Kişisel Veri Saklama ve İmha Politikası

Rev. No: 00

1. AMAÇ

Bu politikanın temel amacı, işletme tarafından gerçekleştirilen kişisel veri saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek; Kanun'un 7. maddesi ve ilgili Yönetmelik uyarınca verilerin hukuka uygun olarak silinmesi, yok edilmesi veya anonim hale getirilmesi süreçlerinde şeffaflığı ve yasal uyumu sağlamaktır.

2. KAPSAM

Bu politika; işletme çalışanları, çalışan adayları, müşteriler, tedarikçiler, ziyaretçiler ve işletme ile temas halindeki tüm gerçek kişilerin, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerini kapsar.

3. TANIMLAR

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

İlgili Kişi : Kişisel verisi işlenen gerçek kişi.

İlgili Kullanıcı: Verilerin teknik olarak depolanması ve yedeklenmesinden sorumlu olan kişi/birim hariç, veri sorumlusu organizasyonu içerisinde verileri işleyen kişilerdir.

Kayıt Ortamı: Kişisel verilerin bulunduğu her türlü ortamdır.

Periyodik İmha: İşleme şartları ortadan kalkan verilerin, politikada belirtilen ve tekrar eden aralıklarla (en geç 6 ayda bir) resen gerçekleştirilecek imha işlemidir.

Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

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

Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.

Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.

Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.

Hizmet Sağlayıcı: İşletme ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek

veya tüzel kişi.

Kayıt Ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.

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

Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan

azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.

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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi,

sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Özel Nitelikli Kişisel Veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.

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

Veri Kayıt Sistem**i:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.

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

VERBİS: Veri Sorumluları Sicil Bilgi Sistemi.

Yönetmelik: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

4. SORUMLULUKLAR

Üst Yönetim: Politikanın uygulanması için gerekli teknik ve idari kaynakların sağlanmasından sorumludur.

KVK Komisyonu/Sorumlusu: İmha süreçlerinin denetimi, envanterin güncelliği ve personelin farkındalık eğitimlerinden sorumludur.

Birim Yöneticileri (İK, Bilgi İşlem, Muhasebe): Kendi süreçlerindeki verilerin saklama sürelerini takip etmek ve süresi dolanları bildirmekle yükümlüdür.

5. İLGİLİ DOKÜMAN VE EKLER

- Kişisel Veri İşleme Envanteri.
- Veri Sahibi Başvuru Formu.
- Kişisel Veri İmha Tutanağı
- Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler).
- Kişisel Verilerin Güvenliğine İlişkin Teknik Tedbirler kapsamındaki Politikalar ve Talimatlar

6. UYGULAMA

6.1. Kayıt Ortamları

İşletme, kişisel verileri güvenli bir şekilde aşağıdaki ortamlarda saklar:

Elektronik Ortamlar: Sunucular (veritabanı, e-posta), yazılımlar (muhasebe, ERP), bulut ortamları, taşınabilir medyalar (USB, HDD), bilgisayarlar ve kamera kayıt cihazları.

Elektronik Olmayan Ortamlar: Özlük dosyaları, sözleşmelerin bulunduğu fiziksel arşivler, ziyaretçi defterleri ve formlar.

Elektronik Ortamlar:	**Elektronik Olmayan Ortamlar:**

• Sunucular (Etki alanı, yedekleme, • e-posta, veri tabanı, web, dosya paylaşım, vb.) • Yazılımlar (ofis yazılımları, portal, ERP, CRM, MRP, bulut tabanlı yazılımlar vb.) • Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) • Kişisel bilgisayarlar (Masaüstü, dizüstü) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kartı) • Yazıcı, tarayıcı, fotokopi makinesi	• Kâğıt • Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) • Yazılı, basılı, görsel ortamlar • İş Başvuru Süreçleri kayıtları • Personel Mülakat Süreçleri kayıtları • İşe yerleştirme Süreçleri kayıtları • Üretim hizmet gerçekleştirme sürecinde oluşturulan basılı kayıtlar • Özlük Süreçleri Kayıtları

6.2. Saklama ve İmhayı Gerektiren Şartlar

Kişisel veriler, Kanun'un 5. ve 6. maddelerindeki işleme şartlarının tamamının ortadan kalkması durumunda silinir, yok edilir veya anonim hale getirilir.

- Saklama Sebepleri: Kanunlarda öngörülme, sözleşmenin ifası, hukuki yükümlülük, bir hakkın tesisi veya korunması.
- İmha Sebepleri: İşleme amacının sona ermesi, saklama süresinin dolması, ilgili kişinin rızasını geri alması veya silme talebinin kabul edilmesi.

