

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

## 1. AMAÇ

Veri sorumlusu sıfatıyla İstanbul Ticaret Sicil Müdürlüğü nezdinde 574900-0 sicil numarası ile kayıtlı olan ve “Oruçreis Mah. Vadi Cad. İstanbul Ticaret Sarayı Blok No: 108 İç Kapı No: 327 Esenler İstanbul” adresinde bulunan “Kıta Depolama ve Dağıtım Hizmetleri Ticaret Anonim Şirketi” (Kısaca “Şirket” olarak tanımlanacaktır) Şirketimizce hazırlanan “Kişisel Veri Saklama ve İmha Politikası” (Politika), 6698 sayılı Kişisel Verilerin Korunması Kanunu (**KVKK**) ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (**Yönetmelik**) başta olmak üzere ilgili mevzuat uyarınca Şirketi’in saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul, esas ve saklama sürelerini belirlemek amacıyla hazırlanmıştır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, **Şirket** tarafından bu doğrultuda hazırlanmış olan **Politikaya** uygun gerçekleştirilir.

## 2. KAPSAM

### 2.1. DÜZENLENEN KAYIT ORTAMLARI

**Şirket** bünyesinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerine uygun bir şekilde aşağıdaki kayıt ortamlarında hassas bir şekilde muhafaza edilir.

#### 2.1.1. Elektronik ortamlar:

- 2.1.1.1. Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım)
- 2.1.1.2. Yazılımlar (ofis yazılımları, portal, vb.)
- 2.1.1.3. MS office dosyaları Kişisel bilgisayarlar (masaüstü, dizüstü)
- 2.1.1.4. Şirket bilgisayarları (masaüstü, dizüstü)
- 2.1.1.5. Ağ cihazları
- 2.1.1.6. Mobil cihazlar ve içerisindeki saklama alanları (telefon, tablet vb.)
- 2.1.1.7. Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
- 2.1.1.8. Bulut sistemleri
- 2.1.1.9. Yazıcı
- 2.1.1.10. Fotoğraf makinesi
- 2.1.1.11. Kamera
- 2.1.1.12. Tarayıcı

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

- 2.1.1.13. Fotokopi makinesi
- 2.1.1.14. Parmak izi okuyucu gibi çevre birimler
- 2.1.1.15. Manyetik bantlar
- 2.1.1.16. Optik diskler (CD, DVD, vb.)
- 2.1.1.17. Çıkarılabilir diskler (USB, hafıza kartı, vb.)
- 2.1.1.18. Zimbra
- 2.1.1.19. Netsis
- 2.1.1.20. Oracle
- 2.1.1.21. File server
- 2.1.1.22. DHCP
- 2.1.1.23. Domain Controller
- 2.1.1.24. ERP sistemi
- 2.1.1.25. Cisco
- 2.1.1.26. Exchange Server
- 2.1.1.27. Roma
- 2.1.1.28. Ms dynamics
- 2.1.1.29. CRM sistemi
- 2.1.1.30. Muhasebe operasyon sistemi
- 2.1.1.31. SQL veri tabanı
- 2.1.1.32. MySQL veri tabanı
- 2.1.1.33. CRM Server
- 2.1.1.34. Nebim
- 2.1.1.35. ERP

## 2.2. Elektronik olmayan ortamlar:

2.2.1. Birim dolapları

2.2.2. Birim arşivi

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

2.2.3. Kurum arşivi

2.2.4. Arşiv

2.2.5. Muhasebe birimi

2.2.6. Kâğıt

2.2.7. Yazılı, basılı, görsel ortamlar

2.2.8. Manuel veri kayıt sistemleri (anket formları, ziyaretçi defteri, aday değerlendirme formları)

### 3. SORUMLULUKLAR

#### 1. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Şirket bünyesinde bulunan kişisel veriler, Şirket 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 Politikada belirtilen elektronik ya da elektronik olmayan ortamlarda güvenli ve hassas bir şekilde saklanır.

Şirket bünyesinde bulunan kişisel veriler, aşağıda yer alan veri işleme şartlarının ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine imha edilir.

- Açık rızanın varlığı,
- Kanun hükmünün varlığı,
- Fiili imkânsızlık nedeniyle açık rızanın alınamaması,
- Sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

- İlgili kişinin kişisel verisinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşuluyla veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması.

