BYZ BEYAZ GIDA PAZARLAMA DAĞITIM SANAYİ ve TİCARET LİMİTED ŞİRKETİ

KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1.GİRİŞ

1.1 Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası ("**Politika**") yürürlükteki mevzuat çerçevesinde Byz Beyaz Gıda Pazarlama Dağıtım Sanayi Ve Ticaret Limited Şirketi'nin (Bundan sonra **"Şirket"** olarak anılacaktır.) tamamına uygulanmakta ve kişisel veri imha ile ilgili ulusal olarak kabul görmüş temel ilkelere dayanmaktadır. İlgili mevzuat kapsamında gerekli imha çalışmalarının yapılmasına ilişkin çerçeve ve esasları içermektedir.

Kişiler Verilerin Korunması Kanunu'nun ("Kanun") 7nci maddesinin üçüncü fıkrasında "Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir" hükmü yer almaktadır. Bu hüküm ve Kanun'un 22 nci maddesinin birinci fıkrasının (e) bendine istinaden Kişisel Verileri Koruma Kurulu ("Kurul") tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") hazırlanmış olup 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete'de yayımlanmıştır.

Yukarıdaki düzenlemeye dayanarak, bu Politikanın amacı, Şirketin faaliyetlerinin yürütülmesinde işlediği kişisel verilerin, Yönetmeliğe uygun şekilde silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

1.2.Kapsam

Şirketimizin hukuki ilişkide bulunduğu çalışan, çalışan yakını, çalışan adayı, kamu görevlisi, kefil, tedarikçi, tedarikçi yetkilisi, tedarikçi çalışanı, ürün veya hizmet alan kişi, ürün veya hizmet alan kişi yetkilisi/çalışanı, potansiyel ürün veya hizmet alıcısı, hissedar/ortak, veli, ziyaretçi, üçüncü kişiler ve üçüncü kişilerin çalışanlarına ait kişisel veriler bu Politika kapsamında olup Şirketin sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. Kısaltmalar ve Tanımlar

Kavram	**Tanım**
Alıcı grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan 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 kişileri
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu
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	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel veri sahibi	Kişisel verisi işlenen gerçek kişi
Kişisel verinin işlenmesi	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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi
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 envanter
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
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
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
Politika	Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika.
Sicil	Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini

Veri işleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişiyi
Veri kayıt sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini
Veri sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder
Yönetmelik	28.10.2017 tarih ve 30224 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. SORUMLULUK ve GÖREV DAĞILIMLARI

Şirketin 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.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıda verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımları

Ünvan	**Birim**	**Görev Tanımı**
Bilgi İşlem Yetkilisi	Bilgi İşlem	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürecinin yönetimi, Veri Sahiplerinin taleplerinin yanıtlanması için gerekli denetim ve kontrollerin yapılması
Muhasebe Yetkilisi	Muhasebe	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürenin yönetimi, 6100 sayılı TTK ve Vergi Mevzuatından kaynaklanan defter, belge saklama yükümlülüklerinin devamının ve yükümlülüklerin ortadan kalkıp kalmadığının kontrolü
İnsan Kaynakları Yetkilisi	İnsan Kaynakları	Personel kişisel verilerinin saklama süresine uygunluğunun sağlanması, periyodik imha

		sürecinin yönetimi, Personellerin Kanun'da belirtilen hakları ile ilgili aydınlatılması taleplerinin alınması ve cevaplandırılması
Satın Alma Yetkilisi	Satın Alma	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürenin yönetimi, yükümlülüklerin ortadan kalkıp kalmadığının kontrolü
Satış Sorumlusu	Satış	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürenin yönetimi, yükümlülüklerin ortadan kalkıp kalmadığının kontrolü
İSG Yetkilileri	İSG Uzmanı İş Yeri Hekimi	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması, periyodik imha sürenin yönetimi, yükümlülüklerin ortadan kalkıp kalmadığının kontrolü

