KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İSKO PLASTİK VE KALIP SANAYİ TİCARET ANONİM ŞİRKETİ

İÇİNDEKİLER

1. AMAÇ VE KAPSAM

Amaç İSKO PLASTİK VE KALIP SANAYİ TİCARET ANONİM ŞİRKETİ (“İSKO” veya “Şirket” olarak anılacaktı) kişisel verilerin işlenmesi ve korunmasına ilişkin 6698 Kişisel Verilerin Korunması Kanunu ve ilgili mevzuata uyum kapsamında gerekli her türlü faaliyeti yürütmekte ve üzerine düşen tüm yükümlülükleri yerine getirmektedir. Kişisel Verileri Saklama ve İmha Politikası (“Politika”), İSKO tarafından gerçekleştirilmekte olan kişisel veri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

İSKO çalışanları, çalışan adayları, müşterileri, hizmet sağlayıcıları, tedarikçileri, iş ortakları, ziyaretçiler ve diğer üçüncü kişilere 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.

2. TANIMLAR VE KISALTMALAR

Açık Rıza	**:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Alıcı Grubu	**:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
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.
Hizmet Sağlayıcı	**:** Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel 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 getirilmesi.
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.
Kişisel veri	**:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kişisel verilerin 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.
Kişisel Veri İşleme Envanteri	**:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
Kişisel Verilerin Korunması Birimi	**:** İSKO tarafından, kişisel verilerin korunması mevzuatına uygunluğun sağlanması, muhafazası ve sürdürülmesi kapsamında Şirket bünyesinde gerekli koordinasyonu sağlayacak olan birimi ifade eder.
Kurul	**:** Kişisel Verileri Koruma Kurulu
Kurum	**:** Kişisel Verileri Koruma Kurumu
KVK Kanunu	**:** 6698 sayılı Kişisel Verilerin Korunması Kanunu
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 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 işlemi.
KVK Politikası	**:** İSKO Kişisel Verileri Saklama ve İmha Politikası
Veri işleyen	**:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.
Veri kayıt sistemi	**:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
Veri sahibi / İlgili Kişi	**:** Kişisel verisi işlenen gerçek kişiyi ifade eder.
Veri sorumlusu	**:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

Veri Sorumluları Sicil Bilgi Sistemi	**:** Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi.
VERBİS	**:** Veri Sorumluları Sicil Bilgi Sistemi

3. 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 gösterilmektedir;

Unvan	Birim	Görev
Yönetim Kurulu Başkanı	Yönetim Kurulu	Politikanın hazırlanması, güncellenmesi, değiştirilmesi ve ilgili ortamlarda yayımlanmasından sorumludur.
Kişisel Verileri Koruma Birimi Müdürü	Kişisel Verileri Koruma Birimi	Politikanın yürütülmesi, uygulanması, çalışanların Politikaya uygun hareket etmesi, Politikanın uygulanmasında ihtiyaç duyulan idari ve teknik çözümlerin sunulmasından sorumludur.
İnsan Kaynakları Müdürü, Bilgi İşlem Müdürü, Mali İşler Müdürü, Satış / Pazarlama Müdürü	İlgili Departmanlar	İş tanımları kapsamında görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

4. KAYIT ORTAMLARI

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

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
✓ Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar (ofis yazılımları, E-sistem, VERBİS.) ✓ 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 Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi	✓ Kağıt ✓ Manuel veri kayıt sistemleri (anket formları, dosyalar, ziyaretçi giriş defteri) ✓ Yazılı, basılı, görsel ortamlar

5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; topluluk şirketleri, müşteriler, tedarikçiler, iş ortakları, hizmet sağlayıcıları, çalışanlar, çalışan adayları ve ziyaretçiler olarak ilişkide bulunulan üçüncü kişilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

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

5.1. 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 amaçlarına uygun süre kadar saklanır. Bu kapsamda Şirket, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun olarak kişisel verileri muhafaza etmektedir. Yasal bir süre mevcut değil ise kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır.

