1. POLİTİKANIN AMACI VE TANIMLAR

1.1. AMAÇ

Veri sorumlusu Akyürek Makine San. Ve Tic. A.Ş. ve Akyurektech Tarım Ürünleri ve Makinaları Dış Tic. San. Ltd. Şti (AKYÜREK) olarak, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") uyarınca yükümlülüklerimizi yerine getirmek ve veri sahiplerinin kişisel verilerini işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirmek amacıyla işbu Kişisel veri saklama ve İmha Politikası (Politika) hazırlamıştır.

1.2. TANIMLAR

Açık Rıza	:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Akyürek	:	Akyürek Makine San. ve Tic. A.Ş. ve Akyurektech Tarım Ürünleri ve Makinaları Dış Tic. San. Ltd. Şti
Alıcı grubu	:	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişiler. Gerçek Kişiler veya Özel Hukuk Tüzel Kişileri, İş Ortakları, Tedarikçiler, Yetkili Kamu Kurum ve Kuruluşları.
Elektronik Ortam	:	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
Fiziksel Ortam	:	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
İlgili kişi	:	Kişisel verisi işlenen gerçek kişi
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 kişiler
İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilme
Kanun	:	24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu
Kişisel veri	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişi Grubu	:	Çalışan Adayı, Çalışan, Hissedar/Ortak, Potansiyel Ürün veya Hizmet Alıcısı, Stajyer, Tedarikçi Çalışanı, Tedarikçi Yetkilisi, Ürün veya Hizmet Alan Kişi, Ziyaretçi, Diğer-Aile Bireyi ve Yakını, İş Ortağı/ Çözüm Ortağı, Alt İşveren, Öğrenci, İşbirliği İçinde Olduğumuz Kurumların Çalışanı/Yetkilisi/Hissedarı olan kişiler
Kurul	:	Kişisel Verileri Koruma Kurulu
Kurum	:	Kişisel Verileri Koruma Kurumu
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
Kişisel veri işleme envanteri	:	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel Verilerin Anonim hale getirilmesi	:	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi

Kişisel Verilerin Silinmesi	:	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel Verilerin yok edilmesi	:	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik	:	28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği
Periyodik imha	:	Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
Sicil	:	Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili
Veri kayıt sistemi	:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi

2. ORTAMLAR VE GÜVENLİK TEDBİRLERİ

2.1. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

AKYÜREK'te saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında saklanır. AKYÜREK her halde veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri Kanun'a, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak işlemek ve korumaktadır.

Fiziki ortamlar	Kâğıt, manuel veri kayıt sistemi (anket formları, ziyaretçi kayıt defterleri, araç kayıt defterleri, Yazılı ve basılı görsel çıktısı
Yerel elektronik ortamlar	Sunucular (Yedekleme, e-posta, veri tabanı, ortak ağ paylaşımı vb.), Kişisel Bilgisayarlar (Masaüstü, dizüstü) Mobil cihazlar (Telefon, tablet vb.) Çıkartılabilir bellekler (USB, hafıza kartı vb.)
Bulut ortamlar	AKYÜREK bünyesinde yer almamakla birlikte, AKYÜREK'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

2.2. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR GÜVENLİĞİNİN SAĞLANMASI

AKYÜREK kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır. İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsamaktadır.

2.2.1.TEKNİK 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.

- ✓ Erişim logları düzenli olarak tutulmaktadır.
- ✓ Gerektiğinde veri maskeleme 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.
- ✓ Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- ✓ Saldırı tespit ve önleme sistemleri kullanılmaktadır
- ✓ Sızma testi uygulanmaktadır.
- ✓ Şifreleme yapılmaktadır.
- ✓ Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- ✓ Veri kaybı önleme yazılımları kullanılmaktadır.
- ✓ Çalışanlar için yetki matrisi oluşturulmuştur.
- ✓ Kişisel veri güvenliğinin takibi yapılmaktadır.
- ✓ Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

2.2.2.İDARİ TEDBİRLER

- ✓ Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- ✓ 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.
- ✓ İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- ✓ Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- ✓ Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- ✓ 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 veriler mümkün olduğunca azaltılmaktadır.
- ✓ Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- ✓ Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- ✓ Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- ✓ Mevcut risk ve tehditler belirlenmiştir.