6.3. Veri Güvenliğine İlişkin Teknik ve İdari Tedbirler

Verilerin güvenli saklanması ve yetkisiz erişimin önlenmesi için şu temel tedbirler alınır:

- Teknik Tedbirler: Yetki matrisi, sızma testleri, güncel anti-virüs sistemleri, şifreleme (kriptografi), güvenlik duvarları, log kayıtlarının tutulması.
- İdari Tedbirler: Çalışanlara KVKK eğitimi verilmesi, gizlilik sözleşmeleri imzalatılması, kurum içi periyodik denetimler ve veri azaltımı (minimizasyon).

6.4 Kişisel Veri Saklamaya İlişkin Açıklamalar

Kişisel verilerin işlenmesi; bu 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 gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.

6698 sayılı Kanun'un 4. maddesi uyarınca, işlenen kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. Bu kapsamda kişisel veriler, Kanun'un 5. ve 6. maddelerinde belirtilen kişisel veri işleme şartları çerçevesinde; ilgili mevzuatta öngörülen veya Kurumumuzun faaliyetlerine dayanan işleme amaçlarına uygun süre kadar saklanmaktadır.

Kişisel Veri Saklamayı Gerektiren İşleme Amaçları

Şirketimiz, **"amaçla sınırlılık" ilkesi gereği**, kişisel verileri ancak belirli, açık ve meşru olan aşağıdaki amaçlar doğrultusunda saklamaktadır:

- İnsan kaynakları süreçlerini ve iş akdi/mevzuattan kaynaklı yükümlülükleri yürütmek.
- Kurumsal iletişimi ve kurum ile iş ilişkisinde bulunan gerçek/tüzel kişilerle irtibatı sağlamak.
- Kurum, fiziksel mekân ve bilgi güvenliğini temin etmek.
- İstatistiksel çalışmalar yapabilmek ve veri sorumluları ile ilgili tercih/ihtiyaç analizi gerçekleştirmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.

- Yasal düzenlemelerin gerektirdiği hukuki yükümlülüklerin yerine getirilmesini sağlamak ve yasal raporlamalar yapmak.
- Çağrı merkezi süreçlerini yönetmek ve doğabilecek hukuki uyuşmazlıklarda ispat yükümlülüğünü yerine getirmek.

Saklamayı Gerektiren Hukuki Sebepler

Kurum faaliyetleri çerçevesinde işlenen kişisel veriler, başta **6698 sayılı Kişisel Verilerin Korunması Kanunu** olmak üzere, tabi olduğumuz diğer mevzuatta öngörülen süreler boyunca muhafaza edilir. Bu kapsamda temel dayanak teşkil eden hukuki sebepler şunlardır:

Ticaret ve Şirketler Mevzuatı

- **6102 Sayılı Türk Ticaret Kanunu (TTK)**: Şirket ortaklarının, yönetim kurulu üyelerinin, ticari defterlerin ve fatura bilgilerinin tutulması için ana gerekçedir.
- **213 Sayılı Vergi Usul Kanunu (VUK)**: Müşteri, tedarikçi ve çalışanların fatura, makbuz, cari hesap ve vergilendirmeye esas kişisel verilerinin tutulmasını zorunlu kılar.
- **6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun**: E-ticaret sitelerinin üyelik, sipariş, teslimat ve onaylı ticari elektronik ileti kayıtlarını tutmasını gerektirir.
- **6098 sayılı Türk Borçlar Kanunu**: ilgili düzenlemelerle zorunlu kayıt edilen kişisel veriler.

İş Hukuku ve Sosyal Güvenlik Mevzuatı

- **4857 Sayılı İş Kanunu:** İşletmelerin personel özlük dosyası oluşturması, çalışan verilerini işlemesi ve iş sağlığı önlemleri alması için yasal dayanaktır.
- **5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu:** Çalışanların SGK prim bildirimleri, maaş kesintileri ve sigorta giriş/çıkış işlemlerinin yapılması için zorunludur.
- **6331 Sayılı İş Sağlığı ve Güvenliği Kanunu:** Çalışanların sağlık raporları, periyodik muayeneleri ve iş kazası kayıtlarının tutulmasına yasal zemin hazırlar.
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik ile Arşiv Hizmetleri Hakkında Yönetmelik ve bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler.

Güvenlik ve Kimlik Mevzuatı

- **1774 Sayılı Kimlik Bildirme Kanunu:** Otel, pansiyon gibi konaklama tesisleri ile araç kiralama (rent-a-car) şirketlerinin müşteri kimliklerini kolluk kuvvetlerine bildirmesini zorunlu kılar.
- **5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu:** İşletmelerin müşterilerine veya çalışanlarına sunduğu Wi-Fi/internet hizmetine ait log (bağlantı) kayıtlarını saklamasını şart koşar.