## 2. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerekğinde veri maskeleyme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri envanteri hazırlanmıştır.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler verileri şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

### 3. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Kişisel verileri imha etmeye (*silmeye, yok etmeye ve anonim hale getirmeye*) yönelik **Şirket** bünyesinde bulunan uygulamalar aşağıdaki gibidir:

#### Kişisel Verilerin Silinmesi

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.
- Fiziki olarak kâğıt, dosya, klasör ortamında bulunan kişisel veriler; ilgili kullanıcıların (arşiv/saklama sorumlusu haricinde diğer tüm çalışanlar) erişemeyeceği, ulaşamayacağı ve girip inceleme yapamayacağı arşiv/saklama/depolama alanlarına ya da bu alanların ilgili bölümlerine

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

depolanır. Burada önemli olan ilgili kullanıcıların bu muhafaza alanlarına giremeyecek ve içeride bulunan kişisel veriler üzerinde herhangi bir işlem yapamayacak olmasıdır. Ya da saklama/depolama/arşiv alanlarının belirli bölümlerinde yine arşiv/saklama sorumluları haricinde hiç kimsenin erişemeyeceği kilitli alanlarda muhafaza edilerek silme işlemi gerçekleştirilebilir.

- Merkezi sunucuda yer alan ofis dosyaları, dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması ile gerçekleştirilmektedir.
- Taşınabilir medyada bulunan kişisel veriler (örneğin flash tabanlı saklama ortamında bulunan veriler) ise şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.
- Veri tabanlarında bulunan kişisel veriler, ilgili satırların/sütunların ya da tablo içerisinde yer alan hücrelerin veri tabanı komutları ile (DELETE vb.) silinmektedir.

### Kişisel Verilerin Yok Edilmesi

- Yerel sistemler üzerindeki kişisel verilerin yok edilmesi de-manyetize etme (medyanın özel bir cihazdan geçirilerek yüksek bir değerde manyetik alana maruz bırakılması), fiziksel yok etme (Medya ve manyetik medyanın eritilmesi, yakılması, öğütücülerin kullanılması) ve üzerine yazma yöntemiyle yok edilmektedir.
- Çevresel sistemler üzerindeki kişisel verilerin yok edilmesi; Ağ cihazları (switch, router vb.), Flash tabanlı ortamlar/sabit disklerin (ATA “SATA, PATA vb.”, SCSI “SCSI Express vb.), Manyetik bant, Manyetik disk gibi üniteler, Mobil telefonlar (Sim kart ve sabit hafıza alanları), Veri kayıt ortamı çıkartılabilir ya da sabit olan yazıcı ve parmak izli kapı geçiş sistemi gibi çevre birimler, Optik diskler olarak belirtebileceğimiz çevresel kayıt sistemleri dijital ortam ise ürün özelliği olarak destekleniyorsa <block erase> gibi yok etme komutunu kullanmak, dijital ortamın ürün özelliği olarak desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da "de-manyetize etme, fiziksel yok etme, üzerine yazma" olarak belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak, son olarak dijital ortam değil ise "de-manyetize etme, fiziksel yok etme, üzerine yazma" yöntemlerin uygun bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- Kâğıt ve mikrofiş ortamlarında bulunan kişisel veriler bulunduğu kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan, bu verilerin bulunduğu ana ortamın yok edilerek imha işlemi gerçekleştirilmektedir.
- Bulut ortamında bulunan kişisel veriler şifrelenerek saklanmakta ve imha süresi geldiğinde yok etme komutu uygulanmaktadır.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

### Kişisel Verilerin Anonim Hale Getirilmesi

- Maskeleye yöntemi ile veri sahibinin tanımlanmasını sağlayan temel belirleyici bilgiler (örn: isim, soyisim, tckn) çıkartılarak anonimleştirme gerçekleştirilmektedir.
- Toplulaştırma yöntemi ile kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek bir şekilde (örn: 25 ile 30 yaş aralığındaki kişilerden gelen iş başvurusunun daha fazla olması) çıkartılarak anonimleştirme gerçekleştirilmektedir.
- Veri Türetme yöntemi ile kişisel verilerin içeriğinden daha genel bir içerik oluşturularak ve kişisel verinin herhangi bir şekilde bir kişiyle bağdaştırılmayacak şekilde (örn: doğum tarihleri yerine yaş yazılması) anonim hale getirme gerçekleştirilmektedir.

#### a) Değer Düzensizliği Sağlamayan Anonimleştirme Yöntemleri

Verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılarak anonimleştirilir. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini koruması sağlanır.

