ÖZ KÖYÜM ZEYTİNCİLİK
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Ağustos 2021

1. POLİTİKANIN AMACI

Hazırlanan işbu 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'')** başta olmak üzere ilgili mevzuat uyarınca **("Şirket")** saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul, esas, saklama, silme ve imha sürelerini belirlemek amacıyla hazırlanmıştır.

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

2. TANIMLAR VE AÇIKLAMALAR

Öz Köyüm Zeytincilik tarafından hazırlanan ve kamuoyu ile paylaşılan Kişisel Verileri Koruma Politikamızda KVKK alanına dair temel kavram tanımları ve açıklamalara ulaşabilirsiniz.

3. SORUMLULUK

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

4. DÜZENLENEN KAYIT ORTAMLARI

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

Elektronik ortamlar:	**Elektronik olmayan ortamlar:**
• Kişisel bilgisayarlar (masaüstü, dizüstü) • Şirket bilgisayarları (masaüstü, dizüstü) • Ağ cihazları • Mobil cihazlar ve içerisindeki saklama alanları (telefon, tablet vb.) • Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri • Sunucular (e-posta, veri tabanı, web, dosya paylaşım, etki alanı, yedekleme,) • Yazılımlar (ofis yazılımları, portal, vb.) • MS office dosyaları • Bulut sistemleri • Yazıcı • Fotoğraf makinesi • Kamera • Tarayıcı • Fotokopi makinesi • Optik diskler (CD, DVD, vb.) • Çıkartılabilir diskler (USB, hafıza kartı, vb.)	• Arşiv • Birim dolapları • Birim arşivi • Muhasebe birimi • Yazılı, basılı, görsel materyal ve ortamlar • Manuel veri kayıt sistemleri (anket formları, ziyaretçi defteri, aday değerlendirme formları)

5. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLERE İLİŞKİN AÇIKLAMALAR

Şirket bünyesinde bulunan kişisel 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, 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 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,
- 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.

6. SAKLAMANIN HUKUKİ SEBEPLERİ

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 6502 Tüketicinin Korunması Hakkında Kanun,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- Bu kanunlar uyarınca ve bunlarla sınırlı olmamak üzere yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama amaçları ve saklama süreleri kadar saklanmaktadır

7. 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.
- Gerektiğinde veri maskeleme 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.

- Kağıt 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.
- 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.
- 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/veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- 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.

8. 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:

NOT: Şimdiye kadar Öz Köyüm Zeytincilik bünyesinde hiçbir bulut sistemi kullanılmamıştır. Ancak ileride kullanılma ihtimaline karşın saklama, silme ve imha politikalarında bulut sistemlerine de yer verilecektir.

Kişisel Verilerin Silinmesi

- Kâğıt 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 saklanmakta ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.
- Bulut sisteminde bulunan veriler silme komutu verilerek 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 gibi yöntemlerle 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.

Kişisel Verilerin Anonim Hale Getirilmesi

- 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.

Öz Köyüm Zeytincilik bünyesinde yapılabilecek belirli anonimleştirme yöntemlerini ayrıca açıklamakta fayda görmekteyiz:

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

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 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.

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

Personel	Birim	Görev tanımı
Arşiv Sorumlusu	Genel Müdürlük	Kişisel verilerin imha edilmesi.
Hukukçu/Avukat	Genel Müdürlük	İlgili kişilerin taleplerinin alınması, usulüne uygunluğunun kontrolü ve talebin cevaplanması.
Yazılımcı	E-Satış Departmanı/Bilgi İşlem	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.
İnsan Kaynakları Personeli	İnsan Kaynakları	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

*Öz Köyüm Zeytincilik, bünyesinde bulunan personel ve yöneticilere bağlı olarak bu tablodaki tanımlanan görevleri farklı personel ve birimlere de yaptırabilir.

10. SAKLAMA VE İMHA SÜRECİ VE SÜRELERE İLİŞKİN TABLO

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

Kişisel verilerin işlenme amacı sona ermiş, ilgili mevzuat ve şirketin belirlediği saklama süresinin de sonuna gelinmişse, kişisel veriler olası hukuki uyuşmazlıkların 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 işbu Politika'da 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 uyuşmazlıkların 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.

ÖRNEK SAKLAMA VE İMHA SÜRECİ

ÖRNEK:

Süreç (Faaliyet): Personel özlük dosyalarının tutulması

Silme zamanı: Sözleşmenin sona ermesinden itibaren 5 yıl

Yok etme zamanı: Silme zamanının tamamlanmasından itibaren 15. 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.

Süreç (Faaliyet)	Faaliyetin Yasal Dayanağı	Silme Zamanı	Saklamanın Yasal Dayanağı	Yok Etme Zamanı
Üyelik ve siparişe ilişkin kayıtlar	E-Ticaret Mevzuatı & 6098 sayılı TBK	Kullanıcı tarafından üyelik hesabının silinmesinden itibaren **20 yıl**.	E-Ticaret Mevzuatı & 6098 sayılı TBK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Üye Müşterilere ilişkin kişisel veriler	E-Ticaret Mevzuatı & 6098 sayılı TBK	Kullanıcı tarafından üyelik hesabının silinmesinden itibaren **20 yıl**.	E-Ticaret Mevzuatı & 6098 sayılı TBK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Çevrimiçi ziyaretlere ilişkin internet trafik bilgileri	5651 sayılı Kanun	Ziyaret tarihinden itibaren **20 yıl.**	5651 sayılı Kanun	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Çalışan adayı değerlendirmesi/ Mülakat	Genel hukuk kuralları	Aday işe alınırsa özlük dosyasına aktarılır. Aday işe alınmazsa başvuru tarihinden itibaren **10 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,	İK TBK	Sözleşmenin sona ermesinden itibaren **20 yıllık** sürenin sonunda silinir.	İK TBK KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.