5.1.1. Saklamayı Gerektiren Hukuki Sebepler

Şirkette, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süreler kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- *6698 sayılı Kişisel Verilerin Korunması Kanunu,*
- *6098 sayılı Türk Borçlar Kanunu,*
- *6100 sayılı Hukuk Muhakemeleri 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,*
- *5237 sayılı Türk Ceza Kanunu,*
- *5271 sayılı Ceza Muhakemesi Kanunu,*
- *6331 sayılı İş Sağlığı ve Güvenliği Kanunu,*
- *4857 sayılı İş Kanunu,*
- *6102 sayılı Türk Ticaret Kanunu,*
- *6502 sayılı Tüketicinin Korunması Hakkında Kanun,*
- *Mesafeli Satış Sözleşmelerine Dair Yönetmelik,*
- *213 sayılı Vergi Usul Kanunu,*
- *193 sayılı Gelir Vergisi Kanunu,*
- *5520 sayılı Kurumlar Vergisi Kanunu,*
- *3065 sayılı Katma Değer Vergisi Kanunu,*
- *4760 sayılı Özel Tüketim Vergisi Kanunu,*
- *488 sayılı Damga Vergisi Kanunu,*
- *6802 sayılı Gider Vergileri Kanunu,*
- *İlgili yasal mevzuat ve bu düzenlemeler uyarınca yürürlükte olan diğer ikincil düzenlemeler*

Çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

5.1.2. Saklamayı Gerektiren İşleme Amaçları

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

- *Çalışanın niteliğinin, tecrübesinin ve ilgisinin açık pozisyona uygunluğunu değerlendirmek,*
- *İşe alım sürecini tamamlamak,*
- *Gerektiği takdirde, Çalışanın ilettiği bilgilerin doğruluğunun kontrolünü yapmak veya üçüncü kişilerle iletişime geçip çalışan hakkında araştırma yapmak,*
- *Başvuru ve işe alım süreci hakkında Çalışan ile iletişime geçmek veya uygun olduğu takdirde, sonradan açılan herhangi bir pozisyon için Çalışan ile iletişime geçmek,*
- *Herhangi bir mevzuatın gereklerini ya da yetkili kurum veya kuruluşun taleplerini karşılamak,*
- *İSKO genelinde personel temin süreçlerini geliştirmek ve iyileştirmek,*
- *İş sözleşmelerinin ifasının ve yürütülmesinin yerine getirilmesi, (Özellikle; Çalışanların izin onayı, bakiye izinlerin görüntülenmesi, izin düzenlemelerinin yapılması, Çalışanların işten çıkış işlemlerinin yapılması, Bordro işlemlerinin yapılmasının sağlanması, Çalışanlara maaş ödemelerinin yapılması)*
- *İş Kanunu, İş Sağlığı ve Güvenliği Kanunu, Sosyal Güvenlik Kanunu ve ilgili mevzuat ile, diğer kanunlar ve mevzuat kapsamında gerekliliklerin yerine getirilmesi (Özellikle; Personel özlük dosyasının oluşturulması, SGK bildirimleri, İŞKUR bildirimleri, karakol bildirimi ile teşvik ve yasal yükümlülük bilgilendirmesinin yapılması, zorunlu bireysel emeklilik sigortası hesabı açılmasının sağlanması, Ar-Ge için teşvik hesaplaması yapılması, İcra dosyalarına çalışanların maaş haciz kesintilerine ilişkin ödeme yapılması, İş kazasının yasal bildirimlerinin yapılması, İş sağlığı ve güvenliği işlemlerinin yapılması, Mevzuat, ilgili düzenleyici kurumlar ve diğer otoritelerce öngörülen diğer bilgi saklama, raporlama, bilgilendirme yükümlülüklerine uymak, Mahkeme kararlarının yerine getirilmesi)*
- *Şirket içerisinde güvenliğin sağlanması*
- *Yurtiçi/yurtdışı eğitim, görevlendirme, denetim ve benzeri iş gereklerinin yerine getirilmesi,*
- *Ticari faaliyetlerin ve şirket operasyonların yürütülmesi ve geliştirilmesi,*
- *İş ortakları, bayiler veya tedarikçilerle yürütülen işlerin icrası ve ilişkilerin yönetimi,*
- *İletişim sağlanması,*
- *Kendisine araç tahsis edilen veya kullandırılan çalışanın araba kullanmaya ehil olduğunun, ehliyetini herhangi bir nedenle kaybetmediğinin teyit edilmesi*
- *Çalışana araç tedarik edilmesi ve park yeri ayarlanmasının sağlanması*
- *Kartvizit basımının sağlanması*
- *Kargo ve kurye aracılığıyla gelen paketlerin ilgili çalışana iletilmesinin sağlanması*
- *Çalışanların güvenliği ve işin yürütülmesi için Şirket aracı kullanımının takip edilmesi*
- *Servis ve seyahat organizasyonunun sağlanması*
- *Outlook'a çalışan verilerinin girilerek çalışanın iş e-postasının oluşturulması*
- *Çalışanlarla ilgili araştırma projeleri yürütülmesi*
- *Çalışanların işe giriş ve çıkışlarının kontrolünün sağlanması*
- *Şirket içi yazışma ve tekliflerinin yapılabilmesi için toplu elektronik posta yönetiminin sağlanması*
- *Çalışanların işe başvuru ve mülakatı süresince toplanan belgelerinin kayıt altına alınması*
- *Kutlama amaçlı iletişimin sağlanması*

