

1. AMAÇ VE KAPSAM

Bu politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu kanuna dayalı olarak çıkarılan “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” kapsamında kişisel verilerin saklanması ve imhasına ilişkin Şirket yükümlülüklerinin yerine getirilmesini sağlamak amacıyla oluşturulmuştur. Bu politika, işbu yönetmeliklere uygun olarak, kişisel verilerin korunması, işlenmesi ve imhasıyla ilgili ulusal olarak kabul görmüş temel ilkelere dayanmaktadır.

Bu politika, Halköde tarafından saklanan ve Kanun kapsamında tanımlanan kişisel verileri ve özel nitelikli kişisel verileri kapsamaktadır. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Halköde tarafından belirlenen bu politika doğrultusunda gerçekleştirilir. Halköde, kişisel verilerin saklanması, erişimi, kullanımı ve imhasıyla ilgili prosedürleri bu politikaya uygun olarak oluşturur ve uygular.

2. TANIMLAR

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini temsil eder.

Ödeme Hizmeti Faaliyetleri: 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun’da belirtilen ödeme hizmeti şirketinin gerçekleştirebileceği faaliyetleri ifade eder.

E-YKS: Elektronik Yönetim Kurulu Sistemini ifade eder.

Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları temsil eder.

Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamları ifade eder.

Hizmet Sağlayıcı/Tedarikçi: Belirli bir sözleşme çerçevesinde mal ve/veya hizmet sağlayan gerçek veya tüzel kişiyi temsil eder.

İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi ifade eder.

İlgili Kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere, veri sorumlusu organizasyonu içerisinde kişisel verileri işleyen çalışanı temsil eder.

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini ifade eder.

İrtibat Kişisi: Türkiye’de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye’de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla Sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.

İşlem Sahibi: Şirket’in gerçekleştirdiği faaliyetleri çerçevesinde sunduğu ürün ve/veya hizmetlerden gerek kendi nam ve hesabına gerekse de başkası nam ve hesabına yararlanan gerçek kişiyi temsil eder.

Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanununu ifade eder.

Kayıt Ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı ifade eder.

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi temsil eder.

Kişisel Veri İşleme Envanteri: Şirketimizin iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verilerin elde edilme kanallarını, kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan

tedbirleri açıklayarak detaylandığı envanteri temsil eder.

Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.

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 işlemi ifade eder.

Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi temsil eder.

Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi ifade eder.

Kurul: Kişisel Verileri Koruma Kurulunu ifade eder.

Kurum: Kişisel Verileri Koruma Kurumunu temsil eder.

Maskleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması vb. işlemleri ifade eder.

Özel Nitelikli Kişisel Veri: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri temsil eder.

Periyodik İmha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi ifade eder.

Politika: Kişisel Verileri Saklama ve İmha Politikasını temsil eder.

Platform/Şirket: Halköde Ödeme Hizmetleri ve Elektronik Para A.Ş.'yi ifade eder.

Veri İşleyen: Veri Sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini temsil eder.

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemini ifade eder.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan tüzel kişi olarak: Halk Elektronik Para ve Ödeme Hizmetleri Anonim Şirketi'ni ifade eder.

Yönetmelik: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği temsil eder.

3. SORUMLULUK VE GÖREV DAĞILIMLARI

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo-1'de belirtilmiştir.

BİRİM/KOMİTE	GÖREV
Yönetim Kurulu	<ul style="list-style-type: none">İşbu Yönetmelik kapsamında imha ve saklama yöntemlerinin belirlenmesinden ve periyodik imha süreçlerine karar verilmesinden sorumludur.
KVKK Uyum Ekibi	<ul style="list-style-type: none">KVKK'ya uygun politikaların oluşturularak, Politikanın hazırlanması, geliştirilmesi, yürütülmesi hususunda ilgili birimler ile koordinasyonun sağlanmasından,Politikada yer alan teknik tedbirlerin belirlenmesinden sorumludur.
Bilgi Teknolojileri Genel Müdür Yardımcılığı	<ul style="list-style-type: none">Şirket verilerinin saklanması ve imhası için teknik tedbirlerin alınmasından,Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

İç Kontrol ve Denetim Bölüm Müdürlüğü	<ul style="list-style-type: none">Saklama ve imha süreçlerine ilişkin tesis edilen kontrollerin iç ve dış mevzuata uyumluluğunun gözden geçirilmesinden sorumludur.
İlgili Bölüm Müdürlükleri	<ul style="list-style-type: none">Kendi iş süreçleri ile ilgili olmak üzere; KVKK'ya uyum sağlamak amacıyla kişisel verilerin işlenmesi, saklanması ve imhasına ilişkin gerekli tedbirlerin alınmasından sorumludur.