Finans ve Tüketici Mevzuatı

- **6502 Sayılı Tüketicinin Korunması Hakkında Kanun:** Satış sonrası garanti, servis, iade ve mesafeli satış sözleşmesi süreçlerinde müşteri verilerinin işlenmesini sağlar.
- **5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun:** Bankalar, finans kuruluşları, döviz büroları ve belirli sektörlerdeki şirketlerin şüpheli işlem bildirimi ve "müşterini tanı" (KYC) ilkeleri kapsamında kimlik tespiti yapmasını zorunlu tutar.

6.5 Kişisel Verilerin İmha Edilmesini Gerektiren Sebepler

Kişisel veriler; ilgili mevzuat hükümlerine uygun olarak işlenmiş olmasına rağmen, **işlenmesini gerektiren sebeplerin ortadan kalkması halinde** Kurum tarafından resen veya ilgili kişinin talebi üzerine silinir, yok edilir ya da anonim hale getirilir. İmhayı gerektiren temel haller şunlardır:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası.
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması.

- İşlemenin sadece açık rıza şartına dayandığı hallerde, ilgili kişinin açık rızasını geri alması.
- İlgili kişinin Kanun'un 11. maddesi kapsamındaki silme ve yok etme başvurusunun kabul edilmesi.
- Saklanmasını gerektiren azami sürenin geçmiş olması ve verileri daha uzun süre saklamayı haklı kılacak bir şartın bulunmaması.
- Kanun'un 5. ve 6. maddelerindeki işleme şartlarının tamamının ortadan kalkması.
- İmha yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde (en geç 6 ayda bir) söz konusu veriler güvenli yöntemlerle imha edilerek kayıt altına alınır.

Kişisel Verilerin Silinmesi ve Yok Edilmesi Teknikleri

Silme (Erişimi Kapatma): Verilerin "ilgili kullanıcılar" için erişilemez ve tekrar kullanılamaz hale getirilmesidir.

- Sunucular: İlgili kullanıcının erişim yetkisi kaldırılır.
- Kağıt Ortamı: Karartma (okunamayacak şekilde çizme/boyama) yapılır.

Yok Etme (Fiziksel/Teknik Geri Döndürülemezlik): Verilerin hiç kimse tarafından erişilemez hale getirilmesidir.

- Fiziksel: Kağıt imha makinelerinde kıyılma veya eritilme.
- Manyetik Medya: De-manyetize etme (yüksek manyetik alan) veya üzerine en az 7 kez veri yazma.

Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi; söz konusu verilerin başka verilerle eşleştirilmesi durumunda dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek konuma getirilmesidir.

Bir kişisel verinin yasal olarak anonim hale getirilmiş sayılabilmesi için; veri sorumlusu, alıcı grupları veya üçüncü kişiler tarafından uygulanan geri döndürme teknikleri ve/veya verilerin farklı veri setleriyle eşleştirilmesi gibi yöntemler de dahil olmak üzere, mevcut kayıt ortamı ve ilgili faaliyet alanı açısından kullanılabilen hiçbir teknik yolla kimliği belirli ya da belirlenebilir bir gerçek kişiyle yeniden ilişkilendirilemez hale getirilmiş olması zorunludur. Şirketimiz bünyesinde anonimleştirilen veriler, KVKK kapsamı dışına çıkacağı için istatistiksel analizler ve AR-GE çalışmaları gibi süreçlerde güvenle kullanılabilmektedir.

Kişisel Verileri Anonim Hale Getirme Teknikleri

Maskeleme: Verinin temel belirleyicisinin (örn. T.C. No'nun bir kısmının) yıldızlanması.

Genelleştirme: "31 yaş" yerine "30-40 yaş aralığı" gibi daha genel bir değer yazılması.

Veri Türetme: Doğum tarihi yerine sadece yaş bilgisinin tutulması.

Veri Karma: Veri seti içindeki değerlerin karıştırılarak bağın koparılması.

Periyodik İmha Süreleri

İşletme, her yıl Haziran ve Aralık aylarında olmak üzere, 6 ayda bir periyodik imha işlemini gerçekleştirir. İmha edilen verilere ilişkin tutanaklar en az 3 yıl süreyle saklanır.

