PEKCAN HAVUZ ARITMA EKIPMANLARI İNŞ. TUR. VE GIDA SAN. TIC. LTD. ŞTI.

KİŞİSEL VERİ SAKLAMA-AKTARMA- SİLME VE İMHA POLİTİKASI

2026

PEKCAN HAVUZ ARITMA EKIPMANLARI İNŞ. TUR. VE GIDA SAN. TIC. LTD. ŞTI.
KİŞİSEL VERİ SAKLAMA, SİLME, İMHA VE AKTARMA POLİTİKASI

Güncelleme Tarihi: 09/03/2026

1. AMAÇ

Kişisel Verileri Saklama, Silme, İmha ve Aktarma Politikası ("Politika"), **PEKCAN HAVUZ ARITMA EKIPMANLARI İNŞ. TUR. VE GIDA SAN. TIC. LTD. ŞTI.** (**PEKCAN HAVUZ** veya **"Şirket"**) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, **Şirket** tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.
Kişisel Verileri Saklama ve İmha Politikası, Gizlilik Politikasında tanımlanan politika hiyerarşisinin bir parçasıdır ve Gizlilik Politikası ile uyumlu olmak zorundadır. Bu politikada yapılacak değişikliklerle ilgili gerektiğinde Gizlilik Politikasında da düzeltmeler yapılır.

2. KAPSAM

Bu Politika **Şirket** Gizlilik Politikasında sayılan ve elektronik ya da fiziksel ortamlarda işlenen ve saklanan kişisel verilerin tamamı için geçerlidir. Hangi birim/fonksiyon bünyesinde hangi faaliyetler kapsamında kimlerin verisinin ne kadar süre saklanacağı Tablo'da belirtilmiştir.

3. TANIMLAR

Bu Kişisel Veri Saklama ve İmha Politikasının uygulanmasında:
Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
Kişisel Veri Koruma Görevli: **Şirket** bünyesinde Yönetimin kararı ile oluşturulan ve kişisel verilerin korunması ve işlenmesine ilişkin iç işleyişten sorumlu Kişisel Verileri Koruma **Görevli**,
Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,
Fiziksel Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamları,
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 ortam.
İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,
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 gerçek veya tüzel kişileri,
Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
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 veriler
Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin, başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
Kişisel Verilerin İmha Edilmesi: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kurum: Kişisel Verileri Koruma Kurumu,

Periyodik İmha: Kanunda 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 işlemini,
Politika: Kişisel Veri Saklama, Silme ve İmha Politikasını,
Rehber: Kurumun Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberini

4. GÖREV TANIMI

Kişisel verilerin saklanması ve imha edilmesine ilişkin süreçler, **Şirket** bünyesinde kurulan ve kişisel verilerin hukuka uygun işlenmesini temin etmekle görevli olan **Görevli** tarafından gerçekleştirilir.
Şirket bünyesindeki tüm birimler ve çalışanlar, 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. İş süreçlerinde özel nitelikli veri işlenme durumu ve yoğunluğu başta olmak üzere, işleme faaliyetlerinin büyüklüğü, organizasyon yapısı gibi kriterler göz önünde bulundurularak **Şirket** bünyesinde birden fazla görevlinin yer alacağı bir **Görevli** görevlendirilir.

4.1. Görevli Görevleri

Görevli şu görevlere sahiptir.

1. Kişisel veri işleme süreçlerinin Kanun'a, yönetmelikleri, diğer ikincil mevzuata, **Şirket** gizlilik politikalarına uygunluğunu temin etmek,
2. Veri sahiplerinden gelen talepleri değerlendirmek ve sonuçlandırmak,
3. Kişisel verilerin imhası süreçlerine fiilen katılmak,
4. Kişisel veri güvenliği konusunda **Şirket** olarak ihtiyaç duyulan tedbirleri belirleyip alınmasını sağlamak,
5. **Şirket** olarak mevzuata uyumluluğa ilişkin periyodik denetim yapmak, yaptırmak,
6. Hukuki alanda ve uygulamadaki gelişme ve değişiklikler konusunda çalışanların farkındalığını artırmaya yönelik eğitim planı hazırlayıp öneride bulunmak.

