VATAN PLASTİK SAN. VE TİC. A.Ş.

KVKK

KİŞİSEL VERİ SAKLAMA
ve
İMHA POLİTİKASI

İçindekiler

1.GİRİŞ
1.1 Amaç

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), VATAN PLASTİK SAN.VE TİC.A.Ş. (“Şirket”) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Ayrıca bu Politikanın amacı, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’a (Kanun) dayalı olarak çıkarılmış bulunan ve 30224 sayılı ve 28.10.2017 tarihli Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in (Yönetmelik) 5. ve 6. maddeleri gereğince; kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik’te belirtilen sair yükümlülüklerin yerine getirilmesi için uygulanacak kuralları belirlemektir.

Şirket çalışanları, çalışan adayları, eğitmen, müşterilerimiz, potansiyel müşterilerimiz, hizmet sağlayıcıları, ziyaretçilere ("İlgili Kişi") ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”) ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin işlemler, Şirket tarafından bu doğrultuda hazırlanmış olan bu politikaya uygun olarak gerçekleştirilir.

1.2 Kapsam

İlgili 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.

1.3 Kısaltmalar ve Tanımlar

Şirket : VATAN PLASTİK SAN.VE TİC.A.Ş.

Politika : Kişisel Verileri Saklama ve İmha Politikası

VERBİS : Veri Sorumluları Sicil Bilgi Sistemi

Kanun : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

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 Sorumlusu : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.

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.

Kurul : Kişisel Verileri Koruma Kurulu.

Veri Kayıt Sistemi : Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

Kişisel Veri İşleme 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,

İlgili Kişi : Kişisel verisi işlenen gerçek kişiyi,

Veri İşleyen : Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

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 işlemini,

Açık Rıza : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı

İfade eder.

2.SORUMLULUK VE GÖREV DAĞILIMLARI

Şirketin tüm çalışanları, Politika kapsamında kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu ekiplere destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Kişisel veri saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Genel Müdür	Şirket yönetimi	• Çalışanların politikaya uygun hareket etmesinden sorumludur.
İnsan Kaynakları Departmanı	İnsan Kaynakları	• Politika'nın hazırlanması, takibi, ve güncellenmesinden sorumlu • Fiziksel ortamda yer alan kişisel verilerin imha sürecinin yönetimi
Bilgi Teknolojileri	Bilgi Teknolojileri	• Politika'nın uygulanmasında ihtiyaç duyulan teknik tedbirlerinalınmasından sorumludur. • Elektronik ortamda yer alan kişisel verilerin imha sürecinin yönetimi
İnsan Kaynakları Ekibi, Hukuk İşleri Ekibi, Bilgi Teknolojileri Ekibi,	Diğer Birimler	• Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

Şirket bünyesinde işbu politika ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi ile ilişkili diğer politikaları, prosedürleri ve formlarını yönetmek üzere, şirket üst yönetiminin kararı gereğince "Bilgi Güvenliği Komitesi" oluşturulmuştur. Bu komitenin görevleri ISO 27001 Bilgi Güvenliği Yönetim Sistemi içerisinde tanımlanmıştır.

3.KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda KVKK hükümleri, ilgili mevzuatlar ve uluslararası veri güvenliği hususları dikkate alınarak güvenli bir şekilde saklanmaktadır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Fiziksel Ortamlar

• Sunucular
  • Etki alanı,
  • Yedekleme sistemi,
  • E-posta sistemi,
  • Veritabanı,
  • Web uygulaması,
  • Dosya paylaşım
• Yazılımlar
  • Muhasebe yazılımları,
  • CRM Yazılımı
  • ERP Yazılımı
• Bilgi güvenliği Sistemleri
  • Güvenlik duvarı,
  • Saldırı tespit ve engelleme,
  • Günlük kayıt dosyası,
  • Antivirüs
• Kişisel bilgisayarlar
  • Masaüstü,
  • Dizüstü,
• Mobil cihazlar
  • Telefon,
• Optik diskler
• Çıkartılabilir bellekler
  • USB bellek,
  • Hafıza Kart
  • Harici Disk
• Yazıcı, tarayıcı, fotokopi makinesi
	• Birim Dolapları
	• Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)
	• Yazılı, basılı, görsel ortamlar
	• Arşiv

4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Şirket tarafından; ilgili kişilere ait kişisel veriler kanuna uygun olarak saklanır ve imha edilir. Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda yer verilmiştir.