6.6 Teknik Ve İdari Tedbirler

Kanun'un 12. maddesi ile 6. maddesinin 4. fıkrası gereğince; kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, güvenli şekilde saklanmasını sağlamak ve hukuka uygun olarak imha etmek amacıyla yeterli önlemler çerçevesinde gerekli teknik ve idari tedbirler alınır.

Kişisel Verilerin Güvenliğine İlişkin Teknik Tedbirler

- **Zafiyet Analizi ve Olay Yönetimi:** Şirketimiz bilişim sistemlerine yönelik risk, tehdit ve zafiyetler, düzenli olarak gerçekleştirilen sızma (penetrasyon) testleri ile tespit edilerek gerekli önlemler alınır. Bilgi

güvenliği olay yönetimi süreçleri kapsamında yapılan gerçek zamanlı analizlerle, sistem sürekliliğini etkileyebilecek tehditler sürekli olarak izlenir.

- **Erişim Yönetimi ve Yetkilendirme:** Bilişim sistemlerine erişim yetkileri; merkezi aktif dizin (Active Directory) üzerinden, kurumsal güvenlik politikalarına uygun olarak hazırlanan "Erişim ve Yetki Matrisi" çerçevesinde sınırlandırılır ve yönetilir.
- **Fiziksel Ortam Güvenliği:** Şirketimize ait bilişim sistemi donanımlarının, yazılımların ve fiziksel ortamlarda saklanan verilerin güvenliği için gerekli idari ve fiziki önlemler alınır.
- **Çevresel Tehditlere Karşı Koruma:** Çevresel risklere karşı sistem odalarına sadece yetkili personelin girişini sağlayan biyometrik/kartlı erişim kontrol sistemleri, 7/24 izleme kameraları, yangın söndürme ve iklimlendirme sistemleri gibi donanımsal; merkezi güvenlik duvarları (Firewall), saldırı önleme sistemleri (IPS/IDS), ağ erişim kontrolü (NAC) ve antivirüs/EDR yazılımları gibi teknik önlemler uygulanır.
- **Risk Bazlı Teknik Kontroller:** Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla olası riskler düzenli olarak analiz edilir; bu risklere uygun teknik tedbirler alınarak periyodik olarak denetlenir.
- **Erişim Logları ve Analizi:** Şirket bünyesinde erişim prosedürleri işletilir. Kişisel verilerin yer aldığı saklama alanlarına yönelik tüm erişimler ve yetkisiz erişim denemeleri güvenli loglama sistemleri ile kayıt altına alınır; bu kayıtlar düzenli olarak raporlanır ve analiz edilir.
- **Geri Dönüştürülemez İmha:** Şirketimiz, mevzuata uygun olarak silinen veya imha edilen kişisel verilerin, ilgili kullanıcılar için tekrar erişilemez ve geri getirilemez olmasını sağlayacak teknik altyapıyı uygular.
- **Veri İhlali Bildirim Sistemi:** Kişisel verilerin yetkisiz üçüncü kişiler tarafından hukuka aykırı şekilde elde edilmesi durumunda, bu durumu en kısa sürede ilgili kişiye ve Kişisel Verileri Koruma Kurulu'na bildirmek üzere dinamik bir ihlal yönetim ve bildirim mekanizması işletilir.
- **Yama ve Güncelleme Yönetimi:** Bilişim sistemlerindeki güncel güvenlik açıkları yakından takip edilerek, üretici yazılım ve güvenlik yamaları sisteme gecikmeksizin entegre edilir.
- **Parola ve Kimlik Doğrulama:** Kişisel verilerin işlendiği tüm elektronik ortamlarda ve kullanıcı hesaplarında güçlü parola politikaları (karmaşıklık ve uzunluk kuralları) zorunlu kılınır.
- **Veri Yedekleme:** Veri kaybı riskine karşı, kişisel verilerin güvenli ve şifreli olarak yedeklenmesini sağlayan merkezi veri yedekleme sistemleri ve politikaları kullanılır.
- **Web Sitesi ve İletişim Güvenliği:** Şirketimize ait internet sitelerine erişimde, veri trafiğinin şifrelenmesi amacıyla güncel SHA-256 Bit RSA algoritmasına sahip güvenli protokol (HTTPS/SSL) kullanılır.

