

**İSTANBUL TERBİYE BOYA SANAYİ VE TİCARET
ANONİM ŞİRKETİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

İÇİNDEKİLER

1. GİRİŞ	4
1.1 Giriş	4
1.2 Politikanın Amacı	4
1.3 Politikanın Kapsamı	4
1.4 Tanımlar.....	4
1.5 Veri Konusu Kişi Gruplarına İlişkin Tanımlar	7
1.6 Politikanın Yürürlüğü	7
2. SORUMLULUK VE GÖREV DAĞILIMI	9
3. KAYIT ORTAMLARI	10
4. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI	10
4.1 Kişisel Verileri Saklama Süreleri ve İmha Süreci	10
4.2 Kişisel Verilerin Saklanması Gerektiren Hukuki Sebepler	9
4.3 Kişisel Verilerin Saklanması Gerektiren İşleme Amaçları.....	11
4.4 Kişisel Verilerin İmha Edilmesini Gerektiren Sebepler	12
5. İDARİ VE TEKNİK TEDBİRLER.....	12
5.1 İdari Tedbirler.....	11
5.1.1 Kişisel Verilerin Korunması Hususunda Kurumsal Yönetimin Sağlanması Hata! Yer işareti tanımlanmamış.	
5.1.2 Departman Özelinde Kişisel Veri İşleme Faaliyetleri ile Risk ve Tehditlerin Belirlenmesi	11
5.1.3 Kişisel Veri İşleme Envanteri Oluşturulması	13
5.1.4 Eğitim ve Farkındalık Çalışmalarının Yürütülmesi	13
5.1.5 Gizlilik.....	14
5.1.6 Kişisel Veri Güvenliği Politikaları ve Prosedürlerinin Belirlenmesi	14
5.1.7 Kişisel Verilerin Mümkün Olduğunca Azaltılması.....	14
5.1.8 Erişim ve Yetkilendirme Süreçlerinin Belirlenmesi	14
5.1.9 Kişisel Verilerin Yetkisiz İfşası Durumunda Bilgilendirme	14
5.1.10 Denetim	14
5.2 Teknik Tedbirler	14
5.2.1 Elektronik Ortamların Güvenliğinin Sağlanması	12
5.2.2 Fiziksel Ortamların Güvenliğinin Sağlanması	15
5.2.3 Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı	15
5.2.4 Kişisel Veri Güvenliğinin Takibi	15
5.2.5 Kişisel Verilerin Yedeklenmesi.....	15
5.2.6 Bilişim Sistemlerine Erişimin Sınırlandırılması ve Kullanıcıların Yetkilendirmesi 16	
5.2.7 Özel Nitelikli Kişisel Verilerin Güvenliği İçin İlave Önlemlerin Alınması	16

6. Kişisel Verileri İmha Yöntemleri.....	16
6.1 Kişisel Verilerin Silinmesi.....	16
6.2 Kişisel Verilerin Yok Edilmesi.....	17
6.3 Kişisel Verilerin Anonim Hale Getirilmesi	17
7. Saklama ve İmha Süreleri	18
7.1 Saklama ve İmha Süreleri Tablosu	18
7.2 İlgili Kişinin Talep Etmesi Halinde İmha.....	20
8. Periyodik İmha Süresi	20
9. Politikanın Güncellenme Periyodu	20

1. GİRİŞ

1.1 Giriş

İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi (“**Şirket**”) Kişisel Verilerin korunması ve işlenmesinde başta Anayasa’nın 20. Maddesinde düzenlenen özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumaya azami önem atfeder. Bu çerçevede, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“**Kanun**”) ile 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“**Yönetmelik**”) uyarınca Kişisel Verilerin hukuka uygun olarak saklanması ve imha edilmesine özen gösterir ve bu konuda gerekli her türlü idari ve teknik tedbiri alır.

1.2 Politikann Amacı

Kişisel Verileri Saklama ve İmha Politikasının (“**Politika**”) amacı, Kanun’un ve Yönetmelik’in amacına uygun olarak kişisel verileri saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda Şirketimizin uyacağı usul ve esasları belirlemektir. Politikann amacı doğrultusunda, Şirketimiz tarafından gerçekleştirilen kişisel verilerin saklanması ve imhası faaliyetlerinde mevzuata tam uyumun sağlanması ve kişisel veri sahiplerinin özel hayatın gizliliği ve veri güvenliği hakkının etkin bir şekilde korunması hedeflenmektedir. Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirketimiz tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.3 Politikann Kapsamı

Bu Politika; gerçek kişi olmak kaydıyla *Çalışan Adaylarını, Çalışanlarını, Hissedar/Ortaklarını, Potansiyel Ürün veya Hizmet Alıcılarını, Tedarikçi Çalışanlarını, Tedarikçi Yetkililerini, Ürün veya Hizmet Alan Kişileri, Referans Kişilerini, Çalışan/Yetkili/Hissedar/Stajyerin Aile Bireylerini* kapsamakta olup bu belirtilen kişilere ait kişisel verileri kapsar.

Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlendiği Şirketimize ait olan ya da Şirketimiz tarafından yönetilen tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır. Verinin aşağıda belirtilen kapsamda “Kişisel Veri” kapsamında yer almaması veya Şirketimiz tarafından gerçekleştirilen kişisel veri işleme faaliyetinin yukarıda belirtilen yollarla olmaması halinde bu Politika uygulanmaz.

1.4 Tanımlar

Bu Politikann uygulanmasında kullanılan kavramlar aşağıda yer verilen anlamları ifade eder:

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

Anonim Hale Getirme	Kişisel Verinin, Kişisel Veri niteliğini kaybedecek ve bu durumun geri alınamayacak şekilde değiştirilmesidir. Ör: Maskeleyme, toplulaştırma, veri bozma vb. tekniklerle Kişisel Verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesidir.
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlardır.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlardır.
İlgili Kişi / Kişisel Veri Sahibi	Kişisel verisi işlenen gerçek kişiyi ifade eder.
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 kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini ifade eder.
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 ifade eder.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
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 işlemidir.
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 envanterdir.

KVK Kurulu	Kişisel Verilerin Korunması Kurulu'dur.
Özel Nitelikli Kişisel Veri	İrk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda bu politikada belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.
Veri İhlali Müdahale Planı	Şirket tarafından işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde (veri ihlali) Şirket nezdinde raporlama yapılacak kişi ve organlar ile Kanun kapsamında gerekli bildirimlerin yapılması ve veri ihlalinin olası sonuçlarının değerlendirilmesi hususundaki sorumluların belirlendiği plandır.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına Kişisel Veri işleyen gerçek ve tüzel kişidir.
Veri Kayıt Sistemi	Kişisel Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
Veri Sorumlusu	Kişisel Verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
Şirket/Şirketimiz	İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi

1.5 Veri Konusu Kişi Gruplarına İlişkin Tanımlar

Bu Politika'da yer alan veri konusu kişi grupları aşağıda verilen anlamları ifade eder:

Çalışan	Şirketimizde iş akdiyle çalışan tüm gerçek kişilerdir.
Çalışan Adayı	Şirketimize herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini şirketimizin incelemesine açmış olan gerçek kişilerdir.

Potansiyel Müşteri (Ürün/ Hizmet Alıcısı)	Ürün ve hizmetlerimize kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişilerdir.
Referans Kişisi	Çalışan Adayı/Çalışan veya diğer konularda kendisinden bilgi almak için iletişime geçilen kişilerdir.
Ürün veya Hizmet Alan Kişi/Müşteri	Şirketimizle herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirketimizin sunmuş olduğu ürün ve hizmetleri kullanan veya kullanmış olan gerçek kişilerdir.
Şirket Hissedarı/Ortağı	İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi hissedarı/ortağı olan kişilerdir.
Tedarikçi Yetkilisi	Bir ürün ya da hizmet sunmak amacıyla Şirketimize girdi, ham madde veya ürün sağlayan gerçek kişiler veya tüzel kişilerin yetkilileridir.
Tedarikçi Çalışanı	Bir ürün ya da hizmet sunmak amacıyla Şirketimize girdi, ham madde veya ürün sağlayan gerçek veya tüzel kişilerin kimliği belirli/belirlenebilir çalışanlarıdır.
Çalışan/Yetkili/ Hissedar/Stajyerin Aile Bireyleri	İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi 'nin Çalışan, Yetkili, Hissedar ve Stajyerlerinin aile bireyleridir.

1.6 Politikann Yürürlüğü

İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi tarafından düzenlenerek xx.xx.2022 tarihinde yürürlüğe giren **Politika**, talep üzerine ilgili kişilerin erişimine sunulur.