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış,

Kanunun 4 üncü maddesinde işlenen kişisel verinin;

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uygun olması gerektiği belirtilmiştir.

Kanunun 5. ve 6. maddelerde ise kişisel verilerin işlenme şartları sayılmıştır.

Buna göre, Şirket faaliyetleri çerçevesinde işlenen kişisel veriler, KVKK ve diğer ilgili mevzuat hükümlerine göre uygun süre kadar saklanır.

4.1 Saklamayı Gerektiren Hukuki Sebepler

İlgili kişilere ait kişisel verileri saklamayı gerektiren sebepler;

- Ticari faaliyetlerin sürdürülebilmesi,
- Hukuki yükümlülüklerin yerine getirilebilmesi,
- Çalışan haklarının ve yan haklarının planlanması ve ifası ile
- Müşteriilişkilerinin yönetilebilmesi amacıyla
- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudandoğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanmasının zorunlu olması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi,
- İlgili kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından ilgili kişilerin açık rızasının bulunması

fiziki veya elektronik ortamlarda güvenli bir biçimde KVKK ve diğer ilgili mevzuatlarda belirtilen sınırlar çerçevesinde saklama süreleri kadar saklanmaktadır.

4.2 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,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.

- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- Çağrı merkezi süreçlerini yönetmek.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü

4.3 İmhayı Gerektiren Sebepler

Kişisel veriler;

- Kişisel verilerin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Kişisel verilerin 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 veri sorumlusu tarafından kabul edilmesi,
- Verim sorumlusunu, 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, veri sorumlusu 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. maddesindeki ilkeler çerçevesinde, Şirket tarafından teknik ve idari tedbirler alınır.

5.1 İdari Tedbirler

Şirket tarafından alınan idari tedbirler:

- Veri güvenliğine ilişkin çalışanların iş sözleşmelerine gizlilik maddeleri eklenmiştir.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak IK disiplin prosedürü hazırlanmıştır.
- Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik denetimler yapılır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetleri giderilir.
- Çalışanlara KVKK ile ilgili hususlarında içeren bilgi güvenliği eğitimleri verilmektedir.
- Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereğierişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.

5.2 Teknik Tedbirler

Şirket tarafından alınan teknik tedbirler:

- Sızma (Penetrasyon) testleri ile bilişim sistemlerine yönelik risk, tehdit ve zafiyetler ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Kurum, 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 Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- 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 alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- 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.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Kişisel veriler ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, 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
Sunucularda Yer Alan Kişisel Veriler	• Sunucularda yer alan kişisel veriler saklanmasını gerektiren süre sona erenler için; • Sistem yöneticisi tarafından dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Veri tabanlarında Yer Alan Kişisel Veriler	• Veri tabanlarında 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. • Veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi
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 flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi
Bulut Sisteminde Bulunan Kişisel Verileri	• Bulut sisteminde bulunan kişisel verilerin saklanmasını gerektiren süre sona erenler için • Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Şirket tarafından Tablo-4'te verilen yöntemlerle yok edilir.

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 için, kâğıt öğütücü cihazlarda 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.

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 ilişkilendirilemeyecek hale getirilmesi işlemidir.

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.

KVKK'nın 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

7. 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;

yer alır.

Saklama ve imha sürelerinin tespitinde aşağıda sırasıyla belirtilen ölçütlerden yararlanılmaktadır:

- Mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir.