3.KAYIT ORTAMLARI

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

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
• Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) • Yazılımlar (ofis yazılımları) • Bilgi güvenliği cihazları (güvenlik duvarı, günlük kayıt dosyası, antivirüs vb.) • Mobil cihazlar (telefon, tablet vb.) • Optik diskler (CD, DVD vb.) • Çıkartılabilir bellekler (USB, Hafıza Kart vb.) • Yazıcı, tarayıcı, fotokopi makinesi • USB, harddisk gibi çıkarılabilir bellekler • Masaüstü ve dizüstü bilgisayar	• Kağıt • Manuel veri kayıt sistemleri • Yazılı, basılı, görsel ortamlar • Klasörler • Dosyalar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; çalışan, çalışan yakını, çalışan adayı, kamu görevlisi, kefil, tedarikçi, tedarikçi yetkilisi, tedarikçi çalışanı, ürün veya hizmet alan kişi, ürün veya hizmet alan kişi yetkilisi/çalışanı, potansiyel ürün veya hizmet alıcısı, hissedar/ortak, veli, ziyaretçi ve sair üçüncü kişiler dahil gerçek kişilerin kişisel verileri KVKK'ya uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 Saklamaya İlişkin Açıklamalar

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Şirket faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Şirket, faaliyetleri çerçevesinde işlenen kişisel verileri, ilgili mevzuatta öngörülen süre kadar muhafaza eder. Bu kapsamda kişisel veriler;

- 213 sayılı Vergi Usul Kanunu
- 4857 sayılı İş Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6098 sayılı Türk Borçlar Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu

başta olmak üzere yürürlükte olan diğer ikincil mevzuatta yer alan saklama süreleri kadar saklanmaktadır.

4.1.2. Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
- Denetim / Etik Faaliyetlerinin Yürütülmesi
- Eğitim Faaliyetlerinin Yürütülmesi

- Erişim Yetkilerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi
- Finans ve Muhasebe İşlerinin Yürütülmesi
- Fiziksel Mekan Güvenliğinin Temini
- Görevlendirme Süreçlerinin Yürütülmesi
- Hukuk İşlerinin Takibi Ve Yürütülmesi
- İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- İletişim Faaliyetlerinin Yürütülmesi
- İnsan Kaynakları Süreçlerinin Planlanması
- İş Faaliyetlerinin Yürütülmesi / Denetimi
- İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- Lojistik Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
- Organizasyon Ve Etkinlik Yönetimi
- Performans Değerlendirme Süreçlerinin Yürütülmesi
- Risk Yönetimi Süreçlerinin Yürütülmesi
- Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Stratejik Planlama Faaliyetlerinin Yürütülmesi
- Taşınır Mal Ve Kaynakların Güvenliğinin Temini
- Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- Ücret Politikasının Yürütülmesi
- Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
- Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- Yönetim Faaliyetlerinin Yürütülmesi

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişini açık rızasını geri alması,

- KVKK'nın 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerin silinmesi ve yok edilmesine ilişkin yapılan başvurunun kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya KVKK'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması ve
- 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.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için KVKK'nın 12. maddesi ile 6. maddesinin 4. fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirket tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan tedbirler aşağıda sayılmıştır;

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

5.2. İdari Tedbirler

Şirket tarafından, işlediği kişisel verilerle ilgili olarak alınan tedbirler aşağıda sayılmıştır;

- Gizlilik taahhütnameleri yapılmaktadır.
- 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.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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 aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel verilerin silinmesi

Veri Kayıt Ortamı	**Açıklama**
Fiziksel ortamda yer alan kişisel veriler	Fiziksel ortamda bulunan kişisel veriler karartma yöntemi kullanılarak veya belgenin, ilgili kullanıcılar tarafından hiçbir şekilde erişilmeyecek şekilde güvenli bir ortamda saklanılması suretiyle silinmektedir.
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Veri tabanlarında yer alan kişisel veriler	İlgili kullanıcının, rol ve izin ataması yapılarak, veri tabanında yer alan kişisel verilere erişimi engellenmektedir.
Taşınabilir cihazlarda (USB, Hard disk, CD, DVD gibi) yer alan kişisel veriler	İlgili kullanıcının dosyaya erişimi engellenmektedir.

