



BOTAŞ INTERNATIONAL ANONİM ŞİRKETİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. POLİTİKANIN AMACI

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), BOTAŞ International Anonim Şirketi nezdinde (kısaca “BIL” ya da “Kurum”) gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır. Kurum; Kurum çalışanları, ziyaretçiler dahil tüm ilgili kişilere ait kişisel verilerin, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”), Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik, ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını amaçlamaktadır. Kişisel verilerin saklanması ve imhasına ilişkin tüm işlemler, Kurum tarafından bu doğrultuda hazırlanmış olan iş bu politikaya uygun olarak gerçekleştirilir.

2. KAPSAM

- BIL çalışanları
- Stajyer
- Tedarikçi çalışanı
- Tedarikçi
- Ziyaretçiler
- Hukuki uyuşmazlık yaşanan kişi
- Arsa malikleri
- Çalışan yakını

ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamında olup, Kurumun sahip olduğu ya da Kurum tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde iş bu Politika uygulanır.

3. TANIMLAR

Kısaltma	Tanım
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
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 getirilmesi.
Kanun/KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 bilgi.
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 işlem.
Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kurul	Kişisel Verileri Koruma Kurulu.
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	Kanun'da yer alan kişisel verilerin işleme 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.
VERBİS	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği veri kayıt sistemi.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	28 Ekim 2017 tarihinde Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

4. KAYIT ORTAMLARI

İlgili kişiye ait kişisel veriler, Kurum tarafından aşağıdaki tabloda listelenen ortamlarda başta Kanun hükümleri olmak üzere, ilgili mevzuata uygun olarak uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Kişisel Veri İşlenen Kurum Elektronik Ortamları:

- Yazışma Takip Sistemi
- Konaklama Yönetim Sistemi
- NCR (Uygunsuzluk Raporu)
- Seyahat Yönetim Sistemi
- Aksiyon Takip Sistemi
- Zimmet Takip Sistemi HSE (Sarf Malzemeler)
- Zimmet Takip Sistemi IMS
- Zimmet Takip Sistemi İdari İşler (Barkodlu)
- CMT Günlük Operasyon Sistem Takibi
- PT Günlük Operasyon Sistem Takibi
- İzin Yönetim Sistemi
- Kamu ve Halkla İlişkiler Sistemi
- Vardiya Yönetim Sistemi
- Hukuk Portalı
- Fazla Mesai Yönetim Sistemi
- BOSS/SOC Kart Sistemi
- Revir Uygulaması
- Atık Yönetim Sistemi
- ECO Kart Sistemi
- Olay Takip Sistemi
- IMS Hizmet Talep Uygulaması
- Anlık Tank Dolum Takip Sistemi (Sonora)
- ERP
- Documentum
- Mühendislik Veri Ambarı
- Araç Takip Sistemi
- Eğitim Yönetim Sistemi
- Personel Devam Kontrol Sistemi
- e-MOC (Değişiklik Yönetim Sistemi)
- e-TPC (Boru Hattı Geçiş Yönetim Sistemi)
- e-PUR (Süreç Uygunsuzluk Raporlama Sistemi)
- Elektronik Belge Yönetim Sistemi
- Aktif Dizin uygulaması

- Dosya Sunucusu
- E-reçete Sistemi
- Log Yönetim/SIEM Uygulaması
- Parmak izi kayıt ve takip cihazı
- Kullanıcı Bilgisayarları (Microsoft Office Programları, masaüstü, notebook)
- Sunucular (Etki alanı, yedekleme, e-posta, veritabanları, web, dosya paylaşım, vb.)
- Bilgi güvenliği cihaz ve uygulamaları (SIEM, Güvenlik duvarı, Anti virüs uygulaması, NAC cihazı, VPN uygulaması, veri sınıflandırma ve DLP uygulaması, şifreleme uygulaması gibi)
- Harddiskler, harici bellekler
- Optik Diskler (CD, DVD)
- Yazıcılar, tarayıcılar, fotokopi makineleri

Elektronik Olmayan Ortamlar:

- Kağıt, belge ve dosyalar
- Manuel veri kayıt sistemleri
- Yazılı, basılı, görsel ortamlar
- Birim dolapları (Kilitli ve sınırlı erişimli)
- Arşiv (Özel korumalı)

5. İLKELER

BİL, kişisel verilerin saklanması ve imhasında aşağıda yer alan ilkeler çerçevesinde hareket etmektedir: Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesinde; Kanun'a ve ilgili mevzuat hükümlerine, Kurul kararlarına ve işbu Politikaya tamamen uygun hareket edilmektedir.

Kurum tarafından kişisel verilerin işlenmesi esnasında, ilgili kişilerin hakları korunmaktadır. Kişisel veriler, KVKK m.4'te yer alan genel ilkelere uygun şekilde toplanmakta ve işlenmektedir.

Kişisel verilerin imha edilmesi ile ilgili yapılan tüm işlemler Kurum tarafından kayıt altına alınmakta ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere 10 (on) yıl süreyle saklanmaktadır.

Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri imha yöntemlerinden uygun olanı Kurum tarafından seçilmektedir. Ancak, ilgili kişinin talebi halinde uygun yöntem gerekçesi açıklanarak seçilecektir.

Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Kurum tarafından re'sen veya ilgili kişinin talebi üzerine imha edilmektedir. Bu hususta ilgili kişi tarafından Kuruma başvurulması halinde;

İletilen talepler en geç 30 (otuz) gün içerisinde sonuçlandırılmakta ve ilgili kişiye bilgi verilmektedir, Talebe konu verilerin üçüncü kişilere aktarılmış olması durumunda, bu durum verilerin aktarıldığı üçüncü kişiye Bildirilmekte ve üçüncü kişiler nezdinde gerekli işlemlerin yapılması temin edilmektedir.

6. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Kurum tarafından işlenen kişisel veriler ilgili mevzuat gereği Kuruma yüklenen kamu hizmetinin ifası amacıyla özellikle; kanunlarda açıkça öngörülmesi, bir sözleşmenin kurulması veya ifasıyla doğrudan

doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması ve açık rıza işlenme şartları kapsamında elektronik veyahut elektronik olmayan ortamlarda güvenli bir biçimde Kanun ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

6.1 Saklamaya İlişkin Açıklamalar

Kurum tarafından işlenen kişisel verilerin muhafaza süreleri Kanun'un m.4/2.d "*İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*" ilkesi dikkate alınarak belirlenmiştir.

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

6.1.1 Saklamayı Gerektiren Hukuki Sebepler

Kurumun 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,
- 4734 sayılı Kamu İhale Kanunu,
- 2942 sayılı Kamulaştırma Kanunu
- 4735 sayılı Kamu İhale Sözleşmeleri Kanunu
- 2286 sayılı Devlet İhale Kanunu
- 5283 sayılı Bazı Kamu Kurum ve Kuruluşlarına Ait Sağlık Birimlerinin Sağlık Bakanlığına Devredilmesine Dair Kanun
- 5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun
- 5115 sayılı Kimlik Bildirme Kanunu
- 3308 sayılı Mesleki Eğitim Kanunu
- 5326 sayılı Kabahatler Kanunu
- 7201 sayılı Tebligat Kanunu
- 5271 sayılı Ceza Muhakemesi Kanunu
- 1136 sayılı Avukatlık Kanunu
- 6100 sayılı Hukuk Muhakemeleri Kanunu
- 4721 sayılı Türk Medeni Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,

- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 5682 sayılı Pasaport Kanunu
- 5510 Sayılı Sosyal Sigortalar Kanunu
- 7315 Sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu
- 2872 Sayılı Çevre Kanunu
- 4734 Sayılı Kamu İhale Kanunu
- Devlet Arşiv Hizmetleri Hakkında Yönetmelik
- Yapım İşleri İhale Uygulama Yönetmeliği
- Kamu Konutları Yönetmeliği
- Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ
- Sektörel SOME Kurulum ve Yönetim Rehberi
- Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği
- 20.10.2012 Tarih ve 28447 Sayılı Resmî Gazetede yayınlanan “Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı”
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler

çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

6.1.2 Saklamayı Gerektiren İşleme Amaçları

BİL, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda muhafaza eder.

- İnsan kaynakları süreçlerini yürütmek,
- Acil durum süreçlerinin yürütülmesi,
- Kurumsal iletişimi sağlamak,
- Basın, yayın ve haber içeriklerini üretmek,
- Kurum güvenliğini sağlamak,
- Sözleşme süreçlerinin sürdürülmesi,
- Genel muhasebe işlemlerinin yürütülmesi,
- Denetim, teftiş ve tetkik faaliyetlerinin gerçekleştirilmesi,
- Eğitim faaliyetlerinin gerçekleştirilmesi,
- İş sağlığı ve güvenliği süreçlerinin yürütülmesi,
- Vatandaşlardan gelen talep ve şikayetlerin değerlendirip sonuçlandırılmasını sağlamak,
- BİL ödemelerini gerçekleştirebilmek,
- BİL tahsilatlarını gerçekleştirebilmek,
- Bakım ve onarım faaliyetlerinin gerçekleştirilmesi,
- Kişilerin BİL sosyal tesislerinden ve BİL hizmetlerinden yararlanabilmesi,
- Projeler ile imzalanan sözleşme ve protokoller neticesinde iş ve işlemleri ifa edebilmek,

- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak,
- Hizmetler ile alakalı kayıt işlemlerinin yapılması ve süreçlerin yürütülmesini sağlamak,
- Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak,
- Yasal raporlamalar yapmak,
- Çağrı merkezi süreçlerini yönetmek,
- Mevzuat gereği Kurumun ifa etmesi gereken işlemleri gerçekleştirmek,
- Mevzuat gereği yetkili kurum ve kuruluşlara Bildirimde bulunmak,
- Kanuni yükümlülükleri yerine getirmek,
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek,
- Kullanıcıya yetki ataması, kaldırılması taleplerinin yerine getirilmesi,
- Seyahatlerin gerçekleştirilmesi ve hakkın tesisi,
- Kurum içi düzeni sağlamak,
- Personelin kıyafet ihtiyacının karşılanması,
- Yemekhane hizmetlerin sürdürülmesi,
- Atığın mevzuata uygun şekilde taşınmasının kontrolü,
- ÇED taahhütlerini ve yasal sorumlulukları yerine getirmek,
- Arama faaliyetlerinin yürütülmesi,
- Kurum içi evrak sistemine uygun şekilde evrakların kaydedilmesi ve saklanması,
- İşletme anlaşması kapsamında petrol kalitesini kontrol edilmesi,
- Projelerin planlanmasının yapılması,
- Erişim güvenliği kapsamında log kayıtlarının alınması,
- Sistem odası güvenliğini sağlamak
- Hukuki süreçlerin ve davaların takibi ve yürütülmesi.

6.2 İmhayı Gerektiren Sebepler

Kişisel veriler;

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya iptali,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- KVK Kanunu m.5 ve m.6'da yer alan, kişisel verilerin işlenmesini gerektiren işleme şartlarının ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,
- KVK Kanunu m.11 gereği ilgili kişinin hakları çerçevesinde yapılan, kişisel verilerinin silinmesi ve yok edilmesine ilişkin başvurunun Kurum tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyetle bulunulması ve bu talebin Kurul tarafından uygun bulunması,

- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması durumlarında, BİL tarafından ilgili kişinin talebi üzerine ya da re'sen silinir, yok edilir veya anonim hale getirilir.

7. ALINAN İDARİ ve TEKNİK TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için; KVK Kanunu m.12 ve m.6/4 gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Kurum tarafından teknik ve idari tedbirler alınır.

Kurum tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

7.1. İdari Tedbirler

- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir
- Kişisel veri envanterleri hazırlanarak, mevcut risk ve tehditler belirlenmiştir.
- Kurum'un VERBİS'e kaydı gerçekleştirilmiştir.
- Kurum nezdinde, KVKK süreçlerini yürütmek ve denetlemek için icra ve karar organı mahiyetinde Kişisel Verileri Koruma Komisyonu (Kurum KVK Komisyonu) oluşturulmuştur.
- Saklanan kişisel verilere Kurum içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- Kurum, kriz yönetimi için "Kişisel Veri İhlali Olayı Müdahale Politikası ve Planı" hazırlamıştır. İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede (72 saat içerisinde) ilgisine ve Kurula bildirir.
- Kişisel verilerin aktarılması ile ilgili olarak, kişisel verilerin aktarıldığı 3. gerçek/tüzel kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
- Kişisel verilerin işlenmesi hakkında Bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
- Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın yöneticisi tarafından bağlı bulunan bir üst yöneticiye bildirilir. Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında, gerekli idari işlem yapılır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri yapılmaktadır.
- Çalışanlar için bilgi güvenliği ve veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.

- Kurum tarafından hazırlanan idari şartname ve sözleşmeler ile iş sözleşmelerine yönelik kişisel veri güvenliğine ilişkin hükümler eklenmiştir.
- Kurum içi periyodik ve rastgele denetim faaliyetleri gerçekleştirilmektedir.
- Özel nitelikli kişisel veri güvenliğine yönelik politika ve prosedürler belirlenmiş ve uygulanmaktadır.
- Veri sorumlusu Kurum ile veri işleyen kişiler arasında kişisel verilerin korunmasına ilişkin sözleşmeler hazırlanmıştır.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Kişisel veriler mümkün olduğunca azaltılmaktadır.
- Kurum'un akdettiği iş sözleşmelerine kişisel verilerin korunmasına ilişkin madde veya bölümler (klozlar) yer almaktadır.
- Kurum'un mal ve hizmet alımlarında kullandığı idari sözleşme, idari şartname ve teknik şartname dokümanlarına ek olarak yüklenicilere yönelik "İdari Şartname/İdari Sözleşme/Teknik Şartname Eki KVK Taahhütnamesi" belgesi hazırlanmıştır.
- Kurum e-postalarında kullanılmak üzere KVK Uyarı Metni hazırlanmıştır.
- Kuruma ait kişisel veri envanterlerinin oluşturulması, düzenlenmesi ve güncellenmesiyle sorum envanter sorumluları birimi oluşturulmuştur.
- ISO 27001 BGYS politikaları uygulanmaktadır

7.2. Teknik Tedbirler:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır
- Anahtar yönetimi uygulanmaktadır
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır
- Çalışanlar için yetki matrisi oluşturulmuştur
- Erişim logları düzenli olarak tutulmaktadır
- Gerektiğinde veri maskeleyme önlemi uygulanmaktadır
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır
- Güncel anti-virüs sistemleri kullanılmaktadır
- Güvenlik duvarları kullanılmaktadır
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.)
- Kişisel veri içeren ortamların güvenliği sağlanmaktadır
- 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
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir
- Saldırı tespit ve önleme sistemleri kullanılmaktadır
- Sızma testi uygulanmaktadır
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir
- Şifreleme yapılmaktadır
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır
- Veri kaybı önleme yazılımları kullanılmaktadır
- Parola güvenliği politikasıyla güçlü, zorlayıcı, periyodik değişim, karakter sınırlaması kısıtlarıyla parola güvenliği sağlanmaktadır
- Kişisel veri içeren ortamların güvenliği için uygun kullanım politikası gereğince kullanıcılar Bilgisayarın başından log off yaparak ayrılmaktadır.

8. KİŞİSEL VERİLERİ KORUMA BİRİMİ

Kurum nezdinde, KVKK süreçlerini yürütmek ve denetlemek için icra ve karar organı mahiyetinde görev ifa edecek, Kişisel Verileri Koruma Komisyonu (Kurum KVK Komisyonu) ihdas edilmiştir. Kişisel Verileri Koruma Komisyonunun yapısı, görevleri, toplantı usulü, üyelerin ve envanter sorumlularının görevleri, işbu politikanın eki “Kurum KVK Komisyonu ve Envanter Sorumluları Çalışma Usul ve Esasları” belgesinde yer almaktadır.

Kurumun tüm birimleri ve çalışanları; kişisel veri işleme, saklama, imha, verilere erişim, veri güvenliğinin sağlanması, ilgili kişi başvurularının cevaplanması, kişisel veri envanteri ve KVK Kanunu ve ilgili mevzuat kapsamındaki diğer yükümlülöklere dair, Kurum KVK Komisyonu tarafından alınan tüm kararları uygulamakla yükümlüdür.

9. 9. KİŞİSEL VERİLERİN İMHASI

Kurum kişisel verileri, ilgili mevzuatta öngörölen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etmektedir. Bu kapsamda, öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörölüp öngörölmediğı tespit edilmekte, bir süre belirlenmişse bu süreye uygun davranılmakta, bir süre belirlenmemişse kişisel veriler işlendikleri amaç için gerekli olan süre kadar saklanmaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde, daha uzun süre işlenmelerine izin veren hukuki bir sebep bulunmaması halinde, kişisel veriler Kurum tarafından iş bu politikaya göre silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Kurum, bir kamu kurumu olması nedeniyle işlediğı verilerin saklama süreleri bakımından başkaca mevzuatlara da tabi olmaktadır. Örneğın kişisel veri içeren fiziki bir belge veya elektronik ortamdaki bir veri; Devlet Arşiv Hizmetleri Hakkında Yönetmelik gereğı aynı zamanda “arşiv belgesi” veya “arşivlik belge” statüsünde olabilmektedir. Bu kapsamda KVK Kanunu ve ilgili mevzuat gereğince bir belge

üzerindeki kişisel verinin imhası amaçlanırken, Devlet Arşiv Hizmetleri Hakkında Yönetmelik gereği “arşiv belgesi” veya “arşivlik belge” vasfında bulunan bir belgenin imhası riski de söz konusu olacaktır. Bu risk göz önüne alınarak, Kurumdaki kişisel veri saklama süreleri belirlenirken ilgili mevzuatta açık bir saklama süresi bulunmuyorsa; öncelikli olarak Devlet Arşivleri Başkanlığı tarafından yayınlanan ve aşağıda URL’si yer alan saklama planlarındaki saklama sürelerine bakılmış ve ilgili veri kategorisine uygun bir süre belirlenmiş ise, bu süre kullanılmıştır.

http://www.devletarsivleri.gov.tr/varliklar/dosyalar/eskisiteden/Formlar/KamuKurumlari/yardimci_hizmetler_saklama.pdf

Devlet Arşivleri Başkanlığı tarafından yayınlanan saklama planlarında uygun bir saklama süresi bulunamamışsa, 6098 sayılı Türk Borçlar Kanunu’ndaki genel zamanaşımı sürelerine bakılmış; kişisel veri işleme faaliyetine uygun bir zamanaşımı süresi de yoksa, KVK Kanunu m.4/2-ç gereği “İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü” olmak şartıyla uygun, makul bir süre tespit edilmiştir.

Söz konusu sürelerin VERBİS’e kaydı sırasında ise her veri kategorisi içerisinde en uzun saklama süresi baz alınmıştır.

Saklama süreleri sözleşmesel bir ilişki varsa, tarafların sözleşmeden kaynaklanan yükümlülüklerinin sona ermesiyle birlikte, diğer faaliyetler bakımından işlem tamamlandıktan ve kesin sonucu alındıktan sonra başlar.

Kişisel veriler, hukuki bir ihtilaf veya dava süreci olması halinde, hukuki süreç tamamlanana kadar saklanır.

10. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

Saklama süresinin sonunda kişisel veriler, Kurum tarafından re’sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

Kurum, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde ise, uygun yöntemi gerekçesini açıklayarak seçer. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere 10 (on) yıl süreyle saklanır.

10.1 Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m.4/b hükmünde “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” şeklinde tanımlanmıştır.

Kişisel veriler aşağıda yer alan tabloda verilen yöntemlerle silinir.

Kişisel Verilerin Silinmesi Tablosu

VERİ KAYIT ORTAMI	AÇIKLAMA
Sunucularda yer alan kişisel veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için, sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç, diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için, evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
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.

10.2 Kişisel Verilerin Yok Edilmesi:

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel veriler aşağıda yer alan tabloda verilen yöntemlerle yok edilir.

Kişisel Verilerin Yok Edilmesi