

ORYANTAL TTN PAKETLEME SANAYİ VE TİCARET ANONİM ŐİRKETİ

KİŐİSEL VERİLERİ KAYIT, SAKLAMA VE İMHA PROSEDR

Versiyon : 1

Dzenleme Tarihi : 01.01.2020

1. GİRİŐ

1.1. Amaç

KiŐisel Verileri Saklama, Kayıt ve İmha Prosedr ("**Prosedr**"), Oryantal Ttn Paketleme Sanayi ve Ticaret Anonim Őirketi ("**Őirket**") tarafından gerçekteŐirilmekte olan saklama ve imha faaliyetlerine iliŐkin iŐ ve iŐlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıŐtır.

KiŐisel verilerin kaydı, saklanması ve imhasına iliŐkin iŐ ve iŐlemler, Őirket tarafından bu dođrultuda hazırlanmıŐ olan iŐbu Prosedre uygun olarak gerçekteŐirilir.

1.2. Kapsam

Őirket alıŐanları, alıŐan adayları, hizmet sađlayıcıları, tedarikiler, mŐteriler ziyaretiler ve diđer nc kiŐilere ait kiŐisel veriler, iŐbu Prosedr kapsamında olup; Őirket'in sahip olduđu ya da Őirkete ynetilen kiŐisel verilerin iŐlendiđi tm kayıt ortamları ve kiŐisel veri iŐlenmesine ynelik faaliyetlerde iŐbu Prosedr uygulanır.

1.3 Kısaltmalar ve Tanımlar

Alıcı Grubu:	Veri sorumlusu Őirket tarafından kiŐisel verilerin aktarıldıđı gerçekte veya tzel kiŐi kategorisi.
Aık Rıza:	Belirli bir konuya iliŐkin, bilgilendirilmeye dayanan ve zgr iradeyle aıklanan rıza.
Anonim Hale Getirme:	KiŐisel verilerin, baŐka verilerle eŐleŐtirilerek dahi hibir surette kimliđi belirli veya belirlenebilir bir gerçekte kiŐiyle iliŐkilendirilemeyecek hale getirilmesi.
alıŐan:	Őirket personeli.
Elektronik Ortam:	KiŐisel verilerin elektronik aygıtlar ile oluŐturulabildiđi, okunabildiđi, deđiŐtirilebildiđi ve yazılabildiđi ortamlar.
Elektronik Olmayan Ortam:	Elektronik ortamların dıŐında kalan tm yazılı, basılı, grsel vb. diđer ortamlar.
Hizmet Sađlayıcı:	Őirket ile belirli bir szleŐme erevesinde hizmet sađlayan gerçekte veya tzel kiŐi.
İliđili KiŐi:	KiŐisel verisi iŐlenen gerçekte kiŐi.
İliđili Kullanıcı:	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kiŐi ya da birim hari olmak zere veri sorumlusu organizasyonu ierisinde veya veri sorumlusundan aldıđı yetki ve talimat dođrultusunda kiŐisel verileri iŐleyen kiŐiler.
İmha:	KiŐisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun:	6698 Sayılı KiŐisel Verilerin Korunması Kanunu.
Kayıt Ortamı:	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt

Kişisel Veri:	sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri İşleme Envanteri:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, 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.
Kurul:	Kişisel Verileri Koruma Kurulu.
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.
Periyodik İmha:	Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Prosedür:	İşbu Kişisel Verileri Kayıt, Saklama ve İmha Prosedürü.
Veri İşleyen:	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Kayıt Sistemi:	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 Şirket'i.
Veri Sorumluları Sicil Bilgi Sistemi:	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu tarafından oluşturulan ve yönetilen bilşim sistemi.
VERBİS:	Veri Sorumluları Sicil Bilgi Sistemi.
Yönetmelik:	28.10.2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Prosedür kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Tablo 1: Sorumlu personel ve görev dağılımı

PERSONEL	GÖREVLİ	SORUMLULUK
Ad-Soyadı Unvan	KVK Komitesi sorumlusu	Her bir departmanın iş süreçlerinin saklama ve periyodik imha sürelerine uygun gerçekleşip gerçekleşmediğinin gözetimi
Adı-Soyadı Unvan	İrtibat Kişisi	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	İnsan Kaynakları Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Bilgi İşlem Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Muhasebe Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Satın Alma Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Fümigasyon Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Kimya Laboratuvarı Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Adı-Soyadı Unvan	Teknik Departman Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

