

KAYHANLAR

ULUSLARARASI TAŞIMACILIK

KİŞİSEL VERİ SAKLAMA

ve

İMHA POLİTİKASI

1.Amaç

İşbu politika Kayhanlar Ulaştırma Taşıma Petrol Ürün Sanayi Ticaret Ltd. Şti.'nin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5 ve 6. maddelerinde öngörülen yükümlülüklerini yerine getirebilmesi, ayrıca temel insan hakkı olan kişisel verilerin korunması hakkına verdiğimiz yüksek önem sebebiyle, kişisel verilerin imha usul ve süreçlerini açıklamak amacıyla hazırlanmıştır.

2.Kapsam

Bu politika, Şirketimiz ile bağlantılı tüm tarafların otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla, elektronik ortamda ya da basılı dokümanlarla işlenen tüm kişisel verilerini kapsamaktadır.

3.Kayıt Ortamları

Kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<p>Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)</p> <p>✓ Kişisel bilgisayarlar (Masaüstü, dizüstü)</p> <p>✓ Mobil cihazlar (telefon, tablet vb.)</p> <p>✓ Optik diskler (CD, DVD vb.)</p> <p>✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.)</p> <p>✓ Yazıcı, tarayıcı, fotokopi makinesi</p>	<p>✓ Kağıt</p> <p>✓ Manuel veri kayıt sistemleri (anket formları, başvuru formları, ziyaretçi giriş defteri vb.)</p> <p>✓ Yazılı, basılı, görsel ortamlar</p>

4.Uygulama

Şirket benimsemiş olduğu vizyon, misyon ve temel değerleri gereğince, idari süreçlerini ve iş süreçlerini bağlı olduğu mevzuatlar doğrultusunda yürütmek, hizmet verdiği kişilere en iyi deneyimi sağlamak için teknolojik kaynak ve altyapıları da kullanarak “veri minimizasyonu” prensibi çerçevesinde kişisel ve özel nitelikli kişisel verileri işler. Verilerin işlenmesinde kanunun 4. maddesinde belirtilen ilkeler ve 12. maddesi gereği alınması gereken tedbirler göz

önünde bulundurulurak işlem yapılır. Kayıt saklama ortamları, elektronik veriler için bilişim sistemi sunucuları, uygulamaları, kurumsal bilgisayar ve depolama ortamlarıdır, basılı dokümanlar için ise ofisler ve arşivlerdir.

4.1.Saklama Gerektiren Sebeplere İlişkin Açıklamalar

İlgili kişiye ait veriler, Şirket tarafından faaliyetlerinin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının planlanması, öğrencilere ve ailelerine sunulan hizmetlerin gerçekleştirilebilmesi, iş ortakları ile süreçlerin işletilebilmesi amacıyla fiziki veyahut elektronik ortamlarda güvenli bir biçimde Kanun ve ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanır.

Saklamayı gerektiren hukuki sebepler aşağıdaki gibidir:

- 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,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler.

Ayrıca kişisel veriler,

- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için saklanması zorunlu olması,
- Kişisel verilerin Şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması, hukuki sebepleri ile de saklanmaktadır.

5. Saklamayı Gerektiren İşleme Amaçları

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

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Kurum güvenliğini sağlamak,
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.

- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- İleride doğabilecek hukuki uyumsuzluklarda delil olarak ispat yükümlülüğü.

5.1.İmhayı Gerektiren Sebeplere İlişkin Açıklamalar

Yönetmelik uyarınca, aşağıda sayılan hallerde kişisel veriler veya özel nitelikli kişisel veriler, Şirket tarafından re' sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ortadan kalkması,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- İlgili kişinin, hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi ya da kurulun gereğinin yapılması yönünde karar vermesi.