2. SORUMLULUK VE GÖREV DAĞILIMI

Şirketimizin 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 saklanmasıyla 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 saklanma ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki tabloda sunulmuştur:

Unvan	Birim	Görev
Yönetim Kurulu Başkanı	İstanbul Terbiye Boya Sanayi Ve Ticaret Anonim Şirketi	Çalışanların politikaya uygun hareket etmesinin sağlanması için gerekli çalışmaların yürütülmesinden sorumludur
Outsource	Hukuk	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi ve güncellenmesinden sorumludur.
Müdür	Muhasebe&İnsan Kaynakları	Politika'nın İK çalışmaları bakımından yürütülmesinden sorumludur.
Bilgi Teknolojileri Uzmanı	Bilgi Teknolojileri	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve ilgili ortamlarda yayınlanmasından sorumludur
Müdür	Muhasebe	Politika'nın uygulanmasının denetlenmesinden sorumludur
Yönetici/Müdür	Diğer birimler (Mali İşler, Muhasebe, Pazarlama, Satış, Satın Alma, Kalite Güvence vs.)	Görevlerine uygun olarak Politika'nın yürütülmesinden sorumludur

3. KAYIT ORTAMLARI

Şirketimiz kişisel verileri aşağıda listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklar:

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> ➤ Sunucular (Yedekleme, e-posta, veritabanı, intranet, dosya paylaşım vb.) ➤ Yazılımlar (ofis yazılımları, İK Yazılım, Bordro Yazılım, vb.) ➤ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ➤ Bilgisayarlar ➤ Optik diskler (CD, DVD vb.) 	<ul style="list-style-type: none"> ➤ Kâğıt ➤ Manuel veri kayıt sistemleri (personel bilgi formları, iş başvuru formları, anket formları, AGİ dosyaları, avans talep formları vb.) ➤ Yazılı, basılı, görsel ortamlar

<ul style="list-style-type: none">➤ Çıkarılabilir bellekler (USB, hafıza kartı vb.)➤ Mobil cihazlar (telefon, tablet vb.)➤ Yazıcı, tarayıcı, fotokopi makinası, parmak izi okuyucu vb. çevre birimler	
---	--

4. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

4.1 Kişisel Verileri Saklama Süreleri ve İmha Süreci

Şirketimiz kişisel verileri Kanun'un 4. maddesi uyarınca ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklar.

Şirketimiz Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin tamamının ortadan kalkması hâlinde, kişisel verileri Kanunun 7. maddesi uyarınca resen veya ilgili kişinin talebi üzerine siler, yok eder veya anonim hâle getirir.

4.2 Kişisel Verilerin Saklanması Gerektiren Hukuki Sebepler

Şirketimiz, faaliyetleri çerçevesinde işlediği kişisel verileri ilgili mevzuatta öngörülen bir saklama süresi bulunuyorsa öngörülen bu süre kadar muhafaza eder. Bu kapsamda Şirketimiz kişisel verileri aşağıdaki kanunlar ve bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklamaktadır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 213 sayılı Vergi Usul Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret 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

Şirketimiz tarafından işlenen kişisel veriler için mevzuatta öngörülen bir saklama süresi bulunmuyorsa, bu durumda kişisel veriler işlendikleri amaç için gerekli süre kadar saklanmaktadır.

4.3 Kişisel Verilerin Saklanması Gerektiren İşleme Amaçları

Şirketimiz, faaliyetleri çerçevesinde işlediği kişisel verileri aşağıdaki amaçlar doğrultusunda saklar:

- Bilgi Güvenliği Süreçlerinin Yürütülmesi
- Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
- Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
- Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi

- Erişim Yetkilerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi
- Finans Ve Muhasebe İşlerinin Yürütülmesi
- Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
- 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 Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
- İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- Lojistik Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
- Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
- Sözleşme Süreçlerinin Yürütülmesi
- Talep / Şikayetlerin Takibi
- Taşınır Mal Ve Kaynakların Güvenliğinin Temini
- Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
- Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
- Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- Yönetim Faaliyetlerinin Yürütülmesi
- Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

4.4 Kişisel Verilerin İmha Edilmesini Gerektiren Sebepler

Şirketimiz kişisel verileri aşağıdaki durumlarda ilgili kişinin talebi üzerine ya da re'sen siler, yok eder veya anonim hale getirir:

- 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. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirketimiz tarafından kabul edilmesi,
- Şirketimizin; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, başvuruya verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde ilgili kişi tarafından Kurula şikâyette bulunulması 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.

5. İDARİ VE TEKNİK TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, kişisel verilerin hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi amacıyla Kanunun 12. maddesi ile 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Şirketimiz tarafından teknik ve idari tedbirler alınır.