Özel Nitelikli Kişisel Verilerin Güvenliğine İlişkin Tedbirler

- **Özel Politika Yönetimi:** Özel nitelikli kişisel verilerin güvenliğinin sağlanmasına yönelik, genel politikalardan bağımsız ayrı bir " Özel Nitelikli Kişisel Verilerin İşlenme Şartları Ve Güvenliği Politikası" uygulanır.
- **Çalışanların Eğitimi ve Farkındalık:** Özel nitelikli kişisel veri işleme süreçlerinde görev alan çalışanlara, bu verilerin hassasiyetine yönelik özel farkındalık eğitimleri verilir. Bu çalışanlarla ek gizlilik sözleşmeleri imzalanır ve erişim yetkileri "en az yetki" prensibine göre tanımlanır.
- **Elektronik Ortam Güvenliği ve Kriptografi:** Özel nitelikli kişisel verilerin işlendiği, saklandığı veya erişildiği elektronik ortamlar, güçlü kriptografik (şifreleme) yöntemler kullanılarak muhafaza edilir. Kriptografik anahtarlar güvenli ve bağımsız ortamlarda tutulur. Bu ortamlardaki tüm işlem kayıtları (log) eksiksiz saklanır, güvenlik güncellemeleri sürekli takip edilir ve düzenli olarak sızma testlerine tabi tutularak sonuçlar raporlanır.
- **Fiziksel Ortam Güvenliği:** Özel nitelikli kişisel verilerin yer aldığı fiziksel ortamlar (arşivler, kilitli dolaplar vb.) için üst düzey güvenlik önlemleri alınarak yetkisiz giriş ve çıkışlar fiziki bariyerlerle engellenir.
- **Güvenli Veri Aktarım Yöntemleri:** Özel nitelikli kişisel verilerin aktarım süreçlerinde şu kurallara riayet edilir:

- **E-Posta:** Kurumsal e-posta adresi üzerinden şifreli dosya formatında veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılır.
- **Fiziksel Medya:** Taşınabilir bellek, CD, DVD gibi cihazlarla aktarılması gerektiğinde veriler kriptografik yöntemlerle şifrelenir ve şifre çözme anahtarı veri ambalajından farklı bir kanaldan alıcıya iletilir.
- **Sunucular Arası Aktarım:** Farklı lokasyonlardaki sunucular arasında veri transferi yapılacağı durumlarda, güvenli tüneller (VPN) veya sFTP (Secure File Transfer Protocol) yöntemleri kullanılır.
- **Fiziksel Evrak (Kağıt):** Kağıt ortamında yapılan aktarımlarda; çalınma, kaybolma veya yetkisiz kişilerin erişimi riskine karşı evraklar "Gizli" ibareli kapalı zarflar ve zimmet tutanakları eşliğinde sevk edilir.

Kişisel Verilerin Güvenliğine İlişkin İdari Tedbirler

- **Kurumsal Politika ve Prosedürlerin Hazırlanması:** Şirket faaliyetleri kapsamında yürütülen kişisel veri işleme süreçlerine ilişkin; "Kişisel Veri Saklama ve İmha Politikası", "Özel Nitelikli Kişisel Verilerin İşlenme Şartları Ve Güvenliği Politikası" ve ilgili işleyiş prosedürleri hazırlanarak şirket genelinde yürürlüğe konulmuştur.
- **Kişisel Veri Envanter Yönetimi:** Şirketimiz bünyesinde işlenen tüm kişisel veriler; işleme amaçları, veri kategorileri, aktarılan alıcı grupları ve azami saklama süreleri bazında "Kişisel Veri İşleme Envanteri"nde kayıt altına alınmakta ve güncel tutulmaktadır.
- **Çalışanlara Yönelik Eğitim ve Farkındalık Çalışmaları:** Tüm şirket çalışanlarına, işe alım süreçlerinden itibaren kişisel verilerin korunması hukuku, veri güvenliği, siber güvenlik riskleri ve özel nitelikli kişisel verilerin korunması konularında periyodik eğitimler verilmekte ve kurumsal farkındalık artırılmaktadır.
- **Sözleşmelerin KVKK Uyumlu Hale Getirilmesi:** Müşteriler, tedarikçiler, iş ortakları ve hizmet sağlayıcılar ile akdedilen tüm sözleşmelere, KVKK ve ilgili mevzuata uyumu zorunlu kılan veri güvenliği hükümleri ve taahhütleri eklenmektedir.
- **Çalışanlar İçin Gizlilik Taahhütnameleri:** Şirket çalışanları ile iş sözleşmelerinin eki niteliğinde, kişisel verilerin gizliliğini korumayı ve yetkisiz şekilde üçüncü kişilerle paylaşmamayı taahhüt eden "Gizlilik ve Veri Güvenliği Taahhütnameleri" imzalanmaktadır.
- **Kurumsal Disiplin Prosedürleri:** Çalışanların veri güvenliği politikalarına ve talimatlarına aykırı hareket etmesi durumunda uygulanacak yaptırımları düzenleyen "Disiplin Prosedürü" işletilmekte ve ihlal durumlarında yasal süreçler uygulanmaktadır.
- **Aydınlatma ve Açık Rıza Süreçlerinin Yönetimi:** Veri sahiplerinin (ilgili kişilerin) haklarını korumak adına, veri toplama kanallarında (web sitesi, fiziki formlar vb.) yasal "Aydınlatma Metinleri" sunulmakta; kanuni istisnaların dışındaki süreçler için "Açık Rıza" mekanizmaları işletilmektedir.
- **Veri Sorumluları Sicili (VERBİS) Yönetimi:** Şirketimizin VERBİS (Veri Sorumluları Sicil Bilgi Sistemi) kayıt yükümlülüğünün bulunması halinde, envanter ile uyumlu şekilde sicil beyanları yapılmakta ve süreçlerdeki değişiklikler sisteme yasal süresi içinde yansıtılmaktadır.
- **Veri Sahibi Başvurularının Yönetimi:** İlgili kişilerin Kanun'un 11. maddesi kapsamındaki hak arama başvurularını (bilgi alma, silme, düzeltme vb.) şirkete iletebilmeleri için yasal kanallar oluşturulmuş ve bu başvuruların en geç 30 gün içinde yanıtlanmasını sağlayan başvuru yönetim süreçleri kurulmuştur.
- **Periyodik ve Rastgele Denetimler:** Şirket içi veri güvenliği uygulamalarının, politikaların ve alınan idari/teknik tedbirlerin etkinliği, belirli periyotlarla veya rastgele zamanlarda iç denetim mekanizmaları ile kontrol edilmekte ve raporlanmaktadır.
- **Veri Azaltımı (Minimizasyon) İlkesi:** Şirket genelinde yürütülen iş süreçlerinde "en az veri" prensibi benimsenmekte; bir iş sürecinin yürütülmesi için gerekli olmayan veya kullanım amacı sona eren kişisel verilerin toplanması ve işlenmesi engellenmektedir.

