

KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI



İçindekiler

1.Amaç 3	
2.Kapsam.....	3
3.Tanımlamalar ve Kısaltmalar	3
4.Kayıt Ortamları.....	5
5.Uygulama	6
5.1.Saklama Gerektiren Sebeplere İlişkin Açıklamalar	6
5.3.Uygulanan Teknik ve İdari Tedbirler	8
5.3.1 İdari Tedbirler	8
5.3.2 Teknik Tedbirler.....	8
5.4.Veri Silme, Yok Etme ve Anonim Hale Getirme.....	10
5.4.1Kişisel Veri Silme	11
5.4.2 Kişisel Veri Yok Etme	11
5.4.3 Kişisel Veri Anonimleştirme.....	11
5.5.Veri Saklama ve İmha Süreleri ve Sorumluları.....	12
5.5.1Veri Saklama ve İmha Sorumluları.....	12
6.Sorumluluk	23
7.Güncelleme Kayıtları	24

his
tektstil

1. Amaç

İşbu politika His Tekstil Sanayi ve Ticaret Anonim Şirketi (“Şirket”) olarak veri sorumlusu sıfatıyla, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik’in 5 ve 6. maddelerinde öngörülen yükümlülüklerini yerine getirebilmesi, ayrıca temel insan hakkı olan kişisel verilerin korunması hakkına verdiğimiz yüksek önem sebebiyle, kişisel verilerin imha usul ve süreçlerini açıklamak amacıyla hazırlanmıştır.

2. Kapsam

Bu politika, Şirketimiz ile bağlantılı tüm tarafların otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla, elektronik ortamda ya da basılı dokümanlarla işlenen tüm kişisel verilerini kapsamaktadır.

3. Tanımlamalar ve Kısaltmalar

Bu doküman içinde geçen kısaltmalar ve tanımlar tabloda gösterildiği gibidir:

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Şirket	1. Organize Sanayi Bölgesi 18. Cadde No:58 Melikgazi/Kayseri adresinde mukim His Tekstil Sanayi ve Ticaret Anonim Şirketi.
Çerez (Cookie)	Kullanıcıların bilgisayarlarına yahut mobil cihazlarına kaydedilen ve ziyaret ettikleri web sayfalarındaki tercihleri ve diğer bilgileri depolamaya yardımcı olan küçük dosyalardır.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
İrtibat Kişisi	Türkiye’de yerleşik olan tüzel kişiler ile Türkiye’de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişi. (İrtibat kişisi Veri Sorumlusunu temsile yetkili değildir. Adından anlaşılacağı üzere yalnızca veri sorumlusu ile ilgili kişilerin ve Kurumun iletişimini “irtibatı” sağlamak üzere görevlendirilen kişidir.)

Kanun/KVKK	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
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 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.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
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 veriler ile biyometrik ve genetik veriler.
Periyodik İmha	Kişisel verilerin işlenmesi için aranan şartların 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	Şirket tarafından oluşturulan kişisel veri koruma politikası.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği.
Kaynak:	6698 sayılı Kişisel Verilerin Korunması Kanunu- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik - Veri Sorumluları Sicili Hakkında Yönetmelik - Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ - Veri Sorumlusuna Başvuru ve Usul Esasları Hakkında Tebliğ Veri sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

4. Kayıt Ortamları

Kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> ✓ Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar (Logo Go, CRM) ✓ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ✓ Ağ üzerinde veri saklama için kullanılan disk sürücüler (NAS) ✓ MS Office dosyaları 	<ul style="list-style-type: none"> ✓ Kağıt ✓ Manuel veri kayıt sistemleri (anket formları, başvuru formları, ziyaretçi giriş defteri vb.) ✓ Yazılı, basılı, görsel ortamlar

✓ Şirket bilgisayarları (Masaüstü, dizüstü)	
✓ Mobil cihazlar (telefon, tablet vb.)	
✓ Optik diskler (CD, DVD vb.)	
✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.)	
✓ Yazıcı, tarayıcı, fotokopi makinesi	

5. Uygulama

Şirket benimsemiş olduğu vizyon, misyon ve temel değerleri gereğince, idari süreçlerini ve iş süreçlerini bağlı olduğu mevzuatlar doğrultusunda yürütmek, hizmet verdiği kişilere en iyi deneyimi sağlamak için teknolojik kaynak ve altyapıları da kullanarak “veri minimizasyonu” prensibi çerçevesinde kişisel ve özel nitelikli kişisel verileri işler. Verilerin işlenmesinde kanunun 4. maddesinde belirtilen ilkeler ve 12. maddesi gereği alınması gereken tedbirler göz önünde bulundurularak işlem yapılır. Kayıt saklama ortamları, elektronik veriler için bilişim sistemi sunucuları, uygulamaları, kurumsal bilgisayar ve depolama ortamlarıdır, basılı dokümanlar için ise ofisler ve arşivlerdir.