Adı-Soyadı Unvan	Tütün Laboratuvarı Departmanı Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
---------------------	---	---

3. KAYIT ORTAMLARI

Kişisel veriler, Şirket tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> ▪ Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) ▪ Yazılımlar (ofis yazılımları ve Şirketçe kullanılan diğer yazılımlar) ▪ 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.) ▪ Çıkarılabilir bellekler (USB, Hafıza Kart vb.) ▪ Yazıcı, tarayıcı, fotokopi makinesi 	<ul style="list-style-type: none"> ▪ Kağıt ▪ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ▪ Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışanlar, çalışan adayları, ziyaretçiler, tedarikçiler, müşteriler, hizmet sağlayıcıları, diğer üçüncü kişiler, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1. Saklamaya İlişkin Açıklamalar

Kanun'un 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5. ve 6. maddelerinde ise kişisel verilerin işleme şartları sayılmıştır. Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süre kadar saklanır.

4.1.1. Kişisel Sağlık Verileri

Şirket tarafından toplanan ve saklanan çalışanlara ilişkin sağlık verileri, yalnızca Şirket bünyesinde görev alan işyeri hekimi tarafından işlenebilecek ve işyeri hekimine ait özel odada ve kilitle dolaplarda saklanabilecektir.

Zorunlu hallerde, söz konusu sađlık verilerinin bulunduđu dolaba eriřim, yalnızca İrtibat Kiřisi tarafından sađlanabilecek, bařkaca hiřbir alıřan veya yetkilinin söz konusu verilere eriřimi söz konusu olmayacak ve verilerin kullanılması ile ilgili yapılması gereken iřin sona ermesi ile birlikte, söz konusu veriler aynı yere kaldırılacak ve aynı řekilde kilitli olarak muhafaza edilecektir.

4.1.2. Diđer Özel Nitelikli Kiřisel Veriler

Gerek řirket alıřanları gerekse 3. Kiřilere ait olan özel nitelikli kiřisel veriler, iřlenme sebebine bakılmaksızın, yalnızca İrtibat Kiřisinin eriřebileceđi ve sadece bu verilerin yer aldıđı belge, kayıt vb. ortamları saklamak üzere özel olarak ayrılmıř kilitli dolaplarda muhafaza edilecektir.

4.1.3. Saklamayı Gerektiren Hukuki Sebepler

řirket'in faaliyetleri erevesinde iřlenen kiřisel veriler, ilgili mevzuatta öngörülen süre kadar řirket nezdinde muhafaza edilir.

Bu kapsamda kiřisel veriler;

- 6698 sayılı Kiřisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borlar Kanunu,
- 4733 sayılı Tütün ve Alkol Piyasası Düzenleme Kurumu Teřkilat ve Görevleri Hakkında Kanun ve ikincil mevzuatı,
- 213 sayılı Vergi Usul Kanunu ve ilgili diđer vergi mevzuatı,
- 5510 sayılı Sosyal Sigortalar ve Genel Sađlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İřlenen Sularla Mücadele Edilmesi Hakkında Kanun,
- 6331 sayılı İř Sađlığı ve Güvenliđi Kanunu,
- 4857 sayılı İř Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- İřyeri Bina ve Eklentilerinde Alınacak Sađlık ve Güvenlik Önlemlerine İliřkin Yönetmelik

Bu kanunlar uyarınca yürürlükte olan diđer ikincil düzenlemeler erevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.4. Saklamayı Gerektiren İřleme Amaları

řirket, faaliyetleri erevesinde iřlemekte olduđu kiřisel verileri ařađıdaki amalar dođrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek,
- İř sađlığı ve güvenliđi süreçlerini yürütmek,
- İhracat süreçlerini gerekleřtirmek,
- řirket güvenliđini sađlamak,
- Bilgi teknolojileri süreçlerini yürütmek,
- Sistem eriřimini ve güvenliđini sađlamak,
- İmzalanan sözleşmeler ve protokoller neticesinde iř ve edimleri ifa edebilmek,
- Müřteri raporlamalarını yapabilmek,
- Yasal düzenlemelerin gerektirdiđi veya zorunlu kıldıđı řekilde, hukuki yükümlölüklerin yerine getirilmesini sađlamak,
- řirket ile iř iliřkisinde bulunan gerek/tüzel kiřilerle irtibat sađlamak,
- Yasal raporlamalar yapmak,