Şirketimiz tarafından alınan idari ve teknik tedbirler aşağıda açıklanmıştır:

5.1 İdari Tedbirler

5.1.1 Departman Özelinde Kişisel Veri İşleme Faaliyetleri ile Risk ve Tehditlerin Belirlenmesi

Şirketimiz tarafından yürütülen tüm kişisel veri işleme faaliyetleri departmanlar özelinde analiz edilir. Bu kapsamda öncelikle kişisel verilerin güvenliğine ilişkin ortaya çıkabilecek risk ve tehditler belirlenir. Risk ve tehditler belirlenirken kişisel verilerin özel nitelikli olup olmadığını, mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiğini ve güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ile niceliğini dikkate alınır.

5.1.2 Kişisel Veri İşleme Envanteri Oluşturulması

Şirketimizdeki iş süreçlerine bağlı olarak gerçekleştirilen kişisel veri işleme faaliyetlerinin ayrıntılandırıldığı bir kişisel veri işleme envanteri oluşturulmuştur. Kişisel veri işleme faaliyetlerinin Kanuna uygun şekilde gerçekleştirilmesini teminen aydınlatma yükümlülüğü başta olmak üzere gerekli yükümlülükler bu envanter esas alınarak her departman ve yürütmüş olduğu faaliyet özelinde belirlenir ve yerine getirilir.

5.1.3 Eğitim ve Farkındalık Çalışmalarının Yürütülmesi

Çalışanlar kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesinin ve erişilmesinin önlenmesi konularında bilgilendirilir.

Kişisel veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi hâlinde; düzenlenen yeni eğitimlerle bu değişiklikler çalışanların bilgisine sunulur ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerin güncel tutulması sağlanır.

5.1.4 Gizlilik

Çalışanların, işledikleri kişisel verileri hukuka aykırı olarak başkalarına açıklamaları ve işleme amacı dışında kullanmamaları için gerekli idari tedbirler alınır. Bu kapsamda, çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik sözleşmeleri imzalatılır.

Çalışanlar tarafından imzalanan sözleşme ve belgelere; edindikleri kişisel verileri Kanun hükümlerine aykırı olarak işlememe, ifşa etmeme ve kullanmama yükümlülüğü getiren kayıtlar koyulur. Bu yükümlülerin görevden ayrılmalarından sonra da devam edeceği konusunda çalışanlar bilgilendirilir ve bu doğrultuda gerekli taahhütler alınır.

Kişisel verilerin hukuka uygun olarak aktarıldığı gerçek ve tüzel kişiler ile akdedilen sözleşmelere, kişisel verilerin korunması için gerekli güvenlik tedbirlerinin alınmasına ilişkin hükümler eklenir.

5.1.5 Kişisel Veri Güvenliği Politikaları ve Prosedürlerinin Belirlenmesi

Kişisel veri güvenliğine ilişkin risklerin önceden belirlenmesini ve istikrarlı şekilde önlem alınmasını teminen Kişisel Veri Güvenliği Politikaları ve Prosedürleri belirlenir. Politika ve prosedürlerin yürürlüğünün sağlanmasından Veri Koruma Grubu sorumludur. Bu kapsamda Komite tarafından düzenli kontroller yapılır, geliştirilmesi gereken hususlar belirlenerek güncellemeler gerçekleştirilir.

Kişisel veri güvenliğine ilişkin politika ve prosedürlere uymayan çalışanlara yönelik uygulanacak disiplin süreci bulunmaktadır.

5.1.6 Kişisel Verilerin Mümkün Olduğunca Azaltılması

Şirketimiz tarafından saklanan kişisel verilerin doğru ve güncel olmasına ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesine özen gösterilir. Bu kapsamda, kayıt ortamlarında tutulan kişisel verilerin işleme amaçları bakımından saklanma durumu periyodik olarak değerlendirilir ve saklanma süresi sona eren kişisel veriler Yönetmelik'e uygun şekilde imha edilir.

5.1.7 Erişim ve Yetkilendirme Süreçlerinin Belirlenmesi

Kanuna uyumluluk amacına uygun olarak kişisel verilere erişim ve yetkilendirme süreçleri departmanlar özelinde tasarlanır ve uygulanır.