5. KİŞİSEL VERİLERİN KAYDEDİLDİĞİ ORTAMLAR

Şirket, Kanun'a uygun olarak gerçekleştirmekte olduğu veri işleme faaliyetleri kapsamında elde ettiği kişisel verileri, işleme amacının gerektirdiği ölçü ile sınırlı olmak kaydıyla fiziksel ve elektronik ortamlarda muhafaza etmektedir. **Şirket** bu kapsamda, kişisel verileri elektronik sunucular (*Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.*), yazılımlar (*ofis yazılımları, portal*), 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.*), çıkartılabilir bellekler (*USB, Hafıza Kartı vb.*), yazıcı, tarayıcı, fotokopi makinesi gibi elektronik ortamlarda ve dosya, arşiv, manuel veri kayıt sistemleri (*belgeler, klasörler, formlar, anket formları vb.*) gibi yazılı, basılı, görsel ortamlarda saklanmaktadır.

6. KİŞİSEL VERİLERİN SAKLANMASINI GEREKTİREN YASAL GEREKÇELER

Şirket yürüttüğü faaliyetler kapsamında işlediği kişisel veriler Tablo'da belirtilen yasal gerekçelere dayalı olarak yürütülen faaliyetler kapsamında, tabloda belirtilen ortamlarda ve sürelerle saklanır. Bunun dışında Kanun'da yer alan veri işleme şartlarına uygun olarak doğrudan veya dolaylı biçimde elde edilen diğer kişisel veriler, **Şirket** tarafından ilgili mevzuatın öngördüğü veya işleme amacının gerektirdiği süre boyunca hukuka ve dürüstlük kurallarına uygun olarak muhafaza edilmektedir.

7. KİŞİSEL VERİLERİN İŞLENMESİNİ GEREKTİREN SEBEPLER

Kişisel veriler;

1. İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
2. İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
3. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
4. Kanunun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun **Şirket** tarafından kabul edilmesi,
5. İlgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi yönündeki talebin **Şirket** tarafından reddedilmesi, verilen cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; ilgili kişinin Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
6. Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması durumlarında, **Şirket** tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

8. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE İŞLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için Kanun'un 12. maddesiyle Kanun'un 6/4. maddesi gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde **Şirket** tarafından teknik ve idari tedbirler alınmaktadır.

8.1. Teknik Tedbirler

Bilgi Güvenliği Politikasında belirtilen idari tedbirlerle birlikte, teknik tedbirlerden silme ve imha ile ilgili şu teknik tedbirler uygulanmaktadır

1. Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
2. **Şirket** bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemleri almaktadır.
3. Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
4. Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
5. **Şirket**, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
6. Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
7. Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
8. Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
9. Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

8.2. İdari Tedbirler

Bilgi Güvenliği Politikasında belirtilen idari tedbirlerle birlikte, idari tedbirlerden silme ve imha ile ilgili şu idari tedbirler uygulanmaktadır

1. Kişisel verilerin hukuka aykırı olarak işlenmenin ve erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, bilgi güvenliği, teknik bilgi beceri, Kişisel

Verilerin Korunması Kanunu ve ilgili diğer mevzuat hakkında, çalışanların niteliğinin geliştirilmesine yönelik eğitimler verilmektedir.

2. **Şirket** tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır. Çalışan ile **Şirket** arasındaki hizmet sözleşmelerine bu doğrultuda gizlilik kayıtları eklenmekte; çalışanlardan bu sır saklama yükümlülüklerinin görevden ayrılmalarının akabinde de devam edeceği yönünde taahhüt alınmaktadır.
3. Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.
4. Kişisel veri işleme envanteri hazırlanmış ve her bir faaliyet için işlenen verilerin işleme süreleri belirlenmiştir.
5. Bilgisayar Ortamındaki Ortak Dosyalarda Bulunan Kişisel Verilerin Temizlenmesi: İşe yaramayan dosya ve resimler silinmiş, işe yarayacağı düşünülen ya da belirtilen dosya ve resimler sadece IT'nin erişimde olan klasörlere eklenmiştir. Bilgi Güvenliği Politikası ve Temiz Masa Temiz Ekran Politikası ile her yıl başında çalışanlara e-posta ile tebliğ edilmek üzere uyarı metinleri oluşturulmuştur.
6. Erişim Yetkileri Güncellenmesi: Ortak dosyalardaki erişim yetkileri kısıtlanarak çalışanların sadece işleriyle ilgili dosyalara erişimi sağlanmıştır. Yeni erişim yetkisi yönetici onayı ve yazılı talep sonrasında verilecek şekilde düzenlenmiştir.
7. İK Ortak Klasörünün Güncellenmesi: Bilgisayar ortamındaki İK klasörleri taranarak gereksiz ya da artık güncelliği kalmamış tüm kişisel veriler temizlenmiştir.
8. Çalışanların e-postalarında yer alan süresi dolmuş kişisel veri içeren e-posta ve eklerinin silinmesi konusunda yıllık uygulama yapılmakta ve çalışanlar uyarılmaktadır.