- **Değişkenleri Çıkarma:** Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan anonimleştirme yöntemidir.
- **Kayıtları Çıkarma:** Veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimleştirme kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.
- **Bölgesel Gizleme:** Veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmak için belli bir kayda ait değerlerin yarattığı kombinasyon ayırt edilebilir hale gelmesine yüksek ihtimalle sebep olabilecekse değer “bilinmiyor” olarak değiştirilir.
- **Genelleştirme:** İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Bu yöntem ile elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.
- **Alt ve Üst Sınır Kodlama:** Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak elde edilir.
- **Global Kodlama:** Alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya nümerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama şeklinde anonimleştirme yöntemidir.
- **Örnekleme:** Bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle kişilere dair isabetli tahmin üretme riski düşürülmüş olur.

#### b) Değer Düzensizliği Sağlayan Anonimleştirme Yöntemleri

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

Mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılarak anonimleştirilir. Veri kümesindeki değerler değişiyor olsa dahi toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

- **Mikro Birleştirme:** Veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.
- **Veri Değiş Tokuşu:** Kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının anonimleştirilmesidir.
- **Gürültü Ekleme:** Seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkartmalar yapılarak anonimleştirilir. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

### c) Anonimleştirmeyi Güçlendirici İstatistiksel Yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

- **K-Anonimlik:** Belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiş bir anonimleştirme istatistiksel yöntemidir.
- **L-Çeşitlilik:** K-Anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşmuştur. Bu yöntemde aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitlilik dikkate almaktadır. Örneğin kişilere ait ad soyad veya kimlik numarası anonimleştirilerek K-anonimlik uygulanmış olmakla birlikte posta kodu, yaş ve etnik köken bilgisi paylaşılmış olduğundan tespit edilebilme ihtimali bulunmaktadır. Bu bilgileri de maskeleyen yöntemi ile anonimleştirerek dış bilgiye sahip kullanıcının tahmin gücünü azaltmıştır.
- **T-Yakınlık:** L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denilmektedir.

- Kurumların kendi takdirleri sonucu anonim hale getirme kararları bu kapsamda, anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmelidir.

#### 4. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BİRİMLERİ VE GÖREV TANIMLARI

Personel	Birim	Görev tanımı
Kd. Danışman	Operasyon	Kişisel verilerin imha edilmesi.
Avukat	Hukuk	İlgili kişilerin taleplerinin alınması, usulüne uygunluğunun kontrolü ve talebin cevaplanması.
Teknik Hz. Md.	Teknik Hizmetler Müdürlüğü	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması, elektronik ortamda bulunan kişisel verilerin imha süreci.
Mali İşler Personeli	Mali İşler	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
İnsan Kaynakları Personeli	İnsan Kaynakları	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

#### 5. SAKLAMA VE İMHA SÜRECİ VE SÜRELERE İLİŞKİN TABLO

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

**Şirket** bünyesinde bulunan kişisel veriler; ilgili mevzuatta öngörülmesi durumunda, mevzuatta belirtilen süre boyunca saklanmaktadır.

Kişisel verilerin işleme amacı sona ermiş, ilgili mevzuat ve **şirketin** belirlediği saklama süresinin de sonuna gelmişse, kişisel veriler olası hukuki uyumsuzlukların çözümlenmesi, yetkili kamu kurum ve kuruluşların hukuka uygun taleplerinin karşılanması veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi amacıyla saklanmaktadır.

İşlenen kişisel veriler, gerçekleştirilen faaliyet veya sürecin bitiminden itibaren Politikada belirtilen süreler kadar saklanır.

**Saklama süreleri**, silme zamanı ve yok etme zamanı olarak ikiye ayrılmaktadır.

**Silme**, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade etmektedir.

**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 kişileri ifade etmektedir.

**Yok etme**, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesini ifade etmektedir. Depolanan/yedeklenen kişisel veriler, belirli süreler sonunda yok edilir.

**Anonim hale getirme**, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade etmektedir.

**Silinen kişisel veriler, yok edilme zamanına kadar olan süre zarfında;**

- **Olası hukuki uyumsuzlukların çözümlenmesi,**
- **Yetkili kamu kurum ve kuruluşların hukuka uygun taleplerinin karşılanması,**
- **Kişisel veriye bağlı bir hakkın ileri sürülebilmesi**

**amaçlarıyla yedeklenir. Yedeklenen kişisel verilere başkaca bir amaçla herhangi bir erişim sağlanmaz.**

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

## ÖRNEK SAKLAMA VE İMHA SÜRECİ

### ÖRNEK:

Süreç (Faaliyet): Personel özlük dosyalarının tutulması

Silme zamanı (erişim yetkisinin kaldırılması): Sözleşmenin sona ermesinden itibaren 5 yıl

Yok etme zamanı: Silme zamanının tamamlanmasından itibaren 15'inci yılı takip eden ilk periyodik imha işlemi

### ÖRNEĞE YÖNELİK AÇIKLAMA:

Yukarıdaki örnekte, personelin özlük dosyasındaki kişisel verileri, personel ile kurulan sözleşmenin sona ermesinden itibaren toplamda 20 yıl süre ile saklanmaktadır.