6.2. Kişisel Verilerin Yok Edilmesi

Şirket olarak, kişisel verilerin hukuka uygun olarak yok edilmesi işlemini gerçekleştirebilmek amacıyla tarafımızca kullanılan yöntemler şu şekildedir:

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	**Açıklama**
Fiziksel ortamda yer alan kişisel veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Çevresel (ağ cihazları, flash tabanlı ortamlar, optik sistemler vb.) ve yerel sistemlerde yer alan kişisel veriler	Kişisel veri içeren cihazlar; yakma, küçük parçalara ayırma, eritme gibi fiziksel işlemlerle yok edilmektedir. Ayrıca, demanyetize etme yöntemi ile aygıtın üzerinde yer alan kişisel veriler okunamaz hale getirilerek yok etme işlemi gerçekleştirilmektedir. Bununla birlikte; özel yazılımlar ile var olan verilerin üzerine rastgele veri

	girişi yapılması sonucu eski verilerin kurtarılmasının önüne geçilerek yok etme işlemi uygulanmaktadır.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından, faaliyetler kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise iş bu Kişisel Veri Saklama ve İmha Politikasında yer alır.

Kişisel verilerin imha süreci, Şirket tarafından her bir ilişkiye uygun olarak ilgili mevzuat gözetilerek belirlenmiş olan saklama süreleri doğrultusunda yürütülmektedir. Saklama süreleri sona eren kişisel veriler, Şirket tarafından belirlenmiş olan periyodik imha sürelerinde silinir, yok edilir veya anonim hale getirilir.

Tablo 5: Süreç Bazında Saklama ve İmha Süreleri Tablosu

SÜREÇ	**SAKLAMA SÜRESİ**	**İMHA SÜRESİ**
İnsan kaynakları çalışan süreçlerinin yürütülmesi	Çalışanın işten ayrılmasından itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
Çalışan adaylarına ilişkin süreçlerin yürütülmesi	İşe kabul edilmeme durumunda başvuru tarihinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
Sözleşme süreçlerinin yürütülmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
Kamera kayıtları	Kayıt altına alınmasını takiben 15 Gün	Kayıt süresinin sonunda otomatik olarak imha edilmekte

Muhasebe ve finans süreçlerinin yürütülmesi	Kayıt altına alınmasını takiben 10 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
Satın alma ve Satış süreçlerinin yürütülmesi	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
Biyometrik veri	İşten ayrılmasından itibaren 1 ay	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde
İş sağlığı ve güvenliği faaliyetlerinin yürütülmesi	Çalışanın işten ayrılmasından itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk 6 aylık periyodik imha süresinde

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi "2.SORUMLULUK VE GÖREV DAĞILIMLARI" başlığı altında yer verilen departmanlar tarafından yerine getirilir.

8. PERİYODİK İMHA SÜRESİ

Yönetmelik'in 11. maddesi gereğince periyodik imha süresi, Şirket tarafından, [6] ay olarak belirlenmiştir. Buna göre, Şirket tarafından her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. POLİTİKA'NIN YAYIMLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da İnsan Kaynakları Departmanında dosyasında saklanır.

10. POLİTİKA'NIN GÜNCELLEME PERİYODU

Politika, ihtiyaç duyulduğunda ve değişen süreçler bulunduğunda güncellenir.

11. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

İşbu Politika, Şirkete ait internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları şirket kaşesi ve şirket yetkilisi imzası ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile İnsan Kaynakları Departmanı tarafından saklanır.