistemleri Direktörü'nün oy hakkı bulunmamaktadır.
- 3.1.3.3.** Komite, aylık periyotta toplanır. Bunun dışında, komite üyelerinden birinin talebi ve/veya olağan dışı bir durum olması halinde komite hemen toplanabilir.
- 3.1.3.4.** Komite'nin görevleri aşağıdaki şekilde belirtilmiştir:
- Kişisel verilerin korunması ve işlenmesi ile ilgili dokümantasyon ihtiyacını belirlemek ve gerektiğinde değişiklikleri veya revizyon çalışmalarını yapmak,
 - KVK Kanunu ve ilgili mevzuata uyumun sağlanması için yapılması gereken hususları tespit etmek ve üst yönetimin onayına sunmak,
 - Kişisel verilerin korunması ve işlenmesine ilişkin politikaların uygulanması ve denetimlerin ne şekilde yerine getirileceğine karar vermek ve bu çerçevede şirket içi görevlendirmede bulunma ve koordinasyonu sağlama hususlarını üst yönetimin onayına sunmak,
 - Kişisel verilerin korunması ve işlenmesi konusunda Şirket içerisinde ve ADO Grubun iş ilişkisi içerisinde olduğu kurumlar nezdinde farkındalığı arttırmak,
 - Kişisel veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını sağlamak; iyileştirme önerilerini üst yönetimin onayına sunmak,

- Kişisel verilerin korunması, aktarılması ve politikaların uygulanmasında kişisel veri sahiplerinin; veri işleme faaliyetleri ve kanuni hakları konusunda bilgilendirilmelerinin sağlanması yönünde eğitimler düzenlenmesini sağlamak,
- Kişisel veri sahiplerinin bilgi talebi, veri silinmesi ve saklanması gibi hususlardaki taleplerini almak ve Üst Yönetime iletmek,
- Başbakanlığa bağlı Kişisel Verilerin Korunması Kurumu'nca (KVK Kurumu) bildirilen, yayımlanan kişisel verilerin korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak Şirket içinde alınması gereken aksiyonları belirlemek ve Üst Yönetime iletmek,
- Kişisel verilerin korunması konusunda yaşanan sorunları KVK Kurumu'na bildirmek ve gelen geri dönüşler paralelinde aksiyonlar almak,
- Yönetim Kurulu Başkanı'nın kişisel verilerin korunması konusunda vereceği diğer görevleri icra etmek.

3.2. KİŞİSEL VERİLERİN İŞLENMESİ

3.2.1. Kişisel Verileri İşleme Usulleri

3.2.1.1. KVK Kanunu'nun 3. maddesinde belirtildiği üzere, 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem, kişisel verilerin işlenmesi kapsamına girmektedir.

3.2.1.2. Şirketimiz; kişisel verilerin işlenmesinde hukuksal düzenlemelerle getirilen ilkeler (Anayasa'nın 20. maddesi ve KVK Kanunu'nun 4. maddesi) ile güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda, kişisel veriler;

- Şirketimizin insan kaynakları politikalarının yürütülmesi doğrultusunda işbu politikaya uygun şekilde; personel temini, insan kaynakları operasyonlarının yürütülmesi, (özlük, bordrolama süreçleri, kariyer yönetimi, eğitim faaliyetleri vb.) iş sağlığı ve güvenliği çerçevesinde yükümlülüklerin (sağlık verileri) yerine getirilmesi ve gerekli tedbirlerin alınması,
- Şirketimizin tüzel/gerçek kişilerle olan ticari ve iş stratejilerinin belirlenmesi ve uygulanması doğrultusunda; Şirketimiz tarafından yürütülen satış (talep, sipariş, bütçelendirme, sözleşme) ve satın alma operasyonları (teklif, değerlendirme vb.), muhasebe ve finans operasyonları, kalite süreçleri, iletişim ve sosyal sorumluluk aktivitelerinin yürütülmesi,
- İlgili mevzuat hükümlerine göre Şirketimizden veri (bilgi, belge vb.) almaya yetkili kamu ve kamu tüzel kişiliğine sahip kuruluşlarla faaliyetlerin yürütülmesi,
- Yukarıdaki maddeler ile sınırlı kalmamak koşuluyla Ado Grup aydınlatma metnindeki 3. madde altında bahsi geçen faaliyetlerin yürütülmesi,

amacıyla işlenmektedir.

3.2.1.3. ADO bünyesinde yürütülen her süreç/bölüm bazında ayrı ayrı analiz edilerek kişisel veri işleme faaliyetleri ortaya konulmaktadır.