Şirket, Kurul tarafından aksine bir karar alınmadıkça, Yönetmelik gereği kişisel verileri re'sen silme, yok etme veya anonim hale getirmeye yönelik aşağıda yöntemlerinden uygun olanını seçmeye yetkilidir. Veri sahibinin talebi halinde, uygun yöntemi gerekçesini açıklayarak seçer. **Ayrıca, Şirket**, kişisel verilerin hukuka uygun olarak silinmesi, yok edilmesi veya anonim hale getirilmesi için her türlü teknik ve idari tedbiri almaktadır.

9. KİŞİSEL VERİLERİN SİLİNMESİ

9.1.Kişisel Verilerin Silinmesi Süreci

Kurumun **Rehberindeki s**ürece uygun şekilde **Şirket** bünyesindeki kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

Silinecek verilerin tespiti → İlgili kullanıcıların tespiti → Kullanıcıların erişim yöntemlerinin tespiti → Verilerin silinmesi (Erişimin kaldırılması)

9.2. Kişisel Verilerin Silinmesi Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun ve Rehberde önerilen yöntemlerden bazıları ya da tamamı tercih edilerek silinir.

9.2.1 Bulut Hizmeti vb. (*Office 365, Salesforce, Google Drive, One Dirve, Dropbox gibi*) Uygulamalardaki Veriler: Bulut ortamındaki verilere "*silme*" komutu verilerek silme gerçekleştirilir. Silme işlemi gerçekleştirilirken, ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilir.

9.2.3 Fiziksel-Kağıt Ortamda Yer Alan Kişisel Veriler: Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Kağıt ortamında bulunan kişisel veriler "*karartma*" yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, üzeri okunamayacak şekilde çizilerek / boyanarak / silinerek ilgili kullanıcılara görünemez hale getirilmesi işlemidir.

9.2.4.Merkezi Sunucuda Yer Alan Kişisel Veriler: Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili dosyanın işletim

sistemindeki "*silme*" komutu ile silinmesi veya ilgili kullanıcıların *erişim yetkisi kaldırılması* işlemidir. Söz konusu işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilir.

9.2.5.Elektronik Ortamda (*Ortak alanlar*, *Veri tabanları*) Yer Alan Kişisel Veriler): Şirket departmanlarının (İK, Muhasebe gibi) iş faaliyetleri için elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, -veri tabanı yöneticisi hariç- diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

9.2.6.Elektronik postalarda yer alan Kişisel Veriler: Kişisel veri bulunduran elektronik postalar Tablo'da belirtilen sürelerin sonunda silinir. Elektronik posta sunucularında tutulan epostalar silinme işleminin ardından 30 günlük süre sonunda imha edilmektedir. Çalışanların kendi cihazlarında tuttukları e-postaların silinmesi konusunda da bu sürelere uyulur. Elektronik postalar, sunucularda kotanın dolması ve/veya önemsiz veya işlevi kalmayan epostaların silinmesi gibi ihtiyaçlar sebepleriyle bir tutanakla kaydedilmek şartıyla "Saklama Süreleri Tablosunda" belirtilen sürelerden önce silinebilir.

9.2.7.Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, "şifreli" olarak saklanmalı ve bu ortamlara "uygun yazılımlar" kullanılarak silinir. Bu ortamlardaki kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek "şifreleme anahtarlarıyla" güvenli ortamlarda saklanır.

10. KİŞİSEL VERİLERİN İMHASI (YOK EDİLMESİ)

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Kurumun Rehberinde **Kişisel Verilerin Yok Edilmesi Yöntemleri** başlığı altında bazı İmha yöntemlerine yer verilmiştir. Kuruluş, sahip olduğu verilerin miktarı ve türü, işleme ve saklama ortamlarının özelliği gibi kriterleri dikkate alarak sayılan yöntemlerden birini, birkaçını ya da tamamını tercih edebilir:

10.1 Yerel Sistemler: Söz konusu sistemlerde yer alan verilerin yok edilmesi için, Kuruluşun işlediği veri türleri ve veri tabanına uygun olacak şekilde bazı yöntemler söz konusudur.

- De-manyetize etme
- Fiziksel Yok etme
- Üzerine Yazma

10.2 Çevresel Sistemler: Yine *ortamın* türüne göre tercih edilebilecek imha yöntemleri Rehberde aşağıdaki gibi sayılmaktadır.

- Ağ Cihazları (switch, router, vb)
- Flash tabanlı ortamlar
- Manyetik bant
- Manyetik disk gibi üniteler
- Mobil telefonlar (Sim kart ve sabit hafıza alanları)
- Optik diskler
- Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri

10.3 Kağıt ve Mikrofiş Ortamları: Kişisel verileri kayıtlı olduğu *Kağıt* gibi fiziksel ortamlar, kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünerek imha edilir.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

10.4 Bulut Ortamı: Bulut ortamlarındaki kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılmasına dikkat edilir. Bulut

bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi sağlanır.
10.5 Diğer Ortamlar: Bakım onarım ya da teknik destek nedeniyle tedarikçiye gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:
i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (10.1)'de belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,
ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması.
İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, **Şirket** tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak sayılan tekniklerle imha edilir. **Şirket** sahip olduğu teknolojik imkanlar ve uygulama maliyetleri ile sınırlı olarak, sayılan yöntemlerden en uygun imha yöntemlerini kullanılmaktadır.

11. ANONİM HALE GETİRME

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu anlamda **Şirket** 6698 sayılı Kanun uyarınca ihdas edilen Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i esas alarak, Kurumca yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'ndeki Anonimleştirme Yöntemlerinden uygun olanı seçer. Bu yöntemler:

11.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

a) Değişkenleri Çıkartma
b) Kayıtları Çıkartma
c) Bölgesel Gizleme
ç) Genelleştirme
d) Alt ve Üst Sınır Kodlama
e) Global Kodlama
f) Örnekleme

11.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

a) Mikro Birleştirme
b) Veri Değiş Tokuşu
c) Gürültü Ekleme

Şirket ayrıca anonimleştirmeyi güçlendirmek amacıyla Rehber'de belirtilen
a) K-Anonimlik
b) L-Çeşitlilik
c) T-Yakınlık
yöntemlerinden bir ya da birkaçını tercih edebilir.
Anonimlik Güvencesi: **Şirket**, anonimleştirme kararı alırken,

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması,
- Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi

hususlarını ve Rehber'de konuyla ilgili öngörülen risk faktörlerini dikkate alır.

12. İMHA SÜRECİNİN DENETİMİ

İmha süreçleri, **Şirket** bünyesinde kişisel veri işleme süreçlerinin hukuka uygunluğunu sağlamak üzere oluşturulan **Görevli** tarafından denetlenmektedir. Periyodik imha süreçleri, bu birim bünyesindeki en az iki kişi tarafından birlikte gerçekleştirilmekte, imha edilen kişisel verilerin herhangi bir kopyasının alınmadığı hususunda bu kişilerden yazılı taahhüt alınmaktadır. Görevliler ayrıca **Görevli** tarafından belirlenecektir.

13. SAKLAMA SÜRELERİ

Şirket tarafından **Saklama Süreleri Tablosu'nda** belirtilen faaliyetler kapsamındaki kişisel veriler yine aşağıda belirtilen yasal gerekçelerle belirlenen saklama sürelerinin sonunda tutuldukları ortamlardan silinir.

14. PERİYODİK İMHA SÜREÇLERİ

Şirket, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. Yönetmeliğin 11. maddesi gereğince Kurul, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, **Şirket** her yıl **OCAK** ve **TEMMUZ** aylarında periyodik imha işlemi gerçekleştirilir.
Kişisel verilerin silinmesi, yok edilmesi ve 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 saklanmaktadır.

15. YÜRÜRLÜK

Politika, yönetimin kararı ile yürürlüğe girer. Yetkililerince imzalanır ve taranmış nüshası elektronik ortamda yayımlanarak kamuya açıklanır. Basılı kâğıt nüshası da **Görevli** tarafından dosyasında saklanır.
Politikanın uygulanması ise Yönetim Kurulunun kararı ile atanan **Görevli** tarafından takip edilir. Yönetim kurulu, re'sen ya da **Görevli** önerisi üzerine Politika yenileyebilir, Politikada değişikliklere gidebilir.

16. İLGİLİ ARAÇLAR VE KAYNAKLAR

16.1 İlgili Kontrol ve Güvence Araçları

1. Gizlilik Politikası
2. Bilgi Güvenliği Politikası
3. Kişisel Veri Envanteri

16.2 Dış Kaynaklar

1. *6698 sayılı Kişisel Verilerin Korunması Kanunu*
2. *KVKK Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi*
3. *KVKK Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)*
4. *KVKK Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber*
5. *KVKK Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*

Daha fazla bilgi için **Görevli** ile temas kurabilirsiniz.