6.Uygulanan Teknik ve İdari Tedbirler

Şirket, bünyesinde kanunun 7'nci ve 12'nci maddesi göz önünde bulundurularak veri saklamada ve imhada teknik ve idari tedbirler alır. Alınan tedbirler aşağıda belirtildiği gibidir;

6.1 İdari Tedbirler

- Şirket bünyesinde bilgi güvenliği yönetim sisteminin kurulması ve işletilmesi,
- Şirket personelleri ve ilgili taraflar ile taahhütnameler ve gizlilik sözleşmelerinin imzalanması ,
- Kişisel veri envanterlerinin oluşturulması,
- Bilgi güvenliği politika ve prosedürlerinin işletilmesi,
- Bilgi güvenliği ve kişisel veri işleme faaliyetleri hakkında eğitimlerin düzenlenmesi ve değerlendirilmesi,
- Çalışan bilgisayar vb. araç gereçlerine yetkisiz erişimlerin önüne geçmek adına söz konusu araç ve gereçleri yalnızca yetkili kişilerin kullanması,
- Şirket içi ya da bağımsız denetimler ile faaliyetlerin gözden geçirilmesi,
- Yapılan işlemler için objektif delil üretecek kayıtların oluşturulması,

6.2. Teknik Tedbirler

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlerle ilgili teknik kontroller yapılmaktadır.
- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili çalışmalar yapılmaktadır.
- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun hazırlık çalışmaları yapılmıştır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

7. Veri Silme, Yok Etme ve Anonim Hale Getirme

Bu politikanın 6.1 maddesinde belirtilen şartların ortadan kalkması halinde, kişisel veriler Şirket tarafından kendiliğinden veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hususta ilgili kişi tarafından Şirket’e başvurulması halinde;

- İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılır ve ilgili kişiye bilgi verilir,
- Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye bildirilir ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilir,
- Durum, şartlar ve mevzuat gereği ilgili kişinin talep ettiği imha usulünün yerine başka bir imha usulünün kullanılması gerekmektedirse, durum ilgili kişiye verilecek cevapta açıklanarak, kullanılması lazım gelen usul ile imha gerçekleştirilir,
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13’üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri kendiliğinden silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı tarafımızca seçilir. Ancak, ilgili kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilir.

İlgili kişinin Kanun’un 11. maddesinde gösterilen hakları kapsamında yaptığı başvurularda verilecek cevaplar ücretsiz olarak karşılanır. Her ne kadar cevabın ücretsiz verilmesi temel ilke olsa da, verilecek cevabın ayrıca bir maliyet gerektirmesi durumunda Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ’in 7. maddesinde gösterilen ücretler Şirket tarafından ilgili kişiden talep edilebilecektir. İlgili madde şöyledir:

Ücret

MADDE 7 – (1) İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.

(2) Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

7.1.Kişisel Veri Silme

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.

Elektronik Ortamda Yer Alan Kişisel Veriler : 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.

Fiziksel 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. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

Taşınabilir Medyada Bulunan Kişisel Veriler : Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

7.2.Kişisel Veri Yok Etme

Fiziksel Ortamda Yer Alan Kişisel Veriler : Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler yakılarak veya kâğıt kırıpma makinelerinde geri döndürülemeyecek şekilde öğütülerek yok edilir.

8.Verit Saklama ve İmha Süreleri ve Sorumluları

8.1.Verit Saklama ve İmha Süreleri

Verit saklama ve imha süreleri kişisel veri envanterinde detaylı olarak gösterilir. Verilerin saklama ve imha süreleri aşağıda belirtildiği gibidir. Kişisel veriler, saklama şartlarının ortadan kalkması üzerine, ilgili kişinin talebi ile veya süresinin gelmiş olması durumunda periyodik imha süresinde Şirket'nin uygun göreceği imha usulü ile imha edilir. Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirket'de her yıl **Haziran** ve **Aralık** aylarında periyodik imha işlemi gerçekleştirilir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Şirket İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen , hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	İş sözleşmesinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

2. Sorumluluk

Şirketin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanması sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