5.1. Saklama Gerektiren Sebeplere İlişkin Açıklamalar

İlgili kişiye ait veriler, Şirketin hizmetlerinin sunulması, ticari faaliyetlerinin kesintisiz olarak sürdürülmesi, insan kaynakları süreçlerinin planlanması ve yürütülmesi, müşteri ilişkilerinin yürütülmesi, çalışan hak ve menfaatlerinin planlanması, tedarik ve iş ortağı süreçlerinin planlanması ve yürütülmesi, etkin iletişimin sağlanması, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde hukuki yükümlülüklerin yerine getirilmesi, sektöre özgü yükümlülüklerin yerine getirilmesi, gerekli kalite ve standart denetim süreçlerinin yerine getirilmesi, kamu kurum ve kuruluşlarına bilgi verilmesi, kurumsal iletişimin sağlanması, güvenliğin sağlanması, istatistiksel çalışmaların yapılması, analiz çalışmalarının yapılması, raporlama çalışmalarının yapılması, imzalanan sözleşme ve protokollerin yüklediği edimlerin ifa edilmesi, İSG mevzuatının gerektirdiği şartların yerine getirilmesi, ileride doğabilecek hukuki uyuşmazlıklarda delil olarak kullanılması veya ispat yükümlülüğünün yerine getirilmesi, yazılı, basılı ve elektronik dergi ve bülten çalışmalarının yapılması, eğitim süreçlerinin planlanması, arşiv süreçlerinin işletilmesi, tedarik zincirinin yürütülmesi amaçlarıyla aşağıda yer alan veri işleme şartları dahilinde İşbu Politikada belirtilen elektronik ya da elektronik olmayan ortamlarda güvenli ve hassas bir biçimde Kanun ve ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanır.

Saklamayı gerektiren hukuki sebepler aşağıdaki gibidir:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 4857 sayılı İş Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik,

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler.

Ayrıca kişisel veriler,

- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanması zorunlu olması,
- Kişisel verilerin Şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,

hukuki sebepleri ile de saklanmaktadır.

5.1.2 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,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.

- Çağrı merkezi süreçlerini yönetmek.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

5.2. İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

Yönetmelik uyarınca, aşağıda sayılan hallerde kişisel veriler veya özel nitelikli kişisel veriler, Şirket tarafından re'sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- İlgili kişinin, hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi ya da kurulun gereğinin yapılması yönünde karar vermesi.

5.3. Uygulanan Teknik ve İdari Tedbirler

Şirket, bünyesinde kanunun 7'nci ve 12'nci maddesi göz önünde bulundurularak veri saklamada ve imhada teknik ve idari tedbirler alır. Alınan tedbirler aşağıda belirtildiği gibidir;

5.3.1 İdari Tedbirler

- Şirket bünyesinde KVK Komitesi kurulması ve işletilmesi,
- Şirket personelleri ve ilgili taraflar ile taahhünameler ve gizlilik sözleşmelerinin imzalanması,
- İş süreçleri üzerinde risk analizlerinin gerçekleştirilmesi,
- Kişisel veri envanterlerinin oluşturulması,
- KVK politika ve prosedürlerinin işletilmesi,
- Bilgi güvenliği ve kişisel veri işleme faaliyetleri hakkında eğitimlerin düzenlenmesi ve değerlendirilmesi,
- Çalışan bilgisayar vb. araç gereçlerine yetkisiz erişimlerin önüne geçmek adına söz konusu araç ve gereçleri yalnızca yetkili kişilerin kullanması,
- Şirket içi ya da bağımsız denetimler ile faaliyetlerin gözden geçirilmesi,
- Yapılan işlemler için objektif delil üretecek kayıtların oluşturulması,

5.3.2 Teknik Tedbirler

- Sızma 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.
- Sistemler üzerinde yazılımsal değişiklik ve/veya güncelleme yapılacağı zaman denemeler test ortamında yapılmakta, varsa güvenlik açıkları tespit edilerek gerekli tedbirler alınmakta ve yapılacak değişikliğe son hali bu işlemlerin ardından verilmektedir.
- Şirketin 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, 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 tedbirlerle ilgili teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- 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 Kurula bildirmek için Şirket tarafından buna uygun hazırlık çalışmaları yapılmıştır.
- 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 politika 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 yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- 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.