- Söz konusu kişisel verinin saklanmasına ilişkin olarak mevzuatta öngörülen sürenin sona ermesi veya ilgili mevzuatta söz konusu verinin saklanmasına ilişkin olarak herhangi bir süre öngörülmemiş olması durumunda sırasıyla;
    - Kişisel veriler, KVKK'nın 6. maddesinde yer alan tanımlama baz alınarak, kişisel veriler ve özel nitelikli kişisel veriler olarak sınıflandırmaya tabi tutulur. Özel nitelikte olduğu tespit edilen tüm kişisel veriler imha edilir. Söz konusu verilerin imhasında uygulanacak yöntem verinin niteliği ve saklanmasının Şirketin nezdindeki önem derecesine göre belirlenir.
    - Verinin saklanmasının KVKK'nın 4. maddesinde belirtilen ilkelere uygunluğu örneğin; verinin saklanmasında Şirket'in meşru bir amacının olup olmadığı sorgulanır. Saklanmasının KVKK'nın 4. maddesinde yer alan ilkelere aykırılık teşkil edebileceği tespit edilen veriler silinir, yok edilir ya da anonim hale getirilir.
    - Verinin saklanmasının KVKK'nın 5. ve 6. maddelerinde öngörülmüş olan istisnalardan hangisi/hangileri kapsamında değerlendirilebileceği tespit edilir. Tespit edilen istisnalar çerçevesinde verilerin saklanması gereken makul süreler tespit edilir. Söz konusu sürelerin sona ermesi halinde veriler silinir, yok edilir ya da anonim hale getirilir.
    - Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Bilgi Teknolojileri Müdürü tarafından yerine getirilir.
    - Yönetmeliğin 11 inci maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir.

Süreç	Saklama Süresi	İmha Süresi
Kurumsal İletişim Faaliyetlerinin Planlanması ve İcrası	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesine müteakip 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İnsanKaynaklarıSüreçlerininYürütülmesi	Faaliyetinsonaermesinitakiben 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Lokasyon	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
KameraKayıtları	2 ay	Saklama süresinin bitimini takiben 180 gün içerisinde

Şirket'in ilgili kişisel veriyi kullanma amacı sona ermedi ise, ilgili mevzuat gereği ilgili kişisel veri için öngörülen saklama süresi tabloda yer alan sürelerden fazla ise veya ilgili konuya ilişkin dava zamanaşımı süresi kişisel yerinin tabloda yer alan sürelerden fazla saklanmasını gerektiriyorsa, yukarıdaki tabloda yer alan süreler uygulanmayabilecektir. Bu halde kullanım amacı, özel mevzuat

veya dava zamanaşımı süresinden hangisi daha sonra sona eriyor ise, o süre uygulama alanı bulacaktır.

8. POLİTİKA'NIN YAYINLANMASI, SAKLANMASI ve GÜNCELLENMESİ

Şirket işbu politika ile ortaya koymuş olduğu esasların şirket içerisinde uygulanmasını temin etmektedir. Kişisel verilerin korunması konusunda ortaya konulan işbu politika ile şirketin ISO 27001 Bilgi Güvenliği Yönetim Sistemi alanında yürüttüğü temel politikalar, prosedürler ve formaları ile de bağı kurularak, şirketin benzer amaçlarla farklı politika esaslarıyla işlettiği süreçler arasında uyumluluk da sağlanmaktadır.

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda saklanır. Basılı kâğıt nüshası da İnsan Kaynakları Müdürlüğü dosyasında tutulur.

Politika, ihtiyaç duyulduğunda veya en az yılda bir defa gözden geçirilir ve gerekli olan bölümler güncellenir.

Şirket tarafından hazırlanan işbu Politika……..tarihinde yürürlüğe girmiştir. Politika'da değişiklik olması durumunda, Politika'nın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir.

İşbu Politika'da yapılan değişiklikler aşağıdaki tabloda yer almaktadır.

Güncelleme Tarihi	Değişikliklerin Kapsamı