**TEKNİK BAĞLANTI ELEMANLARI SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

1. BÖLÜM: İMHA POLİTİKASI'NIN NİTELİĞİ VE AMACI

1.1. GİRİŞ

İşbu imha politikası Teknik Bağlantı Elemanları San. ve Tic. A.Ş.kısaca (“Şirket”) olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve sair mevzuatı uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin “Teknik Bağlantı Elemanları San. ve Tic. A.Ş” tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, çalışanlarımızın, müşterilerimizin, tedarikçilerimizin ve herhangi bir nedenle Şirket nezdinde kişisel verisi bulunan tüm gerçek kişilerin verileri, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yönetilmektedir.

1.2. TANIMLAR

|  |  |  |
| --- | --- | --- |
| **Alıcı grubu** | **:** | Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini, |
| **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 kişileri, |
| **Veri sorumlusu** | **:** | Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, |
| **İlgili kişi** | **:** | Kişisel verisi işlenen gerçek kişiyi, |
| **İmha** | **:** | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini, |
| **Kanun** | **:** | 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu, |
| **Yönetmelik** | **:** | 28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği |
| **Kurul** | **:** | Kişisel Verileri Koruma Kurulunu |
| **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, |
| **Kişisel veri saklama ve imha politikası:** | **:** | Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı, |
| **Veri kayıt sistemi** | **:** | Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini, |

ifade eder.

**2. BÖLÜM: ORTAMLAR VE GÜVENLİK TEDBİRLERİ**

2.1. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Şirket her halde veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri Kanun’a, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak işlemek ve korumaktadır.

|  |  |  |
| --- | --- | --- |
| a) Matbu ortamlar | **:** | Verilerin kâğıt üzerinde tutulduğu ortamlardır. |
| b) Yerel dijital ortamlar | **:** | Teknik Bağlantı A.Ş bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır. |

2.2. ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

Teknik Bağlantı A.Ş kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

2.2.1. Teknik Tedbirler

Şirket kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

* Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
* Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
* Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
* Çalışanlar için yetki matrisi oluşturulmuştur.
* Erişim logları düzenli olarak tutulmaktadır.
* Güncel anti-virüs sistemleri kullanılmaktadır.
* Güvenlik duvarları kullanılmaktadır.
* Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
* Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
* Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
* Saldırı tespit ve önleme sistemleri kullanılmaktadır.
* Şifreleme yapılmaktadır.

2.2.2. İdari Tedbirler

Şirket kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

* Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
* Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
* Kişisel veri işleme, saklama ve imha konularında politikalar hazırlanmaktadır.
* Gizlilik taahhütnameleri yapılmaktadır.
* Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
* İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
* Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
* Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
* Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
* Kişisel veriler mümkün olduğunca azaltılmaktadır.
* Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
* Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

2.2.3. Şirket İçi Denetim

Şirket, Kanun’un 12’nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da başka bir şekilde Şirket’in sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, Şirket bu durumu 72 saat içinde Kurula (KVK Kuruluna) ve en kısa sürede ilgilisine bildirir.

**3. BÖLÜM: KİŞİSEL VERİLERİN İMHASI**

3.1. SAKLAMA VE İMHA NEDENLERİ

3.1.1. Saklama Nedenleri

Şirket’in faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir.

Bu kapsamda kişisel veriler;

• 6698 sayılı Kişisel Verilerin Korunması Kanunu,

• 6098 sayılı Türk Borçlar Kanunu,

• 6102 sayılı Türk Ticaret Kanunu,

• 213 sayılı Vergi Usul 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,

* 4632 Sayılı Bireysel Emeklilik Kanunu

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

**3.1.2. İmhayı Gerektiren Nedenler**

Kişisel veriler;

* İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası (kaldırılması),
* İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
* Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
* KVK Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
* Şirket’in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, ilgili kişinin verilen cevabı yetersiz bulması veya Şirket’in Kanunda öngörülen süre içinde cevap vermemesi hallerinde; ilgili kişinin 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 silinir, yok edilir veya anonim hale getirilir.

3.2. İMHA YÖNTEMLERİ

Şirket, Kişisel Verilerin Korunması Kanunu ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde, ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde siler, yok eder veya anonim hale getirir.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

**3.2.1.1 Silme Yöntem​leri**

**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 Bulunan Kişisel Veriler:** Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, erişim yetkisi sadece sistem yöneticisine verilerek güvenli ortamlarda saklanır.

**3.2.1.2 Yok Etme Yöntemleri**

**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.

**3.2.1.3. Anonimleştirme Yöntemleri**

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi olsa hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle 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.