2.2.3.İÇ DENETİM

AKYÜREK, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin iç denetimler yapmaktadır. İç denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilmektedir. Denetim sırasında ya da sair bir şekilde AKYÜREK sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması halinde, AKYÜREK bu durumu en kısa sürede ilgilisine ve Kurula bildirmektedir.

3. KİŞİSEL VERİLERİN SAKLAMA ve İMHASI

3.1. SAKLAMAYI GEREKTİREN SEBEPLER

- ✓ Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- ✓ Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- ✓ Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- ✓ Kişisel verilerin Şirket'in herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- ✓ Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- ✓ Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

3.2. İMHAYI GEREKTİREN SEBEPLER

- ✓ Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- ✓ Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- ✓ Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- ✓ Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Akyürek tarafından kabul edilmesi,
- ✓ İlgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- ✓ Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

3.3. İMHA YÖNTEMLERİ

AKYÜREK, Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir. Akyürek tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır.

3.3.1.SİLME YÖNTEMLERİ

Fiziki ortamlardaki veriler	Fiziki ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. 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 görünemez hale getirilmesi şeklinde yapılır.
Yerel elektronik ortamlardaki veriler	Yerel elektronik ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz. Yerel elektronik ortamlarda bulunan kişisel veriler, verinin bulunduğu dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarını kaldırılarak da silme işlemi yapılır.
Bulut ortamlardaki veriler	Bulut ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz. Yerel elektronik ortamlarda bulunan kişisel veriler, verinin bulunduğu dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarını kaldırılarak da silme işlemi yapılır.

3.3.2.YOK ETME YÖNTEMLERİ

Fiziki ortamlardaki veriler	Fiziki ortamda bulunan kişisel veriler evrak imha makineleri kullanılarak tekrar bir araya getirilemeyecek şekilde yok edilir.
Yerel elektronik ortamlardaki veriler	FİZİKSEL YOK ETME: Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. DE-MANYETİZE ETME (DEGAUSS) : Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması sağlanır. ÜZERİNE YAZMA: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.
Bulut ortamlardaki veriler	Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

3.3.3.ANAONİM HALE GETİRME YÖNTEMLERİ

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir. AKYÜREK anonimleştirme yöntemlerinin hiçbirini KULLANMAMAKTADIR.

4. KİŞİSEL VERİ SAKLAMA VE İMHA SÜREÇLERİ SORUMLULUK VE GÖREV TANIMLARI

SORUMLU	YETKİLER ve SORUMLULUKLAR
YÖNETİM KURULU	✓ Kanuna uyumluluk sürecinde yürütülen projeler, Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülen süreçler için kaynakları sağlamakla, ✓ BGYS ekibinden ve/veya ilgili kişilerce gelen talepleri karara bağlamakla,

