KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. VERİ SORUMLUSUNUN KİMLİĞİ VE POLİTİKA KAPSAMI

Kişisel Verileri Saklama ve İmha Politikası (kısaca "POLİTİKA" olarak anılacaktır), Veri sorumlusu sıfatını taşıyan ALCAP AMBALAJ SANAYİ VE TİCARET A.Ş. (kısaca "ALCAP" olarak anılacaktır) tarafından gerçekleştirilmekte olan veri saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.

İşbu POLİTİKA, ALCAP tarafından ilgili kişilere ait kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu. (KVKK) ve ilgili mevzuata uygun olarak işlenmesi, saklanması ve "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" hükümleri kapsamında periyodik olarak imha edilmesi faaliyetlerine ilişkin bilgi ve prosedürleri içermektedir.

2. TANIMLAR

Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
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
Veri Sahibi / İlgili Kişi	Kişisel verisi işlenen gerçek kişi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Açık Rıza	Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
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.

Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale gelmesi
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 hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
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.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Kurum	Kişisel Verileri Koruma Kurumu
Kurul	Kişisel Verileri Koruma Kurulu
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

3. VERİ İŞLEME FAALİYETLERİNİN HUKUKİ GEREKÇELERİ

ALCAP iş faaliyetleri kapsamında veri işleme faaliyetlerinin yasal çerçevesi, alttaki listede belirtilen kanun ve yasal düzenlemelere dayanmaktadır.

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 6098 sayılı Türk Borçlar 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
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu
- 4857 sayılı İş Kanunu
- 6102 sayılı Türk Ticaret Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

4. KAYIT ORTAMLARI

ALCAP tarafından işlenen kişisel veriler aşağıdaki fiziksel ortamlarda muhafaza edilmektedir.

- Kişisel bilgisayarlar
- Mobil cihazlar
- Manyetik ve optik kayıt ortamları
- Taşınabilir bellekler
- Sunucular
- Yazılımlar
- Bilgi güvenliği cihaz ve yazılımları
- Ses ve görüntü kaydedici cihaz ve yazılımlar
- Belge üretim, kopyalama cihazları
- Yazılı, basılı, görsel materyaller

5. KİŞİSEL VERİLERİN SAKLANMA VE İMHA SÜRELERİ

ALCAP tarafından elde edilen kişisel veriler, aşağıdaki tabloda belirtilen yasal süreler çerçevesinde saklanmakta ve muhafaza edilmektedir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Sözleşmelerin hazırlanması (iş sözleşmeleri, satış sözleşmeleri vb.)	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim faaliyetlerinin yürütülmesi	Faaliyetlerin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan kaynakları süreçleri	Faaliyetlerin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri işlem süreçleri (mal ve hizmet alım satım işlemleri vb.)	Faaliyetlerin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Finans ve muhasebe süreçleri (bordro bilgileri, faturalar vb.)	Faaliyetlerin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sağlık Bilgileri kaydı (İş sözleşmesi kapsamındaki sağlık raporları)	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Ceza Mahkûmiyeti kaydı (İş sözleşmesi kapsamındaki yasal belgeler)	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Görsel ve işitsel verilerin işlenmesi süreci (Fiziksel mekân ve taşınır malların güvenliği amaçlı görüntü kayıtlarının alınması, çağrı merkezi ses kayıtları)	Veri toplanmasını takiben 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşlem güvenliği süreçleri (kurumsal ağ ve internet sitesi üzerinden toplanan veriler)	Veri toplanmasını takiben 2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

6. PERİYODİK İMHA SÜRESİ

ALCAP, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

7. KİŞİSEL VERİLERİN SİLİNMESİ

ALCAP tarafından işlenen 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 kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun şirket tarafından kabul edilmesi,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

Koşulları gerçekleştiğinde, ALCAP tarafından silinir, yok edilir veya anonim hale getirilir.

8. VERİ GÜVENLİĞİ İÇİN ALINAN ÖNLEMLER

ALCAP kişisel verilerin korunması için aşağıda belirtilen teknik ve idari önlemleri almaktadır. Teknik ve idari önlemlerle ilgili sorunlar ilgili birimlere acil olarak bildirilmektedir.

8.1. İDARİ ÖNLEMLER

Kişisel veri güvenliğini temin etmek için ALCAP tarafından alınan idari önlemler:

- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- 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.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- 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.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

8.2. TEKNİK ÖNLEMLER

ALCAP tarafından, işlenen kişisel verilerle ilgili olarak alınan teknik önlemler aşağıda sıralanmıştır

- Kişisel veri güvenliğini temin etmek amacıyla ALCAP tarafından alınan teknik önlemler:
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- 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.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.
- 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.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- 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 mümkün olduğunca azaltılmaktadır.
- 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.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.

9. KİŞİSEL VERİLERİN SİLİNMESİ VE İMHASI

Elektronik ortamda kayıtlı olan kişisel veriler, saklanmasını gerektiren süre sona erdiğinde ilgili kullanıcılar için hiç bir suretle erişilemez ve kullanılamaz hale getirilir.

Fiziksel ortamlarda kayıtlı olan kişisel veriler, saklanmasını gerektiren süre sona erdiğinde kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

10. SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce POLİTİKA kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması ve denetimi konularında sorumlu birimlere aktif olarak destek verirler.

Kişisel verilerin saklama ve imha süreçlerindeki görev dağılımı aşağıdaki tabloda yer almaktadır.

UNVAN	BİRİM	GÖREV TANIMI
Genel Müdür	Genel Yönetim	Çalışanların POLİTİKAya uygun hareket etmesinden sorumludur POLİTİKA'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur
Kalite Yönetim Temsilcisi	Kalite Güvence Departmanı	POLİTİKA'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur
Muhasebe, Finans, İnsan Kaynakları, Satın Alma, İdari ve Mali İşler	Diğer Birimler	Görevlerine uygun olarak POLİTİKAnın yürütülmesinden sorumludur.

11. DİĞER HUSUSLAR

- POLİTİKA, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, İnternet sayfasında kamuya açıklanır.
- KVKK ve ilgili mevzuat hükümleri ile işbu POLİTİKA arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili mevzuat hükümleri uygulanacaktır.
- POLİTİKA metninde güncelleme yapılması durumunda, yeni POLİTİKA belgesi aynı yöntemlerle ilan edilerek yürürlüğe girer.