4. KAYIT ORTAMLARI

Kişisel veriler, Halköde tarafından Tablo-2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo-2: Kişisel Veri Saklama Ortamları Tablosu

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none">Sunucular (web sunucusu, veri tabanı, dosya paylaşım, etki alanı, yedekleme, e-posta, vb.)Yazılımlar (Ödeme hizmet yazılımları, yardımcı kurum içi süreç yönetim yazılımları, ofis yazılımları, portal, E-YKS)Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)Kişisel bilgisayarlar (masaüstü, dizüstü)Mobil cihazlar (telefon, tablet vb.)Optik diskler (CD, DVD vb.)Çıkarılabilir bellekler (USB, hafıza kartı vb., teyp kartuşları)Yazıcı, tarayıcı, fotokopi makinesi	<ul style="list-style-type: none">KâğıtManuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)Diğer yazılı, basılı ve görsel ortamlar, genel müdürlük veya saklama amacıyla özel hazırlanmış merkezlerdeki kilitli depo, oda, kasa, dolap veya masa çekmeceleri

5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

5.1. Saklamaya İlişkin Açıklamalar

Bilgi sistemleri sürekliliği yönetimi, sürekli olarak yaşayan ve gelişen bir süreç olduğundan, planın işlevsel ve güncel kalması için denetim, gözden geçirme ve güncelleme süreçleriyle sürdürülür.

5.1.1. Saklamayı Gerektiren Hukuki Sebepler

6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, 4208 sayılı Karaparanın Aklanmasının Önlenmesine Dair Kanun, 6362 sayılı Sermaye Piyasası Kanunu, 6098 sayılı Türk Borçlar Kanunu, 6102 sayılı Türk Ticaret Kanunu ve diğer yasa, yönetmelik, tebliğ,

uluslararası anlaşmalar vesair yasal mevzuat hükümleri doğrultusunda ve Şirket Faaliyetleri çerçevesinde her türlü ürün ve hizmetlerde kullanmak, diğer ilgili kanun, yönetmelik, tebliğ, uluslararası anlaşmalar ve sair yasal mevzuat hükümleri ve ilgili mevzuatın öngördüğü kişisel bilgilerin işlenmesi, saklanması, raporlanması ve diğer yükümlülüklerle uymak amacıyla işlenmekte ve saklanmaktadır.

5.1.2. Saklamayı Gerektiren İşleme Amaçları

- Halköde müşterilerine ilişkin kişisel veriler ve özel nitelikli kişisel veriler aşağıdaki amaçlarla işlenmektedir:
- Ödeme Hizmetleri faaliyetlerinin gerçekleştirilmesi ve müşterilere sunulan her türlü ürün ve hizmetlerin kullanılması,
- Ödeme hizmetlerinin mevzuata uygun olarak yürütülmesi ve denetlenmesi,
- Şirketin mülkiyete dayalı haklarının ve güvenliğinin sağlanması,
- Hukuki yükümlülüklerin yerine getirilmesi, özellikle resmi kurumlarca öngörülen raporlama ve bilgilendirme yükümlülüklerinin yerine getirilmesi,
- Hukuki uyuşmazlıklarda delil olarak kullanılabilmesi için gerekli bilgilerin saklanması ve kullanılması,
- İnsan kaynakları süreçlerinin yürütülmesi ve kurumsal iletişimin sağlanması,
- İlgili kişilerin şikayet, soru ve taleplerinin karşılanması,
- İşlem sahibinin kimlik bilgilerinin tespit ve teyit edilmesi amacıyla gerekli kayıt ve belgelerin düzenlenmesi,
- Resmi kurumlar ve diğer kuruluşlar tarafından öngörülen yükümlülüklerle uyulması.