3.2.1.4. İşbu politika ile kişisel verilerin işlenmesinde aşağıdaki temel ilkeler benimsenmiştir:

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve güncel olmasını sağlama,
- Belirli, açık ve meşru amaçlar için işleme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme,
- Kişisel veri işlenmesi öncesi, veri sahiplerini aydınlatma ve bilgilendirme,
- Kişisel veri sahiplerinin haklarını kullanması için gerekli sistemleri kurma,
- Kişisel verilerin muhafazasında gerekli tedbirleri alma,
- Kişisel verilerin işleme amacının gereklilikleri doğrultusunda 3. kişilere aktarılmasında mevzuata ve KVK Kurumu düzenlemelerine uygun davranma,
- Özel nitelikli kişisel verilerin işlenmesi ve korunmasında gereken hassasiyeti gösterme.

3.2.1.5. Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Aşağıda belirtilen şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel veriler işlenebilir:

- Kanunlarda açıkça öngörülmesi,
- Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Kurumun ticari anlamda geçersiz olması, tanınabilirliğinin yok olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Kişisel verinin, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Kişisel verinin, ilgili kişi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- Şirketimizin hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu olması,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

3.2.1.6. Kişisel verilerin işlenmesi hususlarında ADO çalışanlarına yönelik, KVK Kanunu ve buna bağlı yönetmelikler kapsamında; veri güvenliği konularında düzenli olarak eğitimler verilmekte, gizlilik sözleşmeleri yapılmakta, verilere erişim yetkisine sahip kullanıcıların yetki kapsamı ve süreleri net olarak tanımlanmakta ve periyodik olarak yetki kontrolleri yapılmaktadır. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri eşanlı kaldırılmaktadır.

3.2.2. Özel Nitelikli Kişisel Verilerin İşlenmesi

3.2.2.1. KVK kanununun 6. maddesinin 1. fıkrasına göre özel nitelikli kişisel veriler; 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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik bilgilerinden oluşmaktadır.

3.2.2.2. Şirketimizde “**özel nitelikli**” olarak belirlenen kişisel veriler, KVK Kanunu’nun 6. maddesinin 2. fıkrasında belirtildiği şekilde, “**ilgili kişinin açık rızası olmaksızın işlenemez**”.

Ancak, aynı maddenin (6. madde) 3. fıkrasında belirtildiği üzere; sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise; ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

3.3. KİŞİSEL VERİLERİN AKTARILMASI

3.3.1. Genel kural olarak kişisel veriler ilgili kişinin açık rızası olmaksızın aktarılamaz. Ancak, KVK Kanunu'nun 8. maddesine göre; KVK Kanunu'nun 5. maddesinin 2. fıkrası (işbu politika **3.2.1.5.** maddesi) ve 6. maddesinin 3. fıkrasında (işbu politika **3.2.2.2.** maddesi) belirtilen şartların bulunması halinde yeterli korumanın olması kaydıyla, açık rıza aranmaksızın kişisel veriler aktarılabilir.

3.3.2. Aynı zamanda, kişisel verilerin yurtdışına aktarılmasında; **3.3.1.** maddesinde belirtilen hususlar geçerli olup ayrıca KVK Kanunu'nun 9. maddesinin 2. fıkrasındaki (aşağıda belirtilen) maddelerin varlığı halinde kişisel verinin aktarılacağı yabancı ülkede;

- Yeterli korumanın bulunması,
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

3.4. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ

Kişisel verilerin işleme amacı sona ermiş, ilgili mevzuat ve/veya Şirketimizin belirlediği saklama süreleri tamamlanmış, kişisel veri sahibinin talebi veya re'sen Şirketimiz tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir. Bu kapsamda Şirketimiz, ilgili yükümlülüğünü KVK Kanunu'nun 7. maddesi ile "**Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik**"de belirtilen esaslara göre yerine getirmektedir.

3.4.1. **Kişisel verilerin silinmesinde izlenen süreç aşağıdaki gibi belirtilmiştir:**

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi,
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi,
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi,
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

3.4.2. **Kişisel verilerin yok edilmesinde izlenecek yöntemler aşağıdaki gibi belirtilmiştir:**

- **Fiziksel Olarak Yok Etme:** Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla elektronik/otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel veri sonradan kullanılamayacak biçimde fiziksel olarak yok edilmektedir.
- **Sunucu (Bulut) Ortamında Silme ve Yok Etme:** Tamamen veya kısmen elektronik/otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; verinin bir daha belirli kişilerce ya da hiçbir biçimde kurtarılamayacak şekilde ilgili yazılımdan silinmesine ilişkin yöntemleri ifade etmektedir.