5.4. Veri Silme, Yok Etme ve Anonim Hale Getirme

Veri işleme şartlarının ortadan kalkması halinde, kişisel veriler Şirket tarafından kendiliğinden veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta ilgili kişi tarafından Şirket'e başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılır ve ilgili kişiye bilgi verilir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir,
- Durum, şartlar ve mevzuat gereği ilgili kişinin talep ettiği imha usulünün yerine başka bir imha usulünün kullanılması gerekteyse, durum ilgili kişiye verilecek cevapta açıklanarak, kullanılması lazım gelen usul ile imha gerçekleştirilir,
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri kendiliğinden silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilir. Ancak, ilgili kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilir.

İlgili kişinin Kanun'un 11. maddesinde gösterilen hakları kapsamında yaptığı başvurularda verilecek cevaplar ücretsiz olarak karşılanır. Her ne kadar cevabın ücretsiz verilmesi temel ilke olsa da, verilecek cevabın ayrıca bir maliyet gerektirmesi durumunda Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in 7. maddesinde gösterilen ücretler Şirket tarafından ilgili kişiden talep edilebilecektir. İlgili madde şöyledir:

Ücret

MADDE 7 – (1) İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.

(2) Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

5.4.1 Kişisel Veri Silme

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.

5.4.2 Kişisel Veri Yok Etme

Fiziksel Ortamda Yer Alan Kişisel Veriler : Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler yakılarak veya kâğıt kırıpma makinelerinde geri döndürülemeyecek şekilde öğütülerek yok edilir.

Optik / Manyetik Medyada Yer Alan Kişisel Veriler: 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. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

5.4.3 Kişisel Veri Anonimleştirme

Şirket’de anonimleştirme için verinin bulunduğu ortam ve işleme türüne göre değişken çıkarma, gürültü ekleme, mikro birleştirme yöntemlerinden biri kullanılır.

Değişken Çıkarma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden “yüksek dereceli betimleyici” olanlar çıkarılarak mevcut veri seti anonim hale getirilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilir.

Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek

(büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanır.

5.5. Veri Saklama ve İmha Süreleri ve Sorumluları

5.5.1 Veri Saklama ve İmha Sorumluları

Unvan	Görev	Sorumluluk
Departman Sorumlusu	Şirket içi departmanların sorumluları	Biriminde veri saklama ve imha işlemlerini gerçekleştirmek, departmandakilerin politikaya uygun davranmasını sağlamak,
KVKK Birimi	Şirket içi kvkk birimi	Şirkette veri saklama ve imha işlemlerini gerçekleştirmek ve ilgili birimlerin veri saklama ve imha işlemlerinin gerçekleştirilmesine destek vermek,
Üst Yönetim	Şirket iş süreçlerinden sorumlu yöneticiler	Şirkette veri saklama ve imha işlemlerinin uygun gerçekleştirildiğinin denetlemek ya da denetlenmesini sağlamak,

5.5.2 Veri Saklama ve İmha Süreleri

Veri saklama ve imha süreleri kişisel veri envanterinde detaylı olarak gösterilir. Verilerin saklama ve imha süreleri aşağıda belirtildiği gibidir. Kişisel veriler, saklama şartlarının ortadan kalkması üzerine, ilgili kişinin talebi ile veya süresinin gelmiş olması durumunda periyodik imha süresinde Şirket'nin uygun göreceği imha usulü ile imha edilir. Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket'de her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

Kısaltmalar:

TBK: 6098 sayılı Türk Borçlar Kanunu

TTK: 6102 sayılı Türk Ticaret Kanunu

VUK: 213 sayılı Vergi Usul Kanunu

MK: 3213 sayılı Maden Kanunu

İSG: İş Sağlığı ve Güvenliği Mevzuatı

İİK: 2004 sayılı İcra ve İflas Kanunu

TCK: 5237 sayılı Türk Ceza Kanunu

HMK: 6100 sayılı Hukuk Muhakemeleri Kanunu

İK: 4857 sayılı İş Kanunu

AVK: 1136 sayılı Avukatlık Kanunu

Süreç (Faaliyet)	Faaliyetin Yasal Dayanağı	Silme Zamanı	Saklamanın Yasal Dayanağı	Yok Etme Zamanı
Personel adayı değerlendirmesi/ Mülakat	-	Aday işe alınırsa özlük dosyasına aktarılır. Aday işe alınmazsa başvuru tarihinden itibaren 2 yıllık sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Personelin özlük dosyası (özel sağlık sigortası bilgileri, zimmet formları, bordrolar, yemek kartı bilgileri, hak edişler, yan haklar ve edimler, iletişim bilgileri, disiplin kayıtları, eğitim-sertifika-beceri bilgileri, izinler, puantajlar, bildirdgeler, PDKS, özgeçmiş bilgileri, transkript, hesap bilgileri, sürücü belgesi, oturma izni işlemleri, teşvikler, sınavlar, fotoğraf, çalışma belgesi, sosyal yardım ve sosyal izinler, kesintiler, ödemeler, kayıtlar, seyahatler, sigorta bilgileri, plaka, araç vb.)	İK TBK	Sözleşmenin sona ermesinden itibaren 10 yıllık sürenin sonunda silinir.	İK TBK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Özgeçmiş bilgisi (çalışan)	3 yıllık süreler ile güncelliği sorgulanır, güncelliğinin yitirilmesiyle yenilenir veya yok edilir.			
Adli sicil kayıtları	5352 sayılı Adli Sicil Kanunu'ndaki sürelerle paralel bir şekilde güncelliği sorgulanır ve açık rızanın varlığı araştırılır.			

İlgili kişinin açık rızası ile işlenebilen kişisel veriler, ilgili kişinin açık rızasını geri alması söz konusu olduğunda imha edilir.				
Personelin kimlik bilgileri ile işe giriş ve işten çıkış bilgilerinin tutulması (çok tehlikeli işler grubu)	İK TBK İSG	Sözleşmenin sona ermesinden itibaren 40 yıllık sürenin sonunda silinir.	İK TBK İSG KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Personelin kimlik bilgileri ile işe giriş ve işten çıkış bilgilerinin tutulması (çok tehlikeli işler grubu harici)	İK TBK İSG	Sözleşmenin sona ermesinden itibaren 15 yıllık sürenin sonunda silinir.	İK TBK İSG KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Personel ödeme/kesinti işlemleri (İş avansı, Prim, İkramiye, Ayni Yardımlar, Banka Promosyonları, BES, Kıdem, İhbar, İkale, İştirak, Harcırah ve Seyahat Ödemeleri gibi)	İK TBK	Sözleşmenin sona ermesinden itibaren 10 yıllık sürenin sonunda silinir.	İK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
İşe giriş sağlık muayeneleri ve periyodik-poliklinik sağlık muayeneleri, istirahat raporları (çok tehlikeli işler grubu)	İSG İK TBK	Sözleşmenin sona ermesinden itibaren 40 yıllık sürenin sonunda silinir.	İSG İK TBK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
İşe giriş sağlık muayeneleri ve periyodik-poliklinik sağlık muayeneleri, istirahat raporları (çok tehlikeli işler grubu harici)	İSG İK TBK	Sözleşmenin sona ermesinden itibaren 15 yıllık sürenin sonunda silinir.	İSG İK TBK KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
İş kazası tutanağı, acil durum kayıt formu, iş kazası muayenesi ve olay kayıtları, sonuç bildirimleri	İSG	Kazaya karışan kişi ile sözleşme varsa: Sözleşmenin sona ermesinden itibaren 40	İSG KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha

(çok tehlikeli işler grubu)		yıllık sürenin sonunda silinir. Kazaya karışan kişi ile sözleşme yoksa: Kaza tarihinden itibaren 40 yıllık sürenin sonunda silinir.		işleminde yok edilir.
İş kazası tutanağı, acil durum kayıt formu, iş kazası muayenesi ve olay kayıtları, sonuç bildirimini (çok tehlikeli işler grubu harici)	İSG	Kazaya karışan kişi ile sözleşme varsa: Sözleşmenin sona ermesinden itibaren 15 yıllık sürenin sonunda silinir. Kazaya karışan kişi ile sözleşme yoksa: Kaza tarihinden itibaren 15 yıllık sürenin sonunda silinir.	İSG KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
İş Sağlığı ve Güvenliği dahilinde gerçekleştirilen eğitim kayıtları (çok tehlikeli işler grubu)	İK İSG	Sözleşmenin sona ermesinden itibaren 40 yıllık sürenin sonunda silinir.	İK İSG KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
İş Sağlığı ve Güvenliği dahilinde gerçekleştirilen eğitim kayıtları (çok tehlikeli işler grubu harici)	İK İSG	Sözleşmenin sona ermesinden itibaren 15 yıllık sürenin sonunda silinir.	İK İSG KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
El Kitabı, Yönetim Planı, Prosedür, Talimat	TBK İK	Güncelliğini yitirmesiyle silinir.	TBK İK	Silme tarihinden itibaren 3 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
İş Sağlığı ve Güvenliği haricinde gerçekleştirilen eğitim kayıtları	İK MK TBK	Sözleşmenin sona ermesinden itibaren 10 yıllık sürenin sonunda silinir.	İK MK TBK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

				edilir.
İSG Kurul toplantısı yapılması	İSG	Toplantı tarihinden itibaren 5 yıl süre sonra değerlendirilerek güncelliğini kaybedenler silinir.	İSG	Silme tarihinden itibaren 35 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
5237 sayılı Türk Ceza Kanunu kapsamında soruşturmayı gerektiren haller	Ceza zamanaşımı süresi kadar saklanır, bu sürenin sonunda ilk periyodik imha işleminde yok edilir.			
Dava/icra/arabuluculuk dosyalarının tutulması	AVK HMK İİK	Dosyanın kesinleşmesinden itibaren 10 yıllık sürenin sonunda silinir.	AVK HMK İİK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir. Ceza soruşturmasını gerektiren hususlarda ceza zamanaşımı süresinin bitimini takip eden ilk periyodik imha işleminde yok edilir.
Tanıtım filmi ve ilan çalışmaları/ Sosyal – kültürel organizasyon ve aktiviteler/ Özel gün etkinlikleri	-	İlgili süreçte kişisel veriye duyulan ihtiyaç ile güncellik gözetilir, ihtiyaç ve güncelliğin sonlanması ile mümkün olanlar silinir.	KVKK	İlgili kişinin açık rızası ile işlenebilen kişisel veriler, ilgili kişinin açık rızasını geri alması söz konusu olduğunda imha edilir.
Duyurular	-	Duyurunun güncelliğini yitirmesinden itibaren 1 ay sonra silinir.	KVKK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

				edilir.
Portal	-	-	KVKK	Portalde yayınlanan içeriğin güncelliğini yitirmesi ile yok edilir.
Sürece yayılı olmayan hizmet – mal – ürün alımları	TBK TTK	Alım tarihinden itibaren 1 yıllık sürenin sonunda silinir.	TBK TTK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Sürece yayılı olan hizmet – mal – ürün alımları (İhale/Teklif)	TBK TTK	İhale/Teklif sonucu olumlu ise sözleşmesel veya hukuki ilişkinin bitiminden itibaren 5 yıllık sürenin sonunda silinir. İhale/Teklif sonucu olumsuz ise ihale tarihinden itibaren 5 yıllık sürenin sonunda silinir.	TBK TTK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir. Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Gelen – giden kargo teslim alan ve teslim eden	-	Sürecin bitiminden itibaren 1 haftalık sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

Gelen – giden arama kayıtları	-	-	KVKK	Duyulan ihtiyacın ve güncelliğinin yitirilmesiyle yok edilir.
Fihrist – telefon ve e-posta adresleri (çalışan)	TBK	Sözleşmenin sona ermesinden itibaren 6 aylık sürenin sonunda silinir.	TBK KVKK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Kamera kayıtları	-	15 günlük süreyle üzerine yazılır	KVKK İK TBK	15 günlük süreyle üzerine yazılır
Log kayıtları	KVKK İK TBK	Kaydın alınmasından itibaren 2 yıllık sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Log kayıtları (5651 sayılı Kanun) / İnternet erişimi	5651 s.k.	-	KVKK 5651 s.k.	Kaydın alınmasından itibaren 2 yıllık sürenin sonunda imha edilir.
Çalışan adayının ve tedarikçinin konaklama ve ulaşım süreçleri	TBK	-		İşlem tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir. Tedarikçi ile ilişki devam ediyor ise ilişkinin bitiminden itibaren 10 yıllık sürenin sonunda