- İleride doğabilecek hukuki uyumsuzluklarda delil olarak ispat yükümlülüğünü yerine getirmek.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.3. İmhanın Tutanak Altına Alınması

Her bir imha sürecinin sonunda ilgili imha işlemi, bir tutanak ile imha sürecini gerçekleştiren departman sorumlusu ve KVK Komite sorumlusu tarafından kayıt altına alınır. Söz konusu tutanak 5 yıl süreyle Şirket bünyesinde saklanır.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12. maddesiyle 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde ve Şirket tarafından ihdas edilen Özel Nitelikli Kişisel Veri İşleme Prosedürü kapsamında, tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Sızma (Penetrasyon) testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirket'in bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel

Açıklama [OE1]: IT tarafından kontrol edilerek, reel olarak yerine getirilemeyecek tedbirler çıkarılmalıdır.

güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurul'a bildirmek için Şirket tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Şirket internet sayfasına erişimde güvenli protokol (https) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı bir prosedür belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yaptırılmakta ve test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

5.2 İdari Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi,

kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.

- Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanmak üzere gerekli hükümler Disiplin Yönetmeliğine eklenmiştir.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Şirket tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler Şirket tarafından Tablo 3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süresi sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir, arşivde kilitli dolaplarda saklanır ve bu dolapların kilitleri yalnızca evrak arşivinden sorumlu birim yöneticisinde bulunur.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süresi sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Şirket tarafından Tablo 4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel verilerin yok edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenler, kâğıt kırpma makinelerinde geri döndürülemez şekilde yok edilir.
Optik/Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıttadır;
- Süreç bazında saklama süreleri ise Kişisel Veri Kayıt, Saklama ve İmha Prosedürü'nde yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Şirket tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi işbu Prosedür'ün 2. maddesinde belirtilen sorumlular tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

Süreç	Saklama Süresi	İmha Süresi
Mevcut personel için her türlü İK formları ve belgeleri	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Personel özlük dosyası	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşe alım	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan aday özgeçmişleri	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bordrolama	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel özel sağlık sigorta işlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş sağlığı ve güvenliği uygulama ve eğitim kayıtları	İş ilişkisinin sona ermesine müteakip 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Aday tedarikçi listesi	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Üçüncü kişilerle imzalanan sözleşmeler	Sözleşmenin sona ermesini müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Raporlamaları	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Laboratuvar Analizleri	3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kayıt/Takip/Log Sistemleri	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Dosya Paylaşım Kullanılması – Dosya Yönetim Sunucusu, Kimlik doğrulama ve izin hizmetleri vb.	Kullanıcı hesabının kapatılmasından sonra 1 yıl içinde	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hesap ve erişim yönetimi, proje dokümanları oluşturma, sistem	4 yıl	Saklama süresinin bitimini takip eden ilk periyodik

hizmetleri ve uygulama yönetimi		imha süresinde
Güvenlik kamera görüntüleri	Görüntünün alındığı tarihten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ödeme işlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket yönetim kurulu üyeleri ve imza yetkililerine ait bilgiler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Banka kredileri sözleşme takibi	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Teminat mektubu ve raporlama	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bakım, servis ve hizmet yönetimi ve anlık hizmet alımları	Son siparişten sonra 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Depo çalışmaları raporlaması	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Gayrimamul ürün testi	4 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Aday tedarikçi listesi	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İhracat hazırlığı	Son siparişten sonra 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi yönetimi	3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

Yönetmelik'in 11. maddesi gereğince Şirket, periyodik imha süresini altı (6) ay olarak belirlemiştir. Buna göre, Şirket nezdinde her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. PROSEDÜR'ÜN YAYINLANMASI VE SAKLANMASI

Prosedür, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Şirket nezdinde dosyasında saklanır.

10. PROSEDÜR'ÜN GÜNCELLENME PERİYODU

Prosedür, mevzuat değişikliklerinde ve ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

11. PROSEDÜR'ÜN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Prosedür, 01.01.2020 tarihi itibarıyla yürürlüğe girmiştir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Prosedür'ün ıslak imzalı eski nüshaları Şirket yetkili organlarınca iptal edilir ve en az beş (5) yıl süre ile Şirketçe dosyasında saklanır.