- *Eğitim planlamasının yapılması, eğitimlerin raporlaması, eğitim sertifikalarının hazırlanması, gerçekleşen eğitimlere katılan çalışanların takip edilebilmesi, çalışanların aldıkları eğitimler sonucu gelişim süreçlerinin takip edilebilmesi*
- *Kalite kontrolün sağlanması,*
- *Acil durum yönetimi ve ilgili kişilerle iletişim sağlanması,*
- *Şirket çalışanlarına destek verilmesi,*
- *Memnuniyet anketi analizi yapılması,*
- *Müşteri şikayetlerinde müşterinin haklı/haksız ayrımının yapılması, müşteri memnuniyetinin arttırılması, müşteri ihtiyacının anlaşılması ve müşteri ile ilişkili süreçlerin iyileştirilmesinin sağlanması*
- *Müşteriye hizmet kalitesinin değerlendirilmesi ve çalışanlara eğitim verilmesi*
- *Kanunlara ve kişilerin temel hak ve özgürlükleri ve kişisel menfaatlerine aykırı olmayacak şekilde; Şirketin meşru menfaatleri doğrultusunda kullanımı,*
- *İSKO 'nun, topluluk şirketlerinin iş ortaklarının, tedarikçilerinin ve iş ilişkisi içerisinde olunan gerçek kişilerin ticari ve hukuki emniyetinin sağlanması*
- *Sözleşmelerin kurulması ve ifası,*
- *Ürün ve hizmetlerin alınması ve teslim edilmesi,*
- *Ürün veya hizmetlerin güvenilir ve kesintisiz bir şekilde temin edilmesi,*
- *Şirketin ürün ve hizmetlerinin etkinliğinin artırılması,*
- *Ticari faaliyetlerin ve operasyonların yürütülmesi ve geliştirilmesi,*
- *İnternet üzerinden satış ile ilgili üyelik, sipariş, ödeme işlemlerinin gerçekleştirilmesi, lojistik destek ile ürün gönderiminin sağlanması ve bunlarla ilgili iletişim kurulması,*
- *Müşterilerin fırsatlardan, kampanyalardan ve sair hizmetlerden haberdar edilmesi,*
- *Satış ve hizmet sonrası müşteri destek hizmetlerinin, müşteri memnuniyetinin, kurumsal iletişim faaliyetlerinin, müşteri ilişkileri ile müşteri talep ve şikayetlerinin yönetimi süreçlerinin planlanması ve yürütülmesi,*
- *Finans veya muhasebe işlemlerinin yerine getirilmesi ve takibi,*
- *Stratejik planlama ve bilgi güvenliği süreçlerinin planlanması, denetimi ve icrası,*
- *İş ortakları, bayiler veya tedarikçilerle yürütülen işlerin icrası ve ilişkilerin yönetimi,*
- *İSKO 'nun, topluluk şirketlerinin iş ortaklarının, tedarikçilerinin ve iş ilişkisi içerisinde olunan gerçek kişilerin ticari ve hukuki emniyetinin sağlanması*
- *Hukuki sorumlulukların yerine getirilebilmesi,*
- *İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.*

