KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. POLİTİKANIN AMACI

Hazırlanan bu Kişisel Veri Saklama ve İmha Politikası (‘‘Politika’’), 6698 sayılı Kişisel Verilerin Korunması Kanunu (‘‘KVKK’’ veya ‘‘Kanun’’) ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik (‘‘Yönetmelik’’) uyarınca yükümlülüklerimizi yerine getirmek, kişisel verilerin işlendikleri amaç için gerekli olan azami saklama ve imha sürelerini belirlemek amacıyla hazırlanmıştır.

2. DÜZENLENEN KAYIT ORTAMLARI

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

Elektronik ortamlar;

- Ms Office Dosyaları
- Sunucularımız
- Antivirüs programları ve güvenlik duvarı ile hassas bir şekilde korunan bilgisayarlarımız
- Ağ cihazlarımız
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
- Mobil telefonlar ve içerisindeki tüm saklama alanları,
- Yazıcı,
- Flash hafızalar
- Veritabanı

Fiziki ortamlar;

- Birim Dolapları
- Birim Arşivi
- Kurum Arşivi
- Arşiv
- Muhasebe Birimi

3. TANIMLAR VE AÇIKLAMALAR

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	AQUA medikal çalışanları.

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 ortamı,
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Veri Sahibi/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, Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Özel Nitelikli Kişisel Veri	Irk, 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 işlenme 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	Aqua Medikal Kişisel Veri Saklama ve İmha Politikası
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Tedarikçi	Veri Sahibi'nin ticari faaliyetlerini yürütürken bizzat veya hissedar veya yöneticileri aracılığı ile sermayesine iştirak ettiği veya yönetiminde olduğu şirketleri adına her türlü hizmet almak ve

	operasyonel süreci yürütmek amaçlarıyla iş ortaklığı kurduğu tarafları tanımlar
Hukuken Yetkili Kamu Kurum ve Kuruluşlar	İlgili mevzuat hükümlerine göre şirketten bilgi ve belge almaya yetkili kamu kurum ve kuruluşları
Şirket	Aqua Medikal Tıbbi Araç ve Gereçler İnşaat Sanayi Dış Ticaret Limited Şirketi
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 Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

4. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Şirket bünyesinde bulunan kişisel veriler, Şirketimizin hizmetlerinin sunulması, ticari faaliyetlerinin kesintisiz olarak sürdürülmesi, hukuki yükümlülüklerinin yerine getirilmesi, müşteri ilişkilerinin yürütülmesi, çalışan haklarının planlanması ve yerine getirilmesi amacıyla; aşağıda yer alan veri işleme sebepleriyle İşbu Politika'da belirtilen elektronik ya da fiziki ortamlarda güvenli ve hassas bir şekilde saklanmakta ve yine bu sebeplerin ortadan kalkması halinde resen veya ilgili kişinin talebi üzerine imha edilmektedir.

- 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,
- 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.

5. ÖZEL NİTELİKLİ KİŞİSEL VERİNİN KORUNMASI

Şirketimiz, hukuka aykırı olarak işlendiklerinde ayrımcılık yaratma riski taşıyan özel nitelikli olarak belirtilen kişisel verileri işlemez ancak veri sahibinin açık rızası veya kanunun gerekli kıldığı hallerde özel nitelikli kişisel verilerin işlenmesi durumunda KVK Kanunu'nun 6. maddesinde ortaya konulan veri işleme şartlarına göre önlem alır.

➢ Özel nitelikli kişisel veri işlenmesi sürecinde yer alan personele eğitim verilir.
➢ İlgili verilere erişimi engelleyen yetki kısıtlaması sağlanır.
➢ Verilerin toplandığı fiziki ve elektronik ortamlar şifreleme tekniği ile korunur.
➢ Bu verilere ilişkin erişim kayıtları, sistem ve çalışan periyodik olarak denetlenir.

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

Şirketimiz, kişisel verilerin güvenli bir şekilde saklanması ile hukuka uygun olarak işlenmesinin sağlanması ve kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi amacıyla aşağıdaki teknik ve idari tedbirleri almaktadır:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- 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, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- 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.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- 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.
- 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.
- KVKK 9. madde kapsamında; Kişisel veriler ve TTK gereğince aleniyet ilkesi gereği ticaret sicilinde yer alan gerçek/özel hukuk tüzel kişilerine ait bilgiler bulut(cloud) teknolojisi kullanılan uluslar arası uygulamaların (Whatsapp, Google veri tabanlı uygulamalar, Yandex veri tabanlı uygulamalar, Amazon veri tabanlı uygulamalar, Microsoft veri tabanlı uygulamalar) ticari hayatta etkin olarak kullanılması sebebiyle - Kurum tarafından güvenli ülke listesi yayımlanana ve yeniden değerlendirilme süreci başlayana dek- açık rıza alınmaktadır.
- Yeterli koruma listesinin yayınlanmasını takip eden 3 iş günü içerisinde uyum süreci yürütülerek açık rıza ve işin niteliği gereği rıza olmaksızın yürütülecek işlerin tasnifi gerçekleştirilecektir.
- Gerekli görülmesi halinde Bağlayıcı Şirket Kuralları Başvuru sürecine geçilerek şirketler arası eşgüdüm ve etkin çalışmada açık rızanın varlığının aranmadığı prosedüre geçilebilir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler 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.