5.1.8 Kişisel Verilerin Yetkisiz İfşası Durumunda Bilgilendirme

Şirketimiz tarafından işlenen kişisel verilerin Kanuna uygun olmayan yollarla başkaları tarafından elde edilmesi halinde, Veri İhlali Müdahale Planı çerçevesinde gerekli önlemler alınır ve Komite aracılığıyla bu durum en geç 72 saat içinde KVK Kuruluna bildirilir. İhlalden etkilenen İlgili Kişiler belirlenerek makul olan en kısa süre ve en geç 72 saat içerisinde bu kişiler bilgilendirilir.

5.1.9 Denetim

Kişisel verilerin güvenliğine ilişkin idari ve teknik tedbirlerin yeterliliğini ve devamlılığını sağlamak amacıyla veri koruma grubunun gözetiminde periyodik ve rastgele denetimler yapılır ve yaptırılır, gerektiğinde bu tedbirler güncellenir.

5.2 Teknik Tedbirler

5.2.1 Elektronik Ortamların Güvenliğinin Sağlanması

Kişisel verilerin güvenliğinin sağlanmasını teminen kişisel veri içeren bilişim sistemlerinde erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemleri kullanılır. Güçlü şifre ve parola kullanımı ile söz konusu şifre ve parolaların düzenli aralıklarla değiştirilmesi temin edilir.

Yazılım ve donanımların düzgün şekilde çalışması ve güvenlik açıklarının kapatılması için yama yönetimi ve yazılım güncellemeleri düzenli olarak gerçekleştirilir. Zararlı yazılımları engelleyen sistemler kullanılır.

İnternet üzerinden gelen izinsiz erişim tehditlerine karşı güvenlik duvarı ve ağ geçidi tedbirleri uygulanır. Farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel

veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi temin edilir. Şirket internet sayfasının erişiminde güvenli protokol (HTTPS) kullanılır.

5.2.2 Fiziksel Ortamların Güvenliğinin Sağlanması

Şirketimiz bina ve yerleşkelerinde bulunan cihazlarda ve kâğıt ortamında saklanan kişisel verilerin gerek çalınma, kaybolma vb. risklere karşı gerek yangın, sel vb. çevresel tehditlere karşı uygun yöntemlerle korunması için gerekli önlemler alınır.

5.2.3 Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı

Kişisel verilerin güvenli ortamlarda saklanmasını teminen teknolojik gelişmelere uygun sistemler kullanılır. Yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri dikkate alınır.

Cihazların bakım ve onarımı için üretici, satıcı, servis gibi üçüncü kurumlardan hizmet alındığında bu cihazlarda bulunan kişisel verilerin korunması için gerekli önlemler alınır. Kişisel veri içeren cihazların bakım ve onarım işlemi için Şirket dışına çıkarılması gerekiyorsa cihazlardaki veri saklama ortamı sökülerek saklanır ve sadece arızalı parçalar gönderilir. Bakım ve onarım gibi amaçlarla dışarıdan gelen personelin kişisel verilere erişimini ve/veya verileri kopyalamasını engellemek için de gerekli önlemler alınır.

5.2.4 Kişisel Veri Güvenliğinin Takibi

Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenir, sızma veya prosedürlere aykırı bir hareket olup olmadığı takip edilir.

Tüm kullanıcıların işlem hareketlerinin kaydı (Log kayıtları, kapı giriş çıkış kayıtları vb.) düzenli olarak tutulur.

Sızma (Penetrasyon) testleriyle risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınır.

5.2.5 Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, çalınması, kaybolması veya erişilemez hale gelmesi gibi durumlara karşı veri güvenliğinin sağlanmasını teminen veri yedekleme stratejileri geliştirilir.

Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılır. Yedeklenen kişisel verilere sadece sistem yöneticisi tarafından erişilir ve veri seti yedekleri gerekli güvenlik önlemleri alınmak suretiyle ağ dışında tutulur.

5.2.6 Bilişim Sistemlerine Erişimin Sınırlandırılması ve Kullanıcıların Yetkilendirilmesi

Kanuna uyumluluk amacına uygun olarak kişisel verilere erişim ve yetkilendirme süreçlerinde departman özelinde donanımsal ve yazılımsal önlemler alınarak kişisel veri içeren sistemlere erişim sınırlandırılır. Bu çerçevede, kişisel verilere erişim “erişim yetki ve kontrol matrisi” oluşturularak çalışanların iş tanımları ile yetki ve sorumluluklarına göre belirlenir. İlgili sistemlere kullanıcı adı ve şifre kullanılarak erişilmesi sağlanır ve anahtar yönetimi prosedürleri uygulanır. İş akdi sona eren çalışanların verilere erişim izni gecikmeksizin kaldırılır.