5.2. 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 kişinin açık rızasını geri alması,
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- Şirketin, ilgili 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,

Durumlarında, Şirket tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

6. TEKNİK VE İDARİ TEDBİRLER

İSKO, Kanun'un 12. maddesine uygun olarak, kişisel verilerin hukuka aykırı olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerde meydana gelebilecek güvenlik eksikliklerini önlemek için, korunacak verinin niteliğine göre gerekli gizlilik ve güvenlik tedbirlerini almaktadır. Bu kapsamda Şirket, Kişisel Verileri Koruma Kurulu ("Kurul") tarafından yayımlanmış olan rehberlere ve Kararlara uygun olarak gerekli güvenlik düzeyini sağlamaya yönelik ve idari tedbirleri almakta, denetimleri yapmakta veya yaptırmakta, kişisel verilerin hukuka aykırı yollarla ele geçirilmesi halinde yasal düzenlemelerde öngörülen tedbirlere uygun hareket etmektedir.

6.1. İdari Tedbirler

Kişisel verilerin gizliliğinin ve güvenliğinin sağlanması için İSKO, verilerin niteliklerine göre aşağıda gösterilen idari tedbirleri almaktadır;

- Kişisel veri envanteri hazırlanması
- Yürütülen kişisel veri işleme faaliyetleri detaylı olarak incelenerek KVK Kanunu'nda öngörülen kişisel veri işleme şartlarına uygunluğun sağlanması için atılması gereken adımların tespit edilmesi,
- Yasal mevzuata uyum kapsamında iç politikalar düzenlenmesi,
- Kişisel verilerin korunması hakkındaki mevzuata ilişkin olarak çalışanlarını eğitilmesi ve bilinçlendirilmesi,
- Kişisel verilerin aktarıma konu olduğu durumlarda, İSKO tarafından kişisel verilerin aktarıldığı kişiler ile akdedilmiş olan sözleşmelere, kişisel verilerin aktarıldığı tarafın veri güvenliğini sağlamaya yönelik yükümlülükleri yerine getireceğine ilişkin kayıtlar eklenmesi,
- Gizlilik sözleşmeleri yapılması,
- Şirket için periyodik ve rastgele denetimler gerçekleştirilmesi,
- Risk analizleri yapılması,
- İş sözleşmelerine kanuna uygun ilgili hükümler eklenmesi,
- Veri Sorumluları Sicili'ne (VERBİS) bildirim yapılması.
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
- Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması

6.2. Teknik Tedbirler

İSKO tarafından kişisel verilerin gizlilik ve güvenliğinin sağlanmasına ilişkin olarak, imkanlar dahilinde aşağıda gösterilen teknik tedbirler alınmaktadır;

- Teknolojik önlemler alınması ve alınan önlemler gelişmelere paralel olarak güncellenmesi ve iyileştirilmesi,

- Teknik konularda, uzman personel istihdam edilmesi ve uzman iş ortaklarından hizmet alınması,
- Alınan önlemlerin uygulanmasına yönelik düzenli aralıklarla denetim yapılması
- Güvenliği temin edecek yazılım ve sistemler kurulması,
- İSKO bünyesinde işlenmekte olan kişisel verilere erişim yetkisi, belirlenen işleme amacı doğrultusunda ilgili çalışanlar ile sınırlandırılması, yetki matrisi kurulması,
- Erişim logları kaydının yapılması,
- Ağ güvenliği ve uygulama güvenliği sağlanması,
- Yedekleme yapılması,
- Güncel Anti-Virüs sistemleri kullanılması,
- Silme, Yok Etme ve Anonim Hale Getirme işlemlerinin yapılması,
- Anahtar yönetimi yapılması,
- Saldırı tespit ve önleme sistemleri kullanılması,
- Kamera, kilit ve sair fiziksel güvenlik önlemleri alınması,
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmesi, gizlilik sözleşmeleri yapılması, verilere erişim yetkisine sahip kullanıcıların yetkilerinin tanımlanması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınması, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışların engellenmesi,
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. 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.