				imha edilir.
Ulaşım ve Konaklamalarının Programlanması, Çalışan Biletleme bilgileri tablosu	TBK İK	Sözleşmenin sona ermesinden itibaren 10 yıllık sürenin sonunda silinir.	TBK KVKK İK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Yönetim kurulu, Genel kurul, İcra kurulu kararı	TTK	Kararın alındığı yılı takip eden 10 yıllık sürenin sonunda silinir.	TTK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Denetim belgeleri	MK TTK VUK Ve sair kanun	Denetimin türü, maiyeti, denetim sonucunda alınacak aksiyonlar gözetilir. Her halükarda denetim tarihinden itibaren 10 yıllık sürenin sonunda silinir.	MK TTK VUK KVKK Ve sair kanun	Saklanmasına lüzum görülmeyen belgeler silme tarihinde imha edilir. Saklanmasına lüzum görülen belgelere şirketin ihtiyacı ve güncellik gözetilerek imha süresi belirlenir.
Faturalar (Sürece yayılı işlemler)	VUK TTK	Sürecin sonlanmasını takip eden 5 yıllık sürenin sonunda silinir.	VUK TTK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Faturalar (Sürece yayılı olmayan işlemler)	VUK TTK	Faturanın kesildiği yılı takip eden 5 yıllık sürenin sonunda silinir.	VUK TTK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

Tedarikçiler ile yürütülen süreç ve dokümanlar (Örn: tedarikçi ödemeleri, ödeme makbuzu, irsaliye, poliçe, mutabakat, hak ediş, icra yazıları, beyannameler, zeyilname, hizmet ve danışmanlık alımları, bildirgeler, formlar, imza sirküleri, mail order)	TBK VUK TTK	-	TBK VUK TTK KVKK	Tedarikçi ile sözleşmesel veya hukuki işlemin sona ermesinden itibaren 15 yılın sonunda imha edilir.
Teminat mektubu/ Çek	TTK	İlişkinin bitiminden itibaren 5 yıllık sürenin sonunda silinir.	TTK KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
GSM giderleri/ Araç giderleri	-	İşlemin gerçekleştiği yılı takip eden 1 yılın sonunda silinir.	TBK KVKK	Silme tarihinden itibaren 9 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Talep, şikayet ve memnuniyet süreci (sözleşmeden kaynaklanan)	TBK	Talebin veya şikayetin çözüme kavuşturulmasıyla silinir.	KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Talep, şikayet ve memnuniyet süreci (sözleşmeden kaynaklanmayan)	-	Talebin veya şikayetin çözüme kavuşturulmasıyla silinir.	KVKK	Silme tarihinden itibaren 3 yıllık süreyi takip eden ilk periyodik imha işlemi yok edilir.
Melbusat ve KKD	İSG	-	İSG	Bir sonraki KKD temini döneminde yok edilir.
Organizasyon şeması	-	Güncelliğini yitirmesiyle yok edilir.		

Acil durum planlamasının yapılması	İSG	Güncelliğinin yitirmesiyle silinir.	KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Düzenlenen veya katılım sağlanan kurumsal etkinliğin fotoğraflanması ve video oluşturulması	-	-	KVKK	Açık rıza dahilinde gerçekleştirilen ve imhası mümkün olanlar için açık rızanın geri alınmasını takip eden ilk periyodik imha işleminde yok edilir.
Cihaz (bilgisayar, mobil cihaz ve gsm hattı) zimmet formu	TBK İK	Sözleşmenin sona ermesinden itibaren 1 yıllık sürenin sonunda silinir.	TBK İK KVKK	Silme tarihinden itibaren 9 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Tapu Kayıtlarının Tutulması	TBK	Sözleşmenin sona ermesinden itibaren 1 yıllık sürenin sonunda silinir.	TBK KVKK	Silme tarihinden itibaren 9 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Personel servis listeleri oluşturulması	İK	Personelin servisten yararlanmasının sona ermesi ile silinir.	İK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Yatırımcı bilgi ve işlemleri	SPK ve sair kanun	Yatırımcı ile hukuki ve sözleşmesel ilişkinin bitiminden itibaren 10 yıllık sürenin sonunda silinir.	SPK ve sair kanun KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