Kişisel Verilerin Yok Edilmesi

Kişisel veriler, aşağıda verilen yöntemlerle yok edilir.

Veri Kayıt Ortamı	İmha / Silme Yöntemi ve Uygulama Açıklaması
Sunucularda Yer Alan Kişisel Veriler	Saklama süresi sona eren kişisel veriler; Sistem Yöneticisi tarafından ilgili kullanıcıların erişim yetkileri tamamen kaldırılarak **merkezi sistemlerden kalıcı olarak silinir** ve geri getirilemez hale getirilir.
Elektronik Ortamda Yer Alan Kişisel Veriler	Veri tabanları ve bulut sistemlerinde yer alan, saklama süresi dolan veriler; Veri tabanı Yöneticisi hariç diğer tüm çalışanlar (ilgili kullanıcılar) için **erişilemez, kurtarılamaz ve tekrar kullanılamaz** hale getirilir.
Fiziksel Oramda Yer Alan Kişisel Veriler	Kağıt, dosya ve arşiv ortamında tutulan ve süresi dolan veriler; Evrak Arşiv Yöneticisi dışındaki tüm personel için erişilemez kılınır. Ek olarak, üzerindeki kişisel veriler okunmayacak şekilde **karartılır (çizilir/boyanır)** veya fiziksel olarak **evrak imha makinesinde (kırpıcı) yok edilir**.
Taşınabilir Medyada Yer Alan Kişisel Veriler	Flash bellek, CD/DVD ve taşınabilir disklerde yer alan ve saklama süresi dolan veriler; Sistem Yöneticisi tarafından **kriptografik yöntemlerle şifrelenir**, erişim yetkileri kaldırılır ve şifreleme anahtarları güvenli ortamlarda tutularak verinin yetkisiz kullanımı tamamen engellenir.* *bu verileri yukarıdaki gibi şifreleyerek tutulduğunda; "*Bu işlem, arşivsel/yasal zorunluluklar nedeniyle tamamen yok edilemeyen veriler için nihai imhaya kadar geçici bir güvence tedbiri olarak uygulanır*"

Kişisel Veri Saklama ve İmha Süreçlerinin Yönetimi

Şirketimiz tarafından yürütülen faaliyetler kapsamında işlenen kişisel verilerin saklama süreleri ve bu verilere yönelik imha süreçleri aşağıda belirtilen esaslar çerçevesinde yönetilir:

- **Veri Bazlı Saklama Süreleri:** Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm verilerin kişisel veri bazındaki saklama süreleri **Kişisel Veri İşleme Envanteri**'nde yer alır.
- **Veri Kategorisi Bazlı Saklama Süreleri:** Veri kategorileri temelindeki saklama süreleri **VERBİS** (Veri Sorumluları Sicil Bilgi Sistemi) kayıtlarında yer alır.
- **Süreç Bazlı Saklama Süreleri:** İş süreçleri bazındaki saklama süreleri ise **Kişisel Veri Saklama ve İmha Politikası**'nda yer alır.