6.3. Kişisel Verilerin Hukuka Aykırı Yollarla Ele Geçirilmesi Halinde Tedbirler

İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, İSKO bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurulu'na bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir

7. 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.

7.1. Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda gösterilen yöntemlerle silinir;

Veri Kayıt Ortamı	Açıklama
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, veritabanı 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 Yer Alan 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 Verilerin Yok Edilmesi

Kişisel veriler aşağıda gösterilen yöntemlerle silinir;

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.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

7.3. 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 ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmesi kapsamında; kişisel veriler, 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 getirilir.

8. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından, faaliyetleri 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 Kişisel Veri Saklama ve İmha Politikasında

Yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Şirket tarafından güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Kişisel Verileri Koruma Birimi tarafından yerine getirilir.

Şirketin kişisel veri işleme süreçleri bazında saklama ve imha süreleri aşağıda gösterilmektedir:

Süreç	Saklama Süresi	İmha Süresi
Bilişim Sistemlerinin Bakım ve Onarım Faaliyetleri	1 hafta	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Aday Havuzu Oluşturma	İşe başvuru tarihinden itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Özlük Dosyası Oluşturma	İşten ayrılış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Yemek Masraflarının Takip ve Denetimi	1 yıl	Saklama süresinin bitimi tarihinde
Giriş Parmak izi	İşten ayrılış tarihinden itibaren 1 ay	Saklama süresinin bitimi tarihinde
Şirket İş Aracı (Tablet) Konum Takibi ve Denetimi	İşten ayrılış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İşe Giriş Çıkış Takibi ve Denetimi	İşten ayrılış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışanların Takip ve Denetimi	İşten ayrılış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İçerisinde Gerçek Zamanlı Görüntü Kayıt Sistemi ile Fiziksel Mekan Güvenliği Temini	3 ay	Saklama süresinin bitimi tarihinde
Ziyaretçi ve Toplantı Kayıtlarının Oluşturulması ve Takibi	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İş kıyafetlerinin hazırlanması	İşten ayrılış tarihine dek	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mesafeli Ürün Satışı	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Ödemeleri	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Satış Sonrası Hizmetler	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarikçilere İlişkin Ödemelerin Gerçekleştirilmesi	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Ücret Ödemeleri	İşten ayrılış tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ürün / Hizmet Pazarlama Faaliyetleri	Ticari ilişki sona erdikten itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ürün / Hizmet Satış Faaliyetleri	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ürün / Hizmet Tedarik Faaliyetleri	Ticari ilişki sona erdikten itibaren 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

9. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirkette her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

10. YÜRÜRLÜĞÜ, GÜNCELLENMESİ VE YÜRÜRLÜKTEN KALDIRILMASI

Bu Politika dokümanı, İSKO Yönetim Kurulu tarafından onaylandığı andan itibaren yürürlüğe girer. İşbu Politika'nın yürürlükten kaldırılması hususu hariç olmak üzere Politika içerisinde yapılacak değişiklikler ve ne şekilde yürürlüğe konacağı konusunda da İSKO Yönetim Kurulu tarafından İSKO Yönetim Kurulu Başkanı'na yetki verilmiştir. Yönetim Kurulu Başkanı onayıyla işbu Politika içerisinde değişiklik yapılabilecek ve yürürlüğe konabilecektir. İşbu Politika her halde yılda bir kez gözden geçirilir ve varsa değişiklikler Yönetim Kurulu Başkanı onayına sunularak gerçekleştirilir.

Kişisel verilerin korunması ve işlenmesine ilişkin yürürlükte bulunan mevzuat ile İSKO Veri Saklama ve İmha Politikası arasında çelişki bulunması halinde, İSKO yürürlükte bulunan mevzuatın uygulama alanı bulacağını kabul etmektedir.

İSKO Veri Saklama ve İmha Politikası, İSKO internet sitesinde (www.iskogrup.com) yayınlanır. Bu şekilde ilgili kişilerin ve kişisel veri sahiplerinin erişimine açıktır.

İşbu Politika'nın yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Yönetim Kurulu kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre Şirket tarafından saklanır.