3.3. SAKLAMA VE İMHA SÜRELERİ

**3.3.1. Saklama Süreleri**

|  |  |  |
| --- | --- | --- |
| **VERİ SAHİBİ** | **VERİ KATEGORİSİ** | **VERİ SAKLAMA SÜRESİ** |
| Çalışanlar | Çalışanın iş akdinin kurulması ve mevzuattan kaynaklı yükümlülükler için alınan; kimlik, iletişim, finans, mesleki bilgi, görsel kayıt, özlük ve hukuki işlem verileri | İş akdinin devamı süresince ve iş akdinin sona ermesinden itibaren 10 yıl müddetle saklanmaktadır |
| Çalışanlar | İş sağlığı ve güvenliği mevzuatı dolayısıyla alınan; kişisel veriler ile sağlık verileri | İş akdinin devamı süresince ve iş akdinin sona ermesinden itibaren 15 yıl müddetle saklanmaktadır. |
| Çalışanlar | İş akdinin kurulabilmesi dolayısıyla alınan adli sicil kaydı verisi | İş akdinin devamı süresince ve iş akdinin sona ermesinden itibaren 10 yıl müddetle saklanmaktadır. |
| Çalışanlar | Personel devam kontrol sistemi dolayısıyla alınan, kart numarası | İşten ayrılma tarihinden itibaren 5 yıl süreyle saklanmaktadır. |
| Çalışanlar | Ürün kalite kontrol süreçlerinde alınan; kimlik, iletişim, mesleki bilgi verisi | Çalıştığı sürece saklanmaktadır. |
| Çalışanlar | Çalışanların servis araçlarında bulunan takip sistemi dolayısıyla alınan lokasyon verisi | 2 yıl süreyle saklanmaktadır. |
| Çalışanlar | Üretim sürecinin planlanması ve icra edilmesi sırasında alınan; kimlik ve özlük verileri | 10 yıl süreyle saklanmaktadır. |
| Çalışanlar | Bilgi güvenliği yönetimi ile yetkilendirme ve zimmet işlemleri için alınan; kimlik, iletişim, özlük ve işlem güvenliği verileri | Çalıştığı sürece ve işten ayrılma tarihinden itibaren 1 ay süreyle saklanmaktadır. |
| Çalışanlar | Üretim sürecinin takibi dolayısıyla alınan kamera kayıtları | 1 ay süreyle saklanmaktadır. |
| Çalışan Adayları | Çalışan adaylarının başvuru süreçleri esnasında alınan özgeçmiş verileri | 1 yıl süreyle saklanmaktadır. |
| Çalışan Adayları | Çalışan adaylarından alınan; adli sicil kaydı, sağlık bilgisi ve dernek üyeliği gibi özel nitelikli kişisel veriler | 1 yıl süreyle saklanmaktadır. |
| Hissedar, Yönetim Kurulu, İmza yetkilisi, Çalışan | Şirket yönetim süreçlerinde alınan; kimlik, iletişim, finans, özlük verileri | 10 yıl süreyle saklanmaktadır. |
| Hissedar | Şirketin yönetim işlemleri dolayısıyla işlenen risk yönetimi verileri | Süresiz saklanmaktadır. |
| Stajyer | Staj işlemleri dolayısıyla alınan; kimlik, iletişim, finans, görsel kayıt ve özlük verileri | Staj bitiminden itibaren 10 yıl süreyle saklanmaktadır. |
| Stajyer | Staj işlemleri dolayısıyla alınan; sağlık verisi | Staj bitiminden itibaren 10 yıl süreyle saklanmaktadır. |
| Tedarikçi | Mal/hizmet alım süreçlerinde işlenen; kimlik, iletişim, mesleki deneyim, finans, müşteri işlem verileri ile taşıma/ulaşım işlemlerinde alınan araç plakası | İşin devamı süresince ve iş bitiminden itibaren 10 yıl süreyle saklanmaktadır. |
| Müşteri | Ürünlerin satış, kalite kontrol, üretim ve teslim süreçlerinde alınan; kimlik, iletişim, mesleki deneyim ve müşteri işlem verileri | İş bitiminden itibaren 10 yıl süreyle saklanmaktadır. |
| Müşteri, tedarikçi, çalışan, çalışan adayı, çalışan yakını, diğer | İletişim faaliyetlerinin yürütülmesi esnasında alınan santral kayıtları; kimlik, iletişim ve firma unvanı gibi bilgiler | 1 gün süreyle saklanmaktadır. |
| Çalışan, çalışan adayı, hissedar, tedarikçi, stajyer, müşteri, ziyaretçi | Fiziksel mekân güvenliğinin sağlanması için alınan kamera kayıtları | 35 gün süreyle saklanır. |
| Ziyaretçi | Tesise giriş-çıkışların kontrol edilmesi amacıyla alınan; kimlik, iletişim, giriş-çıkış yaptığı saat ve araç plaka bilgisi | Ziyaretin tamamlanmasından sonra 6 ay süreyle saklanmaktadır. |

\* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

**3.3.2.   İmha Süreleri**

Şirket; Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanunun 13’ncü maddesine istinaden Teknik Bağlantı A.Ş’ye başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir.  Şirket’in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Şirket her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.
2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13’ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

3.4. PERİYODİK İMHA

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri her 6 (altı) ayda bir tekrar eder.

3.5. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

Şirket gerek talep üzerine gerekse periyodik imha süreçlerinde resen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Şirket imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

**3.5.1. Teknik Tedbirler**

* Şirket işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
* Şirket imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
* Şirket imha işlemi ile ilgili kayıtları tutar.
* Şirket imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

**3.5.2. İdari Tedbirler**

* Şirket, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
* Şirket, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
* Şirket, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
* Şirket, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
* Şirket, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere **en az üç yıl** süreyle saklar.

4. BÖLÜM POLİTİKA’NIN YAYIMLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da ………………………………….. dosyasında saklanır.

5. BÖLÜM POLİTİKA’NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

6.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Teknik Bağlantı A.Ş Yönetim Kurulu tarafından karar alınmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika’nın ıslak imzalı eski nüshaları Yönetimin Kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile saklanır.