Mevzuata veya şirket politikalarına göre saklama süreleri sona eren kişisel verilerin re'sen (kendiliğinden) silinmesi, yok edilmesi veya anonim hale getirilmesi işlemleri, **İlgili Bölüm Sorumluları** tarafından yasal süresi içinde yerine getirilir.

KİŞİSEL VERİ SAKLAMA SÜRELERİ TABLOSU

Aşağıda belirtilen süreler genel uygulama kaidelerini ifade etmektedir. Şirketimiz bazı özel nitelikli kişisel verileri (Ceza Mahkûmiyeti, Felsefi İnanç, Din, Mezhep ve Diğer İnançlar Dernek Üyeliği, Vakıf Üyeliği, Sendika Üyeliği) işlememeyi ve saklamamayı tercih edebilir.

Kişisel Veri Kategorileri ve Saklama Süreleri Tablosu

Veri Kategorisi	Saklama Süresi	İmha Süresi ve Gerekçesi

Kimlik Bilgisi	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
İletişim Bilgisi	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Özlük Bilgisi	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Mesleki Deneyim	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Görsel ve İşitsel Kayıtlar	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Sağlık Bilgileri *(Özel Nitelikli)*	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Ceza Mahkûmiyeti ve Güvenlik Tedbirleri *(Özel Nitelikli)*	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Felsefi İnanç, Din, Mezhep ve Diğer İnançlar *(Özel Nitelikli)*	Çalışanın İşten ayrılmasından itibaren **15 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Lokasyon Verisi	Çalışanın İşten ayrılmasından itibaren **10 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Diğer Bilgiler (Araç Bilgisi)	Çalışanın İşten ayrılmasından itibaren **10 Yıl**	Süre bitimini takip eden ilk periyodik imha döneminde silinir, yok edilir veya anonim hale getirilir.
Hukuki İşlem	**10 Yıl**	İşlemin kesinleşmesinden veya sona ermesinden itibaren 10 yıl sonra imha edilir.
Fiziksel Mekan Güvenliği	**10 Yıl**	Verinin elde edilme tarihinden itibaren 10 yıl sonra imha edilir.
İşlem Güvenliği	**10 Yıl**	Log veya kayıt tarihinden itibaren 10 yıl sonra imha edilir.
Finans	**10 Yıl**	Mali dönemin kapanmasından veya işlemin bitiminden itibaren 10 yıl sonra imha edilir.

Dernek Üyeliği *(Özel Nitelikli)*	**6 Ay**	Üyeliğin veya işleme amacının sona ermesinden itibaren 6 ay sonra imha edilir.
Vakıf Üyeliği *(Özel Nitelikli)*	**6 Ay**	Üyeliğin veya işleme amacının sona ermesinden itibaren 6 ay sonra imha edilir.
Sendika Üyeliği *(Özel Nitelikli)*	**6 Ay**	Üyeliğin veya işleme amacının sona ermesinden itibaren 6 ay sonra imha edilir.