3.4.3. **Kişisel verilerin anonim hale getirilmesi süreçleri aşağıdaki gibi belirtilmiştir:**

- **Maskeleme:** Veri maskeleme kişisel verinin temel belirleyici bilgisinin veri seti içerisinde çıkarılmasıdır.
- **Toplulaştırma:** Veri toplulaştırma yöntemi, birçok veri toplulaştırılır ve kişisel verilerin herhangi bir başka veriyle ilişkilendirilemeyecek hale getirilmesidir.
- **Veri Türetme:** Kişisel verinin içeriğinden daha genel bir içerik oluşturulur ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanır.
- **Veri Karma:** Kişisel veri seti içindeki değerlerin karıştırılarak değerler ile kişiler arasındaki bağın kopartılmasıdır.

3.5. KİŞİSEL VERİLERİN MUHAFAZASI VE ERİŞİM

Şirketimiz, kişisel verileri KVK Kanunu'nda belirtildiği veya işlendikleri amaç doğrultusunda kişisel verilerin saklanması için belirtilen süreye uygun hareket etmekte, bu kapsamda hukuki ve ceza zaman aşımı sürelerini dikkate almaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler Şirketimiz tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir.

3.5.1. Kağıt Ortamındaki Kişisel Verilerin Muhafazası

- Personelin kişisel verileri, kağıt ortamında özlük dosyalarında muhafaza edilir.
- Özlük dosyalarına sadece İnsan Kaynakları Bölümü personeli erişebilir.
- Özlük dosyaları “Gizli” risk sınıfında sınıflandırılmaktadır.
- Özlük dosyalarına “sadece ilgili birimde çalışan personel erişebilir” şeklinde ulaşılabilir.
- Erişim yetkisi olmayan kişilerin özlük dosyalarına erişiminde Mali ve İdari İşler Grup Başkanı onayı dahilinde izin verilir. Kişisel veriye erişim; yetkili personel nezaretinde yapılır.
- “Özlük” ve “Sağlık” dosyalarının erişim güvenliğinden İnsan Kaynakları ve İdari İşler Bölümü sorumludur.
- İzinsiz erişim vakalarının tespitinde “Disiplin Prosedürü” doğrultusunda hareket edilir.

3.5.2. Dijital Ortamdaki Kişisel Verilerin Muhafazası

- Kişisel verilerin saklandığı dijital ortamlara sadece yetkili personelce erişim sağlanabilir.
- Kişilere özel şifreler ile erişimler kontrol altında tutulmakta, erişimler log kayıtları ile kayıt altına alınmaktadır.
- Dijital ortamdaki verilerin korunmasına yönelik firewall, virüs programları gibi güvenlik sistemleri mevcuttur.
- Dijital ortamdaki kişisel verilerin muhafazası ve bilgi güvenliği ile ilgili tüm tedbirlerin alınmasında, şirket “Bilgi Güvenliği” uygulamaları kapsamında Bilgi Teknolojileri Bölüm Yöneticisi sorumludur.

3.6. HAK VE YÜKÜMLÜLÜKLER

3.6.1. Veri Sahibinin Hakları

3.6.1.1. Kişisel veri sahibi, veri sorumlusuna başvurarak kendisiyle ilgili aşağıda belirtilen hususları öğrenme hakkında sahiptir.

- Kişisel verilerinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı 3. kişileri bilme,
- Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı 3. kişilere bildirilmesini isteme,
- KVK Kanunu ve buna bağlı diğer yasal hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı 3. kişilere bildirilmesini isteme,

- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- KVK Kanunu'na aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme.

3.6.2. Veri Sorumlusunun Hak ve Yükümlülükleri

- 3.6.2.1.** Veri Sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini ve/veya erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, sorumlu olduğu sistemlerde yaşanabilecek muhtemel veri kayıplarının önüne geçmek için uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almakla yükümlüdür.
- 3.6.2.2.** Veri sorumlusu ile veri işleyen kişiler, öğrendikleri/edindikleri kişisel verileri, "**Kişisel Verilerin Korunması Kanunu**" hükümlerine aykırı olacak şekilde başkasına açıklamaz ve işleme amacı dışında kullanamaz. Bu yükümlülük, görevden ayrılımlarından sonra da devam eder.
- 3.6.2.3.** İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu durumu eşanlı Komite ile paylaşır ve akabinde en kısa sürede Kişisel Verilerin Korunması Kurulu'na iletir.
- 3.6.2.4.** Veri sorumlusunun kişisel veri sahibini aydınlatma/bilgilendirme yükümlülüğü, denetim yapma ve yaptırma, sır saklama ve ihlal bildirim sorumluluğu vardır.
- 3.6.2.5.** Şirketimiz, Anayasa'nın 20. ve KVK Kanunu'nun 10. maddesine uygun şekilde, kişisel veri sahiplerini aydınlatmakta ve kişisel veri sahiplerinin bilgi talep etmeleri durumunda gerekli bilgilendirmeyi yapmaktadır.
- 3.6.2.6.** Veri sorumlusu, kişisel verilerin elde edilmesi sırasında ilgili taraflara;
- Veri sorumlusunun ve varsa temsilcisinin kimliği,
 - Kişisel verilerin hangi amaçla işleneceği,
 - İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
 - Kişisel veri toplamanın yöntemi ve hukuki sebebi,
 - KVK Kanunu'nda 11. maddede sayılan diğer hakları
- konusunda bilgi verir.