sınavlar, fotoğraf, çalışma belgesi, sosyal yardım ve sosyal izinler, kesintiler, ödemeler, kayıtlar, seyahatler, sigorta bilgileri, plaka, araç vb.)				
Özgeçmiş bilgisi (çalışan)	**3 yıllık** süreler ile güncelliği sorgulanır, güncelliğinin yitirilmesiyle yenilenir veya yok edilir.			
Adli sicil kayıtları	5352 sayılı Adli Sicil Kanunu'ndaki sürelere 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 **20 yıllık** sürenin sonunda silinir.	İK TBK İSG KVKK	Silme tarihinden itibaren 5yıllık süreyi takip eden ilk periyodik imha işleminde 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 **20 yıllık** sürenin sonunda silinir.	İK KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Muhasebe ve finansal işlemlere dair tüm kayıtlar.	TBK, KVKK	İşlemlerin bitiminden ve hukuki ilişkinin sona ermesinden itibaren **20 yıllık** sürenin sonunda silinir.	TBK, KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
İşe giriş sağlık muayeneleri ve periyodik-poliklinik sağlık muayeneleri, istirahat raporları (çok	İSG İK TBK	Sözleşmenin sona ermesinden itibaren **20 yıllık** sürenin sonunda silinir.	İSG İK TBK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha

tehlikeli işler grubu harici)			KVKK	işleminde yok edilir.
İş kazası tutanağı, acil durum kayıt formu, iş kazası muayenesi ve olay kayıtları, sonuç bildirimi (çok tehlikeli işler grubu)	İSG	Kazaya karışan kişi ile sözleşme varsa: Sözleşmenin sona ermesinden itibaren **20 yıllık** sürenin sonunda silinir. Kazaya karışan kişi ile sözleşme yoksa: Kaza tarihinden itibaren **20 yıllık** sürenin sonunda silinir.	İSG KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Tedarikçilere dair kişisel veriler/kayıtlar	6098 s. TBK	Hukuki ilişki (sözleşmesel ilişki) sona erdikten sonra **20 yıllık** sürenin sonunda silinir.	6098 s. TBK & KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Aydınlatılmış Onam Formu	İK İSG TBK	Kişi ile sözleşme varsa: Sözleşmenin sona ermesinden itibaren **20 yıllık** sürenin sonunda silinir. Kişi ile sözleşme yoksa: Onam tarihinden itibaren **20 yıllık** sürenin sonunda silinir.	İK İSG TBK	Silme tarihinden itibaren 5 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 **20 yıllık** sürenin sonunda silinir.	AVK HMK İİK KVKK	Silme tarihinden itibaren 5 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.
Portal/E-Ticaret otomasyonu	-	-	KVKK	Portalde yayınlanan içeriğin güncelliğini yitirmesi ile yok edilir.
Sürece yayılı olmayan hizmet – mal – ürün alımları	TBK TTK	Alım tarihinden itibaren **3 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 **10 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.
Gelen – giden kargo teslim alan ve teslim eden	-	Sürecin bitiminden itibaren **10 yıllık** sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 5 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 **36 aylık** sürenin sonunda silinir.	TBK KVKK	Silme tarihinden itibaren 1 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Kamera kayıtları	-	15'er günlük süreyle üzerine yazılır	KVKK İK TBK	15'er günlük süreyle üzerine yazılır

Log kayıtları	KVKK İK TBK	Kaydın alınmasından itibaren **20 yıllık** sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde 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.
Telefon ses kaydı	-	Kaydın alınmasından itibaren **1 yıllık** sürenin sonunda silinir.	KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Faturalar (Sürece yayılı işlemler)	VUK TTK	Sürecin sonlanmasını takip eden 5 **yıllık** sürenin sonunda silinir.	VUK TTK	Silme tarihinden itibaren 5 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 5 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 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
GSM giderleri/ Araç giderleri	-	İşlemin gerçekleştiği yılı takip eden **10 yılın** sonunda silinir.	TBK KVKK	Silme tarihinden itibaren 9 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Talep, şikayet ve memnuniyet süreci (sözleşmeden kaynaklanan)	TBK	Talebin veya şikâyetin çözüme kavuşturulmasıyla silinir.	KVKK	Silme tarihinden itibaren 5 yıllık süreyi takip eden ilk periyodik imha işleminde yok edilir.
Talep, şikayet 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.
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.
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 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	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.

11. PERİYODİK İMHA SÜRELERİ

Periyodik imhanın gerçekleşeceği işlem zaman aralıkları Şirket yetkililerince belirlenecektir. Ancak iki periyodik imha işleminin aralığı prensip olarak en fazla 6 ay olacaktır.

Kişisel verilerin imha edilmesine ilişkin yükümlülüğün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinecek, yok edilecek veya anonim hale getirilecektir.

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.

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 birim müdürü, şefi ve personelinin üçlü imzası ile hazırlanan tutanak ile kayıt altına alınır.

MUHAFAZASINA GEREK BULUNMAYAN KİŞİSEL VERİLERİN İMHASINA İLİŞKİN TUTANAK

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