Müşteri dışındaki üçüncü kişilere ilişkin kişisel veriler ve özel nitelikli kişisel veriler,

- Şirket faaliyetlerinden kaynaklı olarak Şirketin yasal haklarını ve meşru menfaatlerini korumak amacıyla işlenmektedir.

Çalışana ilişkin kişisel veriler ve özel nitelikli kişisel veriler,

- İş ilişkisinin yönetimi, ücret ve ücret bilgilerinin kaydedilmesi, yasal bildirimlerin yapılması, iş sağlığı ve güvenliği önlemlerinin uygulanması ve yasal yükümlülüklerin yerine getirilmesi amacıyla işlenmektedir.

Destek hizmetleri firmaları ve ürün/hizmet satın alınan firmalarla akdedilen sözleşmeler kapsamında temin edilen kişisel veriler ve özel nitelikli kişisel veriler,

- Sözleşmelerin ifası ve yükümlülüklerin yerine getirilmesi amacıyla işlenmektedir.

Ayrıca, ilgili mevzuatta öngörülen diğer amaçları gerçekleştirmek maksadıyla da kişisel veriler işlenmektedir.

5.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası, işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- İlgili kişinin kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirketimiz tarafından kabul edilmesi,
- Kurul tarafından verilen kararın uygulanması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması

durumlarında imha edilir.

6. TEKNİK VE İDARİ TEDBİRLER

6.1. Teknik Tedbirler

Kişisel verilerin ve özel nitelikli kişisel verilerin güvenli bir şekilde saklanması, bu verilere güvenli bir şekilde erişilmesi ve yetkisiz erişimlerin önlenmesi hususlarında gerekli düzenlemeler yapılmaktadır. Özel nitelikli kişisel verilerin işlenmesi için ayrıca Kurulun verdiği kararlar çerçevesinde yeterli önlemler alınmaktadır.

Şirketimiz tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda yer 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.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleyme önlemi uygulanmaktadır.

- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup, bunların takibi de yapılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Sızma testi uygulanmaktadır.
- Şifreleme yapılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- 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.
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- Çalışanlar için yetki erişim matrisi oluşturulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

6.2. İdari Tedbirler

Şirketimiz, işlediği kişisel verilerin güvenliğini sağlamak amacıyla bir dizi idari tedbir almaktadır. Bu tedbirler, bilgi güvenliği standartlarına uygun olarak belirlenmiş ve sürekli olarak gözden geçirilmektedir. Aşağıda, alınan idari tedbirlerin detayları yer almaktadır:

- Kişisel veri güvenliğinin sürekli olarak takibi yapılmaktadır. Mevcut riskler ve tehditler belirlenerek uygun önlemler alınmaktadır.

- Özel nitelikli kişisel verilerin elektronik posta yoluyla gönderilmesi durumunda mutlaka şifreleme yöntemleri kullanılarak ve KEP veya kurumsal posta hesapları aracılığıyla gerçekleştirilmektedir.
- Siber güvenlik önlemleri alınmakta ve bu önlemlerin uygulanması sürekli olarak takip edilmektedir.
- Çalışanlar için veri güvenliği ile ilgili disiplin düzenlemeleri bulunmaktadır. Çalışanlar düzenli olarak eğitilmekte ve farkındalık çalışmalarına katılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar oluşturulmuş ve uygulamaya konmuştur.
- Çalışanlar gizlilik taahhütnameleri imzalamakta ve iş akdine veri güvenliği hükümleri eklenmektedir.
- İmzalanan sözleşmelerde veri güvenliği hükümleri bulunmaktadır.
- Halköde tarafından kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmakta ve gerekli önlemler alınmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler düzenli olarak yapılmakta ve sonuçları değerlendirilmektedir.
- Özel nitelikli kişisel veri güvenliği için protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Veri işleyen hizmet sağlayıcıların düzenli aralıklarla denetimi sağlanmakta ve veri güvenliği farkındalığı artırılmaktadır.
- Kişisel verilerin işlenmesi mümkün olduğunca azaltılmakta ve sadece gerektiğinde kullanılmaktadır.
- Kişisel veri işlemeye başlamadan önce ilgili kişilere gerekli bilgilendirme yapılması ve açık rıza alınması sağlanmaktadır.
- Kişisel veri işleme envanteri oluşturulmuş ve düzenli olarak güncellenmektedir. Bu envanter, şirketin işlediği kişisel verilerin tümünü kapsamaktadır.

7. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta belirlenen saklama sürelerinin sona ermesi veya işlendikleri amaç için gerekli olmamaları durumunda, Halköde tarafından işlenen kişisel veriler re'sen veya ilgili kişinin başvurusu üzerine ilgili mevzuat hükümlerine uygun şekilde imha edilir. Kişisel verilerin imha süreci, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gibi üç farklı yöntemle gerçekleştirilebilir. Kişisel verilerin imha süreçlerinde, kişisel veri işleme envanterinde belirtilen süreç bazlı azami saklama süreleri dikkate alınır ve bu süreçler ilgili mevzuata ve bilgi güvenliği standartlarına uygun olarak yürütülür.

7.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi; sadece sınırlı sayıda erişime sahip yetkililerin erişebileceği bir durum dışında, ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini ifade eder.

Silinecek verilerin belirlenmesi sonrasında, yetki yönetimi uygulamaları kullanılarak veriyi kullanan ilgili kullanıcılar belirlenir. Bu kullanıcıların erişim, geri getirme ve tekrar kullanma yetkileri kapatılır veya tamamen ortadan kaldırılır.

7.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, verilerin hiç kimse tarafından erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesini ifade eder.

Yok etme işlemi, verilerin fiziksel kayıt ortamlarında işlendiği durumlarda, verilerin geri getirilme olasılığını tamamen ortadan kaldıracak şekilde gerçekleştirilir.

7.3. Kişisel Verilerin Anonimleştirilmesi

Kişisel verilerin anonim hale getirilmesi işlemi, verilerin tamamen veya kısmen otomatik yollarla işlendiği durumlarda, bu verilerin başka verilerle eşleştirilse dahi, bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.

Bu işlemde, veri setindeki tüm tanımlayıcı bilgiler çıkartılır veya değiştirilir, böylece veri setinin içerdiği bilgilerin bir gerçek kişiyle ilişkilendirilmesi olanaksız hale gelir. Bu şekilde, veri seti içerisindeki bilgilerin kişisel verilerle ilişkilendirilmesi engellenir

ve gizlilik korunmuş olur.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel veriler, mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami saklama süresi boyunca saklanır. Bu süreler belirlenirken şu unsurlar dikkate alınır:

- Hukuki yükümlülük çerçevesinde saklanması gereken süre,
- Kişisel verinin işlenmesini gerektiren hukuki ilişkinin devam edeceği süre,
- Hukuka ve dürüstlük kurallarına uygun olarak meşru menfaatin gözetileceği süre,
- Saklamanın oluşturacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- Verinin doğru ve güncel tutulmasına elverişli olan süre,
- Kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,
- Hukuki bir ihtilafın mevcut olup olmadığı,
- Sektör genel teamülleri.

Tablo-3: Kişisel Verileri Saklama ve İmha Süreleri Tablosu

İLGİLİ KİŞİ	AÇIKLAMA	SAKLAMA SÜRESİ (*)	İMHA SÜRESİ
Halköde işlemlerinin doğrudan ya da dolaylı tarafları	Kişisel veri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Halköde işlemlerinin doğrudan ya da dolaylı tarafları	Özel nitelikli kişisel veri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Destek Hizmeti Sunucusu/Tedarikçi	Kişisel veri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Diğer 3. Kişiler	Kişisel veri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

*Süreler son işlem tarihinden/işlenme şartlarının tamamının ortadan kalkmasından itibaren başlamaktadır.

Yönetmeliğin 11 inci maddesi gereğince Halköde, periyodik imha süresini altı aylık

periyodik dönemler olarak belirlemiştir.

Kişisel verilerin ve özel nitelikli kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

9. YÜRÜRLÜK

Bu Politika, 26.08.2024 tarihli Yönetim Kurulu Kararı ile kabul edilmiştir. Kabul edildiği tarih itibariyle yürürlüğe girmiştir.