İçindekiler

1. GİRİŞ

1.1. Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası ("***Politika***"), 6698 sayılı Kişisel Verilerin Korunması Kanunu ("***Kanun***") ve Kanun'un ikincil düzenlemesini teşkil eden Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("***Yönetmelik***") uyarınca yükümlülüklerimizi yerine getirmek ve **ULUSOY RAYLI SİSTEMLER ANONİM ŞİRKETİ** ("***Şirket***") olarak tarafımızca gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Şirketimiz, kişisel verilerin işlendiği herhangi bir iş sürecine dahil olan çalışan adayı, çalışan, yönetici, ortak, tedarikçi, müşteri, ziyaretçi ve diğer üçüncü kişilere ait kişisel verilerin, T.C Anayasası, uluslararası sözleşmeler ve ilgili sair mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirketimiz tarafından bu doğrultuda hazırlanmış olan Politika'ya uygun olarak gerçekleştirilir.

1.2. Kapsam

Şirketin kişisel veri işlediği iş süreçlerine dahil olan gerçek kişilere ait kişisel veriler ve özel nitelikli kişisel veriler, işbu Politika kapsamındadır.

Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla kişisel verilerin işlendiği sistemlerde yer alan tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

Kişisel Veri İşleme Envanteri, işbu Politika'nın ayrılmaz bir parçası olup, Şirketin veri işleme faaliyetlerine, işlenen veri kategorilerine, verileri işlenen ilgili kişi gruplarına ve imha sürelerine ilişkin bu Politika'da yer verilen açıklamalar Kişisel Veri İşleme Envanterinin özeti niteliğindedir.

1.3. Kısaltmalar ve Tanımlar

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 hâle getirilmesi*
Çalışan adayı	:	*Şirket personel adayı*
Çalışan	:	*Şirket personeli*
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*
İlgili Kişi	:	*Kişisel verisi işlenen gerçek kişi*
İmha	:	*Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi*
Kanun	:	*6698 sayılı Kişisel Verilerin Korunması Kanunu*
Kayıt Ortamı	:	*Tamamen ya da 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 saklanması 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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*
Kurul	:	*Kişisel Verileri Koruma Kurulu*
Kurum	:	*Kişisel Verileri Koruma Kurumu*
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	:	*Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi*
Politika	:	*Kişisel Verileri Saklama ve İmha Politikası*
Veri İşleyen	:	*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*
Veri Sorumlusu	:	*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*
Veri Kayıt Sistemi	:	*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*
Veri Sorumluları Sicil Bilgi Sistemi	:	*Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi*
VERBİS	:	*Veri Sorumluları Sicil Bilgi Sistemi*
İrtibat Kişisi	:	*Veri Sorumlusu tarafından Kanun ve Kanuna dayalı olarak çıkarılmış ve çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak Kurum ile iletişimi sağlamak amacıyla Veri Sorumluları Siciline kayıt esnasında bildirilen gerçek kişi*
Yönetmelik	:	*28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce Politika 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 olarak saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verileri saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de gösterilmiştir:

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	DEPARTMAN / BİRİM	GÖREV VE SORUMLULUK
İnsan Kaynakları Yetkilisi	İnsan Kaynakları	Politika ve prosedürlerin uygulanması için gerekli görev dağılımını yapmak, uygun gördüğü kişileri yetkilendirmek ve Şirket genelinde iş süreçlerinin Politika'da belirtildiği şekilde saklama ve imha sürelerine uygunluğunun sağlanmasından sorumludur.
İnsan Kaynakları Yetkilisi	İnsan Kaynakları	Politika'nın hazırlanması, güncellenmesi, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur. Periyodik imha döneminde kişisel veri imha sürecinin yönetiminin gerçekleştirilmesi, Politika'nın asgari olarak yıllık bazda gözden geçirilmesi, ilgili kişi tarafından kişisel verilerin silinmesi veya yok edilmesine ilişkin yapılan talep ve başvuruların takip edilmesinden sorumludur.
Bilişim Teknolojileri Uzmanı	Bilişim Teknolojileri Uzmanı	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.
İşyeri Hekimi – İş Güvenliği Uzmanı	İşyeri Hekimi ve İş Güvenliği Uzmanı	Görevi dahilinde olan özellikle çalışanların sağlık verileri ile ilgili süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yürütülmesinden sorumludur.