Belirtilen 20 yıllık sürenin ilk 5 yılında, İnsan Kaynakları Birimi bu veriye erişebilir.

5 yılın sonunda bu veriye İnsan Kaynakları Birimi erişemez.

5 yılın sonunda bu veriye verinin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim erişebilir.

20 yılın sonunda bu veri, hiç kimsenin erişemeyeceği bir şekilde yok edilir.

### Kısaltmalar:

TBK : 6098 sayılı Türk Borçlar Kanunu

TTK : 6102 sayılı Türk Ticaret Kanunu

VUK : 213 sayılı Vergi Usul 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

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

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, bildirgeler, 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.
<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür		

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

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	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 işleminde yok edilir.
Personel ödeme/kesinti işlemleri (İş avansı, Prim, İkramiye, Ayni Yardımlar, Banka Promosyonları, BES, Kıdem, İhbar, İ kale, 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 işleminde yok edilir.
İşe giriş sağlık muayeneleri ve periyodik-poliklinik sağlık muayeneleri, istirahat raporları	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 işleminde yok edilir.
İş kazası tutanağı, acil durum kayıt formu, iş kazası muayenesi ve	İSG	Kazaya karışan kişi ile sözleşme varsa: Sözleşmenin sona ermesinden itibaren 15	İSG KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

Doküman No	
Yayın Tarihi	
Revizyon Tarihi	
Revizyon No	0
Evrak Sınıfı	Hizmete Özel

olay kayıtları, sonuç bildirimi		yıllık sürenin sonunda silinir. Kazaya karışan kişi ile sözleşme yoksa: Kaza tarihinden itibaren 15 yıllık sürenin sonunda silinir.		imha işleminde yok edilir.
İş Sağlığı ve Güvenliği dahilinde gerçekleştirilen eğitim kayıtları	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.
Sair çalışma alanları kontrol formları	TBK	Formun güncelliğini yitirmesiyle silinir.	TBK İK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Aşı, Pansuman ve Enjeksiyon Defteri, Poliklinik Defteri	İSG	Yeni deftere geçildiğinde silinir.	İSG TBK İK	Silme tarihinden itibaren 40 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.
5237 sayılı Türk Ceza Kanunu kapsamında	Ceza zımanışımı süresi kadar saklanır, bu sürenin sonunda ilk periyodik imha işleminde yok edilir.			
<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür		

Doküman No	
Yayın Tarihi	
Revizyon Tarihi	
Revizyon No	0
Evrak Sınıfı	Hizmete Özel

soruşturmayı gerektiren haller				
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 zamanasını 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

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

				imha işleminde yok edilir.
Portal	-	-	KVKK	Portalda yayınlanan içeriğin güncelliğini yitirmesi ile yok edilir.
Sürece yayılı olmayan hizmet – mal – ürün alımları	TBK TTK	Alım tarihinden itibaren 10 yıllık sürenin sonunda silinir.	TBK TTK	Silme tarihinden itibaren 5 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 10 yıllık sürenin sonunda silinir. İhale/Teklif sonucu olumsuz ise ihale tarihinden itibaren 5 yıllık sürenin sonunda silinir.	TBK TTK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir. Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

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.
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 işleminde yok edilir.
Kamera kayıtları	-	6 aylık süreyle üzerine yazılır	KVKK İK TBK	6 aylık 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 işleminde yok edilir.
Log kayıtları (5651 sayılı Kanun) / İnternet erişimi	5651	-	KVKK 5651	Kaydın alınmasından itibaren 2 yıllık sürenin sonunda imha edilir.

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

Doküman No	
Yayın Tarihi	
Revizyon Tarihi	
Revizyon No	0
Evrak Sınıfı	Hizmete Özel

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	TTK VUK Ve sair kanun	Denetimin türü, maiyeti, denetim sonucunda alınacak aksiyonlar gözetilir. Her halükârda denetim tarihinden itibaren 10 yıllık sürenin sonunda silinir.	TTK VUK KVKK Ve sair kanun	Saklanmasına lüzum görülmeyen belgeler silme tarihinde imha edilir. Saklanmasına lüzum görülen belgelere <b>şirketin</b> 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.