Kişisel Veri Saklama ve İmha Politikası Sorumluluk Matrisi

Unvan	Bağlı Olduğu Departman	Politika Rolü	KVKK Kapsamındaki Özel Sorumluluk Alanı ve Görev Tanımı
Genel Müdür	Üst Yönetim	Üst Düzey Sorumlu ve Onay Makamı	Politikanın şirket genelinde uygulanmasını denetler, imha süreçleri için gerekli kaynakları tahsis eder ve nihai onayları verir.
Fabrika Müdürü	Fabrika Yönetimi	Operasyonel Uygulama Sorumlusu	Fabrika sahasındaki tüm departmanların veri saklama ve periyodik imha sürelerine uyumunu koordine ve kontrol eder.
İnsan Kaynakları Sorumlusu	İnsan Kaynakları	Uygulama ve İmha Sorumlusu	Çalışan ve aday özlük dosyaları, performans, iş başvurusu ve çalışan sağlık/ceza verilerinin saklanması ve periyodik imhasını yönetir.
Satış Sorumlusu	Satış ve Pazarlama	Uygulama ve İmha Sorumlusu	Müşteri potansiyel verileri, satış sözleşmeleri, onaylı ticari ileti kayıtları ve pazarlama verilerinin saklanması ve imhasını yönetir.
Müşteri Temsilcisi	Müşteri İlişkileri (CRM)	Uygulama ve İmha Sorumlusu	Müşteri talep/şikayet kayıtları, çağrı merkezi verileri ve aktif müşteri iletişim bilgilerinin takibi ile periyodik imha süreçlerini yürütür.
Finans Müdürü	Mali İşler / Finans	Uygulama ve İmha Sorumlusu	Şirketin banka hesap verileri, ödeme/tahsilat kayıtları, kredi/finansman belgeleri ve risk yönetimi verilerinin saklanması ve imhasını yönetir.
Muhasebe Sorumlusu	Mali İşler / Muhasebe	Uygulama ve İmha Sorumlusu	Faturalar, cari hesaplar, makbuzlar, vergi beyannameleri ve maaş bordrolarına esas mali verilerin yasal sürelere uygun saklanması ve imhasını yürütür.
İdari İşler Sorumlusu	İdari İşler	Uygulama ve İmha Sorumlusu	Kamera (CCTV) kayıtları, ziyaretçi giriş-çıkış logları, şirket araç/filo bilgileri ve fiziki mekân güvenliği verilerinin saklanması ve imhasını yönetir.
Satın Alma Sorumlusu	Satın Alma	Uygulama ve İmha Sorumlusu	Tedarikçi yetkilileri ve alt yüklenicilere ait kimlik, iletişim, imza sirküleri ve teklif/sözleşme verilerinin saklanması ve periyodik imhasını yönetir.

Üretim Sorumlusu	Üretim	Uygulama ve İmha Sorumlusu	Üretim hatlarında görevli personelin vardiya kayıtları, verimlilik verileri ve üretime bağlı operasyonel kişisel verilerin saklanması ve imhasını yürütür.
Kalite Yönetim Sorumlusu	Kalite Yönetimi	Denetim ve Uygulama Sorumlusu	Müşteri memnuniyet anketleri, düzeltici-önleyici faaliyet (DÖF) kayıtları ve kalite denetim süreçlerindeki kişisel verilerin saklanması ve imhasını yönetir.
İSG Uzmanı	İş Sağlığı ve Güvenliği	Uygulama ve İmha Sorumlusu	İş kazası raporları, ramak kala kayıtları, İSG eğitim katılım tutanakları ve risk analizlerindeki kişisel verilerin yasal süresince saklanması ve imhasını yönetir.
İşyeri Hekimi	Sağlık Birimi	Özel Nitelikli Veri Sorumlusu	Çalışanların periyodik sağlık muayene raporları, engellilik/sağlık durumları ve revir kayıtları gibi **özel nitelikli verilerin** şifreli/kilitli saklanması ve imhasını yürütür.
AR-GE Sorumlusu	Araştırma ve Geliştirme	Uygulama ve İmha Sorumlusu	AR-GE projeleri, ürün test süreçleri ve yenilikçi çalışmalarda kullanılan (mümkünse anonimleştirilmiş) kişisel verilerin saklanması ve periyodik imhasını yönetir.
Bakım Sorumlusu	Bakım ve Onarım	Uygulama ve İmha Sorumlusu	Cihaz/makine bakım kayıtları, dış servis teknik personel bilgileri ve bakım operasyonlarındaki kişisel verilerin saklanması ve imhasını yürütür.

Tüm Pozisyonlar İçin Ortak Esaslar (Politika Maddesi)

Yukarıda listelenen tüm sorumlular; kendi görev alanları dahilinde yürütülen süreçlerde kişisel verilerin **saklama sürelerine uygunluğunu sağlamak**, yetkisiz erişimleri önlemek ve şirketin belirlediği **periyodik imha süreleri** (Örn: 6 ayda bir) geldiğinde verilerin re'sen imha edilmesini/silinmesini koordine etmekle yükümlüdür.

7. POLİTİKANIN DAĞITIM ŞEKLİ

İşbu politika;

- Bir özet olarak Kurumsal KVK Politikası içinde, işletmenin resmi internet sitesinde kamuya açık şekilde yayımlanır.
- İşletme bünyesindeki ortak ağ sürücülerinde (KVK Klasörü vb.) tüm çalışanların erişimine sunulur.
- Yeni işe başlayan personele oryantasyon eğitimleri kapsamında tebliğ edilir.
- Gerektiğinde veri işleyenlere e-posta yoluyla gönderilir.
- Fiziksel alanlarda (ziyaretçi girişleri vb.) ilgili kişilerin görebileceği şekilde asılır veya yönlendirme yapılır.