3.7. KİŞİSEL VERİLERİN İHLALİ

- 3.7.1.** KVK Kanunu'na uyum konusunda kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesinin tespiti halinde "**Önemli Kişi Erişim Listesi**"nde belirtilen yetkili kişi tarafından KVK Kurulu'na bildirilir.
- 3.7.2.** Kişisel verilerin hukuka aykırı olarak işlenmesi, paylaşılması ve gerektiğinde silinmemesi durumunda TCK'nın 135 ile 140. maddeleri uyarınca işlemler, Hukuk Müşavirliğince yürütülür.
- 3.7.3.** Kişisel verilerin ihlali suçunun işlenmesi halinde aşağıdaki yasal müeyyideler uygulanır:
- Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.
 - Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile yargılanır.
 - Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde bir yıldan iki yıla kadar hapis cezası verilir.

4. TANIMLAR

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

Özel Nitelikli Kişisel Veriler: 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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik bilgileridir.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan kişidir.

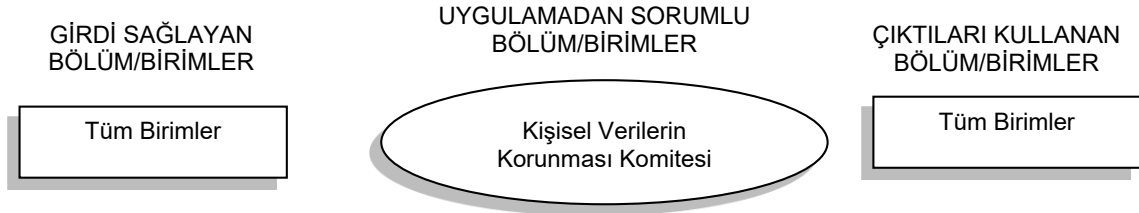
Kişisel Verilerin Anonim Hale Getirilmesi: Verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek bir hale getirilmesidir.

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen kişidir.

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Kişisel Verilerin İşlenmesi: 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.

5. SORUMLULUKLAR



Bu politikanın uygulanması **YÖNETİM KURULU BAŞKANI/CEO**'nun sorumluluğundadır. Politikanın uygulanması ile ilgili yetkiler **KİŞİSEL VERİLERİN KORUNMASI KOMİTESİ**'ne devredilmiş ve uygulama ile ilgili olarak görevlendirilmiştir.

6. REFERE DOKÜMANLAR

Doküman Tipi	Doküman Adı	Doküman No	Adres
Yasal Mevzuat	Kişisel Verilerin Korunması Kanunu	-	ADS
Yasal Mevzuat	Türk Ceza Kanunu	-	ADS
Politika	Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Prosedürü	PR.YNT.00.001	ADS
Prosedür	Disiplin Prosedürü	PR.MII.02.001	ADS
Prosedür	Risk Yönetimi Prosedürü	PR.YNT.01.003	ADS
Form	Erişim Yetkilendirme Listesi	FR.YNT.01.016	ADS
Form	Yetki Listesi	FR.YNT.01.001	ADS

7. DOSYALAMA SİSTEMATİĞİ

Klase Edilen Belge	Adres	Süre

Hazırlayan Kişisel Verilerin Korunması Komitesi	Kontrol Denetim Sistemleri Direktörü	Onay Yönetim Kurulu Başkanı
---	--	---------------------------------------



KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

Dok. No: PL.YNT.00.010

Yayın Tarihi: 18.07.2018

Revize Tarihi/No: -

8. REVİZYON KURALI

İlgili doküman **Kişisel Verilerin Korunması Komitesi**'nin görüşü alınarak **Yönetim Kurulu Başkanı** onayı ile revize edilir. Bu politika yılda bir kez gözden geçirilmeli ve politikaya uyumu sağlanmalıdır.

9. REVİZYON NEDENİ

Revizyon Tarihi	Revizyon No	Revizyon İçeriği

Hazırlayan Kişisel Verilerin Korunması Komitesi	Kontrol Denetim Sistemleri Direktörü	Onay Yönetim Kurulu Başkanı
---	--	---------------------------------------