<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür
-------------------------------------	---	---------------------------------

Doküman No	
Yayın Tarihi	
Revizyon Tarihi	
Revizyon No	0
Evrak Sınıfı	Hizmete Özel

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 işleminde 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 işleminde yok edilir.
Talep, şikâyet ve memnuniyet süreci (sözleşmeden kaynaklanan)	TBK	Talebin veya şikâyetin çözüme kavuşturulmasıyla silinir.	KVKK	Silme tarihinden itibaren 10 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

Talep, şikâyet ve memnuniyet süreci (sözleşmeden kaynaklanmayan)	-	Talebin veya şikâyetin çözüme kavuşturulmasıyla silinir.	KVKK	Silme tarihinden itibaren 3 yıllık süreyi takip eden ilk periyodik imha işleminde 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.

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

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/ <b>Şirket</b> işleyişini ilgilendiren yazışmaların- evrakların takibi	Evrakın niteliğine göre tabloda yer alan süreler uygulanır.			

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

E-posta içerikleri	E-postalar 6 aylık periyotlar halinde gözden geçirilir. E-postada kişisel veri ihtiva eden belge ve kayıtlara bakılarak tabloda yer alan süreler uygulanır.
Tabloda belirtilmeyen hususlar	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 bulundurularak 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	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. PERİYODİK İMHA SÜRELERİ

Kişisel verilerin imha edilmesine ilişkin yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinir, yok edilir veya anonim hale getirilir. Periyodik imha, tüm kişisel veriler için **6 aylık zaman aralıklarında (Her yılın 2. ve 8. ayının sonunda) gerçekleştirilir.**

Silinen, yok edilen ve anonim hale getirilen verilere ilişkin işlemlerin bulunduğu tutanaklar diğer hukuki yükümlülükler hariç olmak üzere en az **3 yıl süre ile** saklanır.

<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

## 7. MEVCUT KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASINDA YAPILAN GÜNCELLEME İÇERİĞİ TABLOSU

GÜNCELLEME TARİHİ	GÜNCELLENMEDEN ÖNCE	GÜNCELLENDİKTEN SONRA

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

## 8. TUTANAK

Yukarıda belirtilen silme, yok etme ve anonim hale getirme işlemleri; işlemleri gerçekleştiren ilgili birim müdürü, şefi ve personelinin üçlü imzası ile hazırlanan tutanak ile kayıt altına alınır.

İmhayı Yapan Birim	
İmhayı Yapan Birim Müdürü	
İmhayı Yapan Birim Şefi	
İmhayı Yapan Birim Personeli	
İmha Karar Tarihi- Sayısı	
Kişisel Verinin Bulunduğu Yer	
İmha Yapılan Süreç	
Nakliyeyi Yapan Firma / Kişi	
Yükleme Yapılan Araçların Plakası	
İmhanın Yapıldığı Yer	
İmhanın Yapılış Şekli	

**İmhayı Yapan Birim Müdürü**

**İmhayı Yapan Birim Şefi**

**İmhayı Yapan Birim Personeli**

İmha İşleminde Rol Alan Diğer Kişiler Ad, Soyad, Unvan ve İmzaları:

Adı Soyadı	Unvan	İmza

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

#### 4. TANIMLAR VE KISALTMALAR

Kıta Depolama	Kıta Depolama ve Dağıtım Hizmetleri Ticaret Anonim Şirketi
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme/ Anonimleştirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Çalışan/ Personel	Şirket çalışanları, personeli veya stajyerleri
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 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 kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yollardan işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür
-------------------------------------	---	---------------------------------

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
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
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
Özel Nitelikli Kişisel Veri	İrk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler.
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.
Politika	Kişisel Veri Saklama ve İmha Politikası
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Şirket	KITA DEPOLAMA

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
EYS Ekip Üyesi	Yönetim Temsilcisi	Genel Müdür

	<b>KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI</b>	Doküman No	
		Yayın Tarihi	
		Revizyon Tarihi	
		Revizyon No	0
		Evrak Sınıfı	Hizmete Özel

Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi, dizin.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesidir.
Yönetmelik	28 Ekim 2017 tarihinde Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

<b>HAZIRLAYAN</b> EYS Ekip Üyesi	<b>KONTROL EDEN</b> Yönetim Temsilcisi	<b>ONAYLAYAN</b> Genel Müdür
-------------------------------------	---	---------------------------------