7. 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:

KİŞİSEL VERİLERİN SİLİNMESİ

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.
- Kağıt ortamında bulunan kişisel veriler; karartma yöntemi (çizilerek/boyanarak/silinerek) kullanılarak silinmektedir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılmaktadır.

- 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.

KİŞİSEL VERİLERİN YOK EDİLMESİ

- 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, Optik diskler olarak belirtebileceğimiz çevresel kayıt sistemleri dijital ortam ise ürün özelliği olarak destekleniyorsa 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.
- Kağıt ve mikro ofis 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.

KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

- Maskeleme 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 bağdaştırılamayacak şekilde (örn: doğum tarihleri yerine yaş yazılması) anonim hale getirme gerçekleştirilmektedir.

(Aşağıda, uygulamada kullanılan anonimleştirme yöntemlerine ilişkin tanımlar ve açıklamalar bulunmaktadır. Şirket bünyesinde bu yöntemlerden bir veya birkaçının kullanılması durumunda ilgili yöntemlerin seçilmesi/belirtilmesi gerekmektedir)

A) DEĞER DÜZENSİZLİĞİ SAĞLAMAYAN ANONİMLEŞTİRME YÖNTEMLERİ

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 imkansız 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 DÜZENSİZLİĞİ SAĞLAYAN ANONİMLEŞTİRME YÖNTEMLERİ

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) ANONİMLEŞTİRMEYİ GÜÇLENDİRİCİ İSTATİSTİKSEL 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 türetilebilmesi 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 istatiksel 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 maskeleme 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 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.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALANLARIN UNVANLARI, BIRIMLERI VE GÖREV TANIMLARI

PERSONEL	BİRİM	GÖREV TANIMI
Arşiv Sorumlusu	Arşiv Sorumlusu	Kişisel verilerin imha edilmesi.
Avukat	Hukuk	İlgili kişilerin taleplerinin alınması, usulüne uygunluğunun kontrolü ve talebin cevaplanması.
Muhasebe Personeli	Muhasebe - Finansman	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması.

Muhasebe/Finansman – İdari işler Müdürü	Muhasebe - Finansman	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
Pazarlama – Satın Alma Personeli	Pazarlama Satın Alma	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
Ar–ge Personeli	Ar-Ge	Görevi dahilinde herhangi bir kişisel veri işlenme hususu bulunmamaktadır.
İthalat – İhracat Personeli	İthalat - İhracat	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

9. SAKLAMA VE İMHA SÜRELERİNE İLİŞKİN TABLO

Şirket bünyesinde bulunan kişisel veriler; ilgili kanunlarda ve mevzuatta öngörülmesi durumunda bu mevzuatta belirtilen süre boyunca saklamaktadır.

Kişisel verilerin işlenme amacı sona ermiş, ilgili mevzuat ve şirketin belirlediği saklama süresinin de sonuna gelinmişse, kişisel veriler yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zamanaşımı süreleri esas alınır. Bu durumda kişisel verilere herhangi bir başka amaçla erişim yapılmamaktadır. Kişisel veriler söz konusu süreler sona erdikten sonra imha edilmektedir.

SAKLANAN KİŞİSEL VERİLER	SAKLAMA SÜRESİ	SAKLAMA SÜRESİ
MUHASEBE VE FİNANSAL İŞLEMLERE İLİŞKİN TÜM KAYITLAR (KİMLİK,İLETİŞİM,LOKASYON, ÖZLÜK,)	Sözleşmesel ilişkinin sona erme tarihinden itibaren 10 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
VEKALETNAMELER, İMZA SİRKÜLERİ, GENEL KURUL KARARLARI, AZİLLER GİBİ GENEL ŞİRKET KARARLARINA İLİŞKİN BELGELER	İlk kaydın yapıldığı tarihten itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

ÜÇÜNCÜ KİŞİLERLE İMZALANAN SÖZLEŞMELER (KİRA SÖZLEŞMELERİ, HİZMET SÖZLEŞMELERİ, TEDARİK SÖZLEŞMELERİ)	İlgili sözleşmenin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
İHALE/İŞYERİ AÇMA/BAKANLIKLAR-MÜSTEŞARLIKLAR EVRAK HAZIRLAMA SÜREÇLERİ	Sürecin sona erme tarihten itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
İŞ SAĞLIĞI VE GÜVENLİĞİ UYGULAMALARI KAPSAMINDA ELDE EDİLEN KİŞİSEL VERİLER	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
TEDARİKÇİ İLETİŞİM VE TANITIM FORMLARI	İş İlişkisinin sona erme tarihinden itibaren 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
ÇALIŞANLARA AİT KİŞİSEL SAĞLIK VERİLERİ	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
ÇALIŞANLARIN İŞE ALIM DOSYALARI, ÖZLÜK VERİLERİ	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
İŞ SAĞLIĞI VE GÜVENLİĞİ UYGULAMALARI KAPSAMINDA ELDE EDİLEN KİŞİSEL VERİLER	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
MÜŞTERİ TALEP/ŞİKÂYET BİLGİLERİ	Kaydın alınmasından itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

PERSONEL İLE İLGİLİ MAHKEME/İCRA BİLGİ TALEPLERİNİN CEVAPLANMASI	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
PERSONEL FİNANSMAN SÜREÇLERİ	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
TÜM BİRİMLERCE EDİNİLEN İLETİŞİM BİLGİLERİ	İletişim bilgilerinin edinildiği tarihten itibaren 10 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
5651 SAYILI YASA GEREĞİ İNTERNET KULLANIM LOGLARI TUTULUR	2 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
FİZİKSEL GÜVENLİK AMACIYLA KAMERA KAYITLARININ TUTULMASI	2 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
PERSONEL ADAYI DEĞERLENDİRME	Olumsuz sonuçlanan değerlendirmeler 3 yıl süre ile saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
EĞİTİM FAALİYETLERİ	İş sözleşmesinin sona ermesi ile birlikte İSG mevzuatı kapsamında yer alan kişisel veriler 15 yıl, diğer veriler ise 10 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
İZİNLER	Personelin iş ilişkisinin sona ermesinden itibaren 10 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

İŞ YERİ AÇILIŞ İŞLEMLERİ	İşlenen kişisel verilerin 10 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
FATURA TAHAKKUKU	Türk Ticaret Kanunu'ndan kaynaklanan durumlarda 10 yıl, Vergi Usul Kanunu'ndan kaynaklanan durumlarda ise 5 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
BEYANNAME DÜZENLENMESİ	Vergi Usul Kanunu uyarınca 5 yıl saklanır.	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
SÖZLEŞME SÜRECİNİN BİR BÖLÜMÜ VE SÖZLEŞMENİN MUHAFAZASI	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
LOKASYON BİLGİLERİ	Ticari faaliyetin bitmesinden itibaren 5 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
KVK SÜREÇLERİ (AYDINLATMA, AÇIK RIZA, BAŞVURU VE ŞİKAYETLER)	İlgili kaydın yapıldığı tarihten itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
SİLME YOK ETME ANONİM HALE GETİRME KAYIT SÜRECİ	İşlem tarihinden itibaren 3 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
POSTA- KARGO İŞLEM KAYITLARI	İşlem tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
STAJYER İŞLEMLERİ	Stajın sona ermesinden	Saklama süresinin bitimini takip eden ilk

	itibaren 10 yıl	periyodik imha işleminde imha edilir.
ÇALIŞAN ADAYLARINA İLİŞKİN VERİLER	Başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.
MÜŞTERİLERE İLİŞKİN KİŞİSEL VERİLER	Hukuki/sözleşme ilişkisinin bitmesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde imha edilir.

10. 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 1. ve 7. 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.

11. POLİTİKA'NIN YAYINLANMASI, SAKLANMASI VE YÜRÜRLÜĞE GİRMESİ

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Politika, ihtiyaç duyuldukça gözden geçirilir. İlgili mevzuatta yapılacak her türlü resmi değişiklik ardından bu de değişikliğe uyumlu olacak şekilde iş bu Politika'da değişiklik yapabilir. Kişisel Verileri Koruma Kanunu ile ilgili düzenlemeler ve iş bu Politika arasında bir uyumsuzluk olması halinde KVKK düzenlemeleri esas alınır. Politika, Kurumun internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Şirket Yetkilisi tarafından iptal edilerek imzalanır ve en az 20 yıl süre ile Şirket bünyesinde tarafından saklanır.

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

GÜNCELLEME TARİHİ	GÜNCELLENMEDEN ÖNCE	GÜNCELLENDİKTEN SONRA

13. TUTANAK

Yukarıda belirtilen silme, yok etme ve anonim hale getirme işlemleri; işlemleri gerçekleştiren ilgili Şirket Yetkilisi ve İrtibat kişisinin ortak imzası ile hazırlanan tutanak ile kayıt altına alınır.