İmza sirküleri	TTK ve sair kanun	Güncellik ve duyulan ihtiyaca göre belirlenir.	TTK ve sair kanun	Güncellik ve duyulan ihtiyaca göre belirlenir. Güncel olmayan ve ihtiyaç duyulmayanlar yok edilir.
TTK'dan kaynaklı üst yönetim raporlamaları	TTK	Rapor neticesinde işlem yapılırsa işlemin devam ettiği sürecinin bitiminden itibaren 10 yıllık sürenin sonunda silinir. Rapor neticesinde işlem yapılmazsa raporlamadan itibaren 10 yıllık sürenin sonunda silinir.	KVKK	Tüzel kişiliğin sona erme tarihinden itibaren 10 yıl sonra yok edilir.
TTK'dan kaynaklanmayan üst yönetim raporlama ve bilgilendirmeleri	-	Güncellik ve duyulan ihtiyaca göre belirlenir.	KVKK	Güncellik ve duyulan ihtiyaca göre belirlenir.
İmha tutanağı	KVKK	İmhanın gerçekleştirilmesinden itibaren 3 yıllık sürenin sonunda silinir.	KVKK	Tüzel kişiliğin sona erme tarihinden itibaren 10 yıl sonra yok edilir.
Gelen – giden evrak/ Şirket işleyişini ilgilendiren yazışmaların- evrakların takibi	Evrakın niteliğine göre işbu tabloda yer alan süreler uygulanır.			
E-posta içerikleri	E-postalar 6 aylık periyotlar halinde gözden geçirilir. E-postada kişisel veri ihtiva eden belge ve kayıtlara bakılarak işbu tabloda yer alan süreler uygulanır.			

Tabloda belirtilmeyen hususlar	İşbu tabloda belirtilmeyen süreçlere ait kişisel verilere yönelik saklama ve imha süreleri; kişisel veri ihtiva eden belge ve kayıtların saklanmak zorunda olduğu süre, faaliyet gösterilen sektörde teamül kabul edilen süreler, ilgili kişiler ile hukuki ilişkinin devam edeceği süre, hukuka ve dürüstlük kurallarına uygun olarak veri sorumlusunun meşru menfaatinin geçerli olacağı süre, kişisel verinin güncelliği gibi hususların göz önünde bulundurulması ve tablodan yararlanılarak belirlenir.
Birimler bazında saklama ve imha sürecinin işletilmesi	Saklama ve imha süreçleri işletilirken, ilgili birimden/birimlerden saklama ve imhaya konu kişisel veri veya kişisel veri ihtiva eden belge temin edilir. Saklama ve imha süreçleri ilgili birim/birimler ile koordineli bir şekilde işletilir.
İmhanın ertelenmesi	İşbu tabloda belirtilen saklama, silme, yok etme, anonim hale getirme zamanlarının sonuna gelindiğinde, saklama ve imhaya ilişkin değerlendirme yapılır. Değerlendirme sonucunda kişisel verinin (veya kişisel veri ihtiva eden belgenin) güncelliği, hukuki veya sözleşmesel ilişkinin ve yükümlülüklerinin devam etme durumu, kişisel veriye veya ilgili belgeye duyulan objektif ihtiyaç durumu değerlendirilerek saklama ve imha süreci işletilir veya makul bir süreye ertelenir. Bu işlem tutanak altına alınır. Tutanak, en az 3 yıl süre ile saklanır.

6. Sorumluluk

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 saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda gösterilmiştir.

Görev	Birim	Unvan
Dokümanın Hazırlanması:	KVKK Komitesi (Tüm çalışanların katkısı ile)	KVKK Komite Üyeleri
Dokümanın Kontrolü:	KVKK Komitesi	KVKK Komite Üyeleri
Dokümanın Onaylanması:	Üst Yönetim	Üst Yönetim Üyeleri
Dokümanın Yayınlanması:	Üst Yönetim	Üst Yönetim Üyeleri
Dokümanın Güncellenmesi:	İrtibat Kişisi	İnsan Kaynakları Müdürü
Dokümanın Uygulanması:	Tüm çalışanlar ve veri işleyenler	Tüm çalışanlar ve veri işleyenler
Dokümanın Yayından Kaldırılması:	Üst Yönetim	Üst Yönetim Üyeleri

7. Güncelleme Kayıtları

Güncelleme No	Tarih	Güncelleme Nedeni	Güncelleme Sayfa No	Güncellenen Bölüm