5.2.7 Özel Nitelikli Kişisel Verilerin Güvenliği İçin İlave Önlemlerin Alınması

Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika ve prosedür hazırlanmıştır. Bu kapsamda özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik eğitimler düzenlenir, gizlilik sözleşmeleri yapılır ve verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanır. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ve fiziksel ortamlarda yeterli güvenlik önlemleri alınır ve verilerin aktarımında ilave tedbirler uygulanır. Tüm bu hususlar “Özel Nitelikli Kişisel Verilerin Güvenliği Politikası” ve “Özel Nitelikli Kişisel Verilerin Güvenliği Prosedürü”nde ayrıntılı şekilde düzenlenmektedir.

6. Kişisel Verileri İmha Yöntemleri

Şirketimiz ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel verileri, resen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen yöntemlerle imha eder. Şirketimiz ilgili kişinin talebi halinde kişisel verilerin imhası için uygun yöntemi gerekçesini açıklayarak seçer.

6.1 Kişisel Verilerin Silinmesi

Kişisel veriler aşağıdaki tabloda sunulan 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, 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 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.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler aşağıdaki tabloda sunulan yöntemlerle yok edilir:

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makinelerinde geri döndürülemez 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 değerlerde manyetik alana maruz bırakılması suretiyle veya üzerine yazma (optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılması) yöntemi kullanılarak 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 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. Şirketimiz kişisel verileri anonim hale getirirken maskeleyme, değişken çıkartma, genelleştirme yöntemleri kullanır.

Maskeleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemlerdir.

Değişken çıkartma: Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir.

Genelleştirme: Kişisel veriyi özel bir değerden daha genel bir değere çevirerek ilgili veriyi gerçek bir kişiye erişmeyi imkânsız hale getirecek şekilde bir gruba ait toplam değerleri veya istatistikleri gösterir hale getirme işlemidir.

7. Saklama ve İmha Süreleri

Şirketimizin, faaliyetleri çerçevesinde işlediği 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 kayıta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

yer almaktadır.

Şirketimiz kişisel verileri imha etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir. Söz konusu imha işlemi Komite tarafından görevlendirilen birimler tarafından yerine getirilir.

Kişisel verilerin imha edilmesiyle ilgili yapılan bütün işlemler Şirketimiz tarafından kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere üç yıl süreyle saklanır.

7.1 Saklama ve İmha Süreleri Tablosu

İş Süreci	Veri Kategorisi	İmha Süresi
Personel Temin Süreçleri	Başvurunun alınmasını takiben 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
İnsan Kaynakları Süreçleri	İş ilişkisinin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
İş Sağlığı ve Güvenliği Süreçleri(sağlık belgeleri dahil)	İş ilişkisinin sona ermesini takiben 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Yönetim Süreçleri	İş ilişkisinin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Mali Süreçler	İş ilişkisinin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Sözleşme Süreçleri	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde

Mal/Hizmet Satış ve Satın Alım Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Donanım ve Yazılıma Erişim Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Log Kayıt Takip Süreçleri	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
İnternet Sitesi Kayıt Takip Süreçleri	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Adli Süreçler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde
Kurumsal İletişim Süreçleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha işleminde

7.2 İlgili Kişinin Talep Etmesi Halinde İmha

Veri sahipleri Şirketimize başvurarak kendisine ait kişisel verilerin imha edilmesini talep edebilir.

Bu durumda Şirketimiz başvuranın kişisel verilerine ilişkin işleme şartlarının mevcut durumunu kontrol eder ve kişisel veri işleme şartlarının tamamı ortadan kalkmışsa talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirketimiz bu işlemi en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa bu durumu üçüncü kişiye bildirir.

Şirketimiz kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa ilgili veri sahibinin talebini, gerekçesini açıklayarak reddedebilir. Bu durumda ret cevabını ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

Şirketimize iletilen talebin ayrıca bir maliyeti gerektirmesi hâlinde, ilgili kişiden Kurulca belirlenen tarifedeki ücret alınabilir. Başvuru Şirketimizin hatasından kaynaklanmışsa alınan ücret ilgiliye iade edilir.

8. Periyodik İmha Süresi

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

9. Politikanın Gncellenme Periyodu

Ŗirketimiz, Politika'yı ihtiya duyulduka gzden geirir ve gerekli olan blmleri gnceller.