

BELBİM ELEKTRONİK PARA VE ÖDEME HİZMETLERİ A.Ş.
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;

- Sunucularımız,
- Antivirüs programları ve güvenlik duvarı ile hassas bir şekilde korunan bilgisayarlarımız,
- Ağ cihazlarımız,
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri,
- Exchange Server ve E-Postalar,
- Mobil telefonlar ve içerisindeki tüm saklama alanları,
- Yazıcı, Parmak izi okuyucu gibi çevre birimler,
- Manyetik bantlar,
- Optik diskler,
- Flash hafızalar,
- MsSQL, MySQL ve Oracle Veri Tabanları
- Active Directory,
- Kurumsal uygulamalar (PARE, Jira, Siebel vb.).

Fiziki ortamlar;

İnsan Kaynakları Şefliği tarafından tutulan kayıtlar, fiziki ortamda ofislerde yer alan dolaplarda muhafaza edilmektedir. Bu dolaplar halihazırda kilitli dolaplar değildir ancak kayıtların kilitli dolaplarda muhafazası için gereken aksiyonların alınması planlanmaktadır.

Sözleşmeler Şefliği tarafından tutulan kayıtlar, fiziki ortamda sadece birim personelinin erişebileceği kilitli dolaplarda saklanmaktadır.

İdari İşler Şefliği tarafından tutulan kayıtlar, fiziki ortamda sadece birim personelinin erişebileceği kilitli dolaplarda saklanmaktadır.

Satın Alma Şefliği tarafından tutulan kayıtlar, fiziki ortamda kilitsiz dolaplarda ancak klasörlenmiş vaziyette saklanmaktadır. Kayıtların kilitli dolaplarda muhafazası için gereken aksiyonların alınması planlanmaktadır.

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	Belbim A.Ş. 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	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	Belbim A.Ş. Kişisel Veri Saklama ve İmha Politikası
Silme	Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.
Şirket	Belbim A.Ş.
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

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 gibi Şirketimizin Kişisel Verilerin İşlenmesi ve Korunması Politikası'nda daha detaylı şekilde belirtilen amaçlarla; aşağıda yer alan hukuki sebepler kapsamında İşbu Politika'da belirtilen elektronik ya da fiziki ortamlarda güvenli ve hassas bir şekilde saklanmakta ve yasal saklama süresinin sona ermesi ya da veri işleme amacının ortadan kalkması halinde resen veya İlgili Kişi'nin talebi üzerine imha edilmektedir.

- Açık rızanın varlığı,
- Veri işleme faaliyetinin kanunlarda açıkça öngörülmesi,

- Fiili imkânsızlık nedeniyle açık rızanın alınamaması veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri Sorumlusu'nun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması,
- Kişisel Veriler'in İlgili Kişi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşuluyla, Veri Sorumlusu'nun meşru menfaatleri için veri işlemenin zorunlu olması.

5. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ VE ALINMASI PLANLANAN 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.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Anahtar yönetimi uygulanmaktadır.
- 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 logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- 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 gerekli güvenlik tedbirleri alınmaktadır .
- 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 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.
- Bilgi sistemlerine yönelik mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

Şirketimiz tarafından ilerleyen süreçte alınması planlanan tedbirler ise aşağıda belirtilmektedir:

- Gerektiğinde veri maskeleyme uygulanması;
- Kişisel verilerin mümkün olduğunca azaltılması;
- Özel nitelikli kişisel verilerin Taşınabilir Bellek, CD, DVD ortamında aktarılmasının yasaklanması;
- Özel nitelikli kişisel verilerin Şirket içinde e-posta yoluyla aktarımında, şifreleme yönteminin kullanılması;
- Veri işleyen hizmet sağlayıcıların veri güvenliği konusunda belirli aralıklarla denetimi;
- Veri kaybı önleme yazılımı kullanılması (halihazırda kullanılan yazılım veri kaybı ile ilgili bilgilendirmede bulunsa da, önleme işlevi mevcut değildir).

6. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINACAK TEKNİK VE İDARİ TEDBİRLER

Kişisel verileri imha etmeye (*silmeye, yok etmeye ve anonim hale getirmeye*) yönelik Şirket bünyesinde ilerleyen süreçte gereken aksiyonlar alınacaktır. İmha sürecinde aşağıdaki hususlara uygun hareket edilecektir:

Kişisel Verilerin Silinmesi

- Bulut sisteminde bulunan veriler silme komutu verilerek silinmektedir.

- 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 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.

Kişisel Verilerin Anonim Hale Getirilmesi

- Maskeleyme yöntemi ile veri sahibinin tanımlanmasını sağlayan temel belirleyici bilgiler (Ör: isim, soy isim, TCKN) çıkartılarak anonimleştirme gerçekleştirilmektedir.
- Toplulaştırma yöntemi ile kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek bir şekilde (Ör: 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 (Ör: 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 teklik 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 kümeyle 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 maskeleyme 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.

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

PERSONEL	BİRİM	GÖREV TANIMI
Arşiv Sorumlusu	Arşiv	Kişisel verilerin imha edilmesi.
Avukat	Hukuk	İlgili kişilerin taleplerinin alınması, usulüne uygunluğunun kontrolü ve talebin cevaplanması.

Bilgi İşlem Personeli	Bilgi İşlem/Bilgi Teknolojileri	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, ilgili kişilerin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması.
İdari İşler Personeli	İdari İşler Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.
İnsan Kaynakları Personeli	İnsan Kaynakları Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetiminin yapılması.

8. 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 işleme amacı sona ermiş, ilgili mevzuat ve şirketin belirlediği saklama süresinin de sonuna gelinmişse, kişisel veriler yalnızca olası hukuki uyumsuzluklarda 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.

Veri Kategorisi ve İlgili Kişi Grupları	Saklama Süresi	İmha Süresi
Çalışanlara ait özlük bilgileri	İstihdam ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Çalışanlara ait HES kodları	İstihdam ilişkisi süresince	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Özel sağlık sigortası süreçleri kapsamında çalışanlardan temin edilen veriler	İstihdam ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
İş sağlığı ve güvenliği kapsamında temin edilen sağlık verileri	İstihdam ilişkisinin sona ermesinden itibaren 15 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde

İş sağlığı ve güvenliği kapsamında temin edilen diğer veriler	İstihdam ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Çalışanlardan temin edilen diğer veriler	İstihdam ilişkisinin sona ermesinden itibaren azami 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Çalışan adaylarından temin edilen veriler	Verilerin elde edilmesinden itibaren 1 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Kart kullanıcılarından temin edilen veriler	Kartın aktif olduğu süre boyunca ve en fazla kartın inaktif hale gelmesinden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Üye işyerlerinden temin edilen veriler	Üye işyeri ile olan sözleşmesel ilişkinin bitiminden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Tedarikçi, iş ortağı ve temsilcilerden temin edilen veriler	Ticari ilişkinin bitiminden itibaren 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Türk Ticaret Kanunu ve Vergi Usul Kanunu uyarınca tutulan defterler/kayıtlarda yer alan veriler	Verilerin ilişkili olduğu yıldan itibaren azami 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Hukuki süreçlerde kullanılan veriler	Hukuki sürecin kesinleşmesinden itibaren en fazla 10 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
Çağrı merkezi kayıtları	Verilerin elde edilmesinden itibaren 3 yıl	Saklama süresinin sona ermesini takiben 6 ay içerisinde
İşyerindeki kamera kayıtları	Verilerin elde edilmesinden itibaren en fazla 3 ay	Saklama süresinin sona ermesini takiben 6 ay içerisinde

9. 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.

10. 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.

Kamuoyuna saygılarımızla arz olunur.