	✓ Belli ve/veya belirsiz zamanlarda iç denetim yaptırmakla yükümlüdür.
BGYS (Bilgi Güvenliği Yönetim Sistemleri) LİDERİ	✓ Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yapmak, yaptırmakla, ✓ Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülen süreçleri yönetmek, ekibini sevk ve idari etmekle, ✓ Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikalarının uygunluğunu denetlemek, yaygınlığını arttırmak için yöntemler belirlemek, uygulamak, eğitimlerin yapmak ve yaptırmakla, ✓ Saklama ve imha süreçlerinin yürütmekle, ✓ İlgili kişilerden gelen talepleri değerlendirmek, karara bağlamak, karara bağlamak için yönetim kuruluna bildirmekle, ✓ Veri envanterini hazırlanması ve güncel tutulması için gerekli süreç analizlerini yapmak ve yaptırmakla, ✓ Belli ve/veya belirsiz zamanlarda iç denetim yapmakla yükümlüdür.
BGYS (Bilgi Güvenliği Yönetim Sistemleri) EKİBİ	✓ BGYS Lideri tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin alınan kararlar uyarınca yerine getirmekle, ✓ Saklama ve imha süreçlerinin denetlemek ve raporlamakla, ✓ Çalışanlara KVKK eğitimlerini vermek, eğitimleri güncel tutmakla, ✓ Politikanın uygulanması için gerekli teknik tedbirler için çözüm sunmakla, ✓ Veri güvenliğini sağlamak için idari ve teknik tedbirleri almak aldırmak, denetlemekle, ✓ Elektronik ortamda işlenme nedeni ve saklama süresi biten verilerin imhasını sağlamak, sağlatmakla yükümlüdür.
İRTİBAT KİŞİSİ	✓ VERBİS e veri kayıt işlemlerini gerçekleştirmek, güncelleştirmeleri yapmak ✓ İlgili kişiler ve kurumdan gelen iletileri sonuçlandırmakla yükümlüdür.

5. KİŞİSEL VERİ SAKLAMA VE İMHA SÜRELERİ

5.1. Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

5.2. AKYÜREK, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder.

5.3. İlgili kişi, Kanunun 13'ncü maddesine istinaden AKYÜREK'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

5.3.1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; AKYÜREK talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. AKYÜREK' in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. AKYÜREK, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.

5.3.2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep AKYÜREK tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Veri Kategorisi	Veri Saklama Süresi	İmha Süresi
Kimlik	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Lokasyon	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Özlük	İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki İşlem	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri İşlem Veri	Müşteri ilişkisinin sona ermesi +10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Fiziksel Mekan Güvenliği	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem Güvenliği	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mesleki Deneyim	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Pazarlama	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Görsel Ve İşitsel Kayıtlar	Hukuki ilişkinin sona ermesi+10 yıl / İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kılık Ve Kıyafet	İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık Bilgileri	İş sözleşmesinin sona ermesi +15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	İş sözleşmesinin sona ermesi +15 yıl/Başvurunun olumsuz sonuçlanması itibariyle 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Diğer Bilgiler- Çalışan Adayı/Stajyer	İş sözleşmesinin sona ermesi +15 yıl/Başvurunun olumsuz sonuçlanması itibariyle 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Diğer Bilgiler-Aile Bireyleri ve Yakın Bilgisi	İş sözleşmesinin sona ermesi +15 yıl/Başvurunun olumsuz sonuçlanması itibariyle 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

6. PERİYODİK İMHA

Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik kapsamında periyodik imha süresini 6 ay olarak belirlenmiştir.

Akyürek her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirir.

7. POLİTİKANIN YÜRÜRLÜĞE GİRMESİ, GÜNCELLENME PERİYODU VE YÜRÜRLÜKTEN KALDIRILMASI

7.1. AKYÜREK, Kişisel veri işleme, saklama ve imha politikasını ıslak imzalı (basılı kağıt) ve elektronik olmak üzere iki farklı ortamda yayımlar.

7.2. İnternet sayfamız www.akyurekltd.com da kamuya açık olarak sunulmuştur.

7.3. İnternet sitemizde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

7.4. Basılı kağıt nüshası Yönetim Sistemleri tarafından saklanır.

7.5. Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenerek tekrar yayınlanır.

7.6. Politikada yapılan güncellemeler derhal metne işlenir, güncellemelere ilişkin açıklamalar politikanın sonunda açıklanır ve internet sitesinde yayınlanır. Islak imzalı eski nüshaları da iptal kaşesi vurularak 10 yıl süreyle saklanır

7.7. Yayın tarihi 14.02.2019 ve revizyon numarası V00 dir, Son güncelleme ile _____ tarihli ve _____ revizyon numaralı politika yürürlükten kalkmıştır.