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

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
• **Sunucular** *(Yedekleme, e-posta, veri tabanı, web, dosya paylaşımı)* • **Yazılımlar** *(Şirketin kullandığı yazılımlar/sistemler)* • **File Server** • **Bilgi güvenliği cihazları** *(güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs programı)* • **Kişisel bilgisayarlar** (Masaüstü, dizüstü) • **Optik diskler** *(CD, DVD)* • **Çıkartılabilir bellekler** *(USB, Hafıza Kart)* • **Yazıcı, tarayıcı, fotokopi makinesi**	• **Birim dolapları** • **Manuel veri kayıt sistemleri** *(Formlar vb.)* • **Şirket Arşivi**

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Çalışan adayları, çalışanlar, yöneticiler, ortaklar, tedarikçiler, müşteriler ve ziyaretçiler başta olmak üzere ilişkide bulunulan üçüncü kişilere ve üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına/yetkililerine ait kişisel veriler Kanuna 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 verilerin *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. maddelerde ise kişisel verilerin işlenme şartları sayılmıştır.

Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, *ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.*

4.1.1. Saklamayı Gerektiren Hukuki Sebepler

Şirket faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler,

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 5411 sayılı Bankacılık Kanunu,

- 7201 sayılı Tebligat Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 3308 sayılı Mesleki Eğitim Kanunu,
- 4857 sayılı İş Kanunu,
- 193 sayılı Gelir Vergisi Kanunu,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2. Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- İnsan kaynakları süreçlerini yürütmek,
- Kurumsal iletişimi sağlamak,
- Kurum güvenliğini sağlamak,
- İmzalanan sözleşmeler ve protokoller kapsamında iş ve işlemleri ifa edebilmek,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- İş ilişkisi içerisinde bulunulan gerçek/tüzel kişiler ve kurum ve kuruluşlar ile irtibat sağlamak,
- Yasal raporlamalar yapmak,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü sağlamak.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler,

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin kişisel verilerinin silinmesi veya yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, Kanunda öngörülen süre içinde cevap vermemesi veya ilgili kişinin Şirketin verdiği cevabı yetersiz bulması hallerinde, ilgili kişinin Kurul'a şikayette bulunması ve bu şikayetin 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 ya da resen silinir, yok edilir veya anonim hale getirilir.

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 Kanun'un 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurum tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirket tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

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

- Kişisel verilerin arşivlendiği fiziksel ortamların güvenliğinin sağlanması için bahse konu veriler, kilitli dolaplarda muhafaza edilmekte; erişim yetki ve rol dağılımları için politikalar oluşturulmakta ve uygulanmaktadır.
- Şirket bünyesindeki bilgisayarlarda zararlı yazılım tespit eden, önleyen, tespit edilen zararlı yazılımları silen yazılımlar kullanılmakta ve zararlı yazılım tespit eden veri tabanları güncel tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Yetki kontrol listesi ile Şirkete ait bilgisayarlarda yer alan dosyalar üzerinde yetkililer belirlenmiştir.
- Sızma (Penetrasyon) testleri ile Şirketin 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.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal *(sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi yerel alan ağını oluşturan kenar anahtarların fiziksel 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, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, 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 testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamlar için yeterli güvenlik önlemleri alınmakta, fiziksel güvenlik 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 kritopgrafik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Özel nitelikli kişisel verilerin 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:

- Çalışanlar, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin muhafazasının sağlanması için alınacak idari tedbirler ve Kanuna uyum süreci hakkında eğitim almaktadır.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Şirket bünyesinde Kişisel Veri İşleme Envanteri hazırlanmıştır.
- Şirket faaliyetleri kapsamında imzalanan sözleşmeler veri güvenliği hükümleri içermekte veya veri güvenliğine ilişkin protokoller imzalanmaktadır.
- Kişisel verilerin korunmasına ilişkin olarak çalışanlar ile "Kişisel Verilerin Korunmasına İlişkin Personel Sözleşmesi" akdedilmektedir.
- Kişisel veri güvenliğine ilişkin politika ve prosedürler hazırlanmış ve yürürlüğe koyulmuştur.
- Veri İhlali Müdahale Planı hazırlanmış ve yürürlüğe koyulmuştur.
- Şirket içi periyodik ve rastgele denetimler yapılmaktadır.
- KVKK uyum sürecinde yapılan analizlerle tespit edilen hususlarda iyileştirme için aksiyonlar alınmıştır.
- Özel nitelikli kişisel verilerin güvenliğine yönelik politika bulunmaktadır.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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

Silme: Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Yok Etme: Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

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

Şirket, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde, uygun yöntemi gerekçesini açıklayarak seçer.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler, Tablo-3'te belirtilen yöntemlerle silinir.

Tablo-3: Kişisel Verilerin Silinmesi

VERİ KAYIT ORTAMI	AÇIKLAMA
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre 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 süre sona erenler, veri tabanı 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 süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre 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, Tablo-4'te belirtilen yöntemlerle yok edilir.

Tablo-4: Kişisel Verilerin Yok Edilmesi

VERİ KAYIT ORTAMI	AÇIKLAMA
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler (CD, DVD, Blu-Ray, Teyp kartuşu)	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır.

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, 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.

Şirket, aşağıda örneklendirilen kişisel verilerin anonim hale getirilmesi yöntemlerinden biri veya birkaçını verilerin saklandığı ortam veya işleme yöntemine bağlı olarak kullanabilmektedir.

Değer düzensizliği sağlamayan anonim hale getirme yöntemleri	• Değişkenleri çıkartma • Kayıtları çıkartma • Alt ve üst sınır kodlama • Bölgesel gizleme • Örnekleme
Değer düzensizliği sağlayan anonim hale getirme yöntemleri	• Mikro-Birleştirme • Veri Değiş-Tokuşu • Gürültü Ekleme • Tekrar Örnekleme
Anonim hale getirmeyi kuvvetlendirici istatistik yöntemler	• K-Anonimlik • L-Çeşitlilik • T-Yakınlık

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 Kişisel Veri İşleme Envanterinde;
- Süreç bazında saklama süreleri ise işbu Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde İrtibat Kişisi tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için resen silme, yok etme veya anonim hale getirme işlemi İrtibat Kişisi tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş başvuru süreçlerinin yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan kaynakları süreçlerinin yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

İş sağlığı ve güvenliği süreçlerinin yürütülmesi (İş Sağlığı ve Güvenliği Uzmanı ve İşyeri Hekimi tarafından tutulan kayıtlar)	İş ilişkisinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim faaliyetlerinin yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşme süreçlerinin yürütülmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans ve muhasebe işlerinin yürütülmesi	Faaliyetin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi kayıtlarının oluşturulması	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera kayıtları	1 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

**İlgili kişi tarafından kişisel verinin silinmesi veya yok edilmesi adına Şirkete başvuruda bulunulması ve talebin Şirket tarafından kabulü halinde, imha işlemi talebin Şirkete ulaştığı tarihten itibaren 30 gün içerisinde gerçekleştirilir.*

8. PERİYODİK İMHA SÜRESİ

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

9. POLİTİKA'NIN YAYIMLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve internet sitesinde olmak üzere iki farklı ortamda yayımlanır. Basılı kağıt nüsha İnsan Kaynakları Birimi tarafından saklanır.

10. POLİTİKA'NIN YÜRÜRLÜĞÜ VE GÜNCELLEME PERİYODU

İşbu Politika, …./……/…….. tarihi itibariyle yürürlüğe girmiştir.

İşbu Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

No	Versiyon	Tarih	Hazırlayan	Değişiklik
1	1.0	…….	İrtibat Kişisi	……..
2	2.0	…….	İrtibat Kişisi	……..
3.	3.0	…….	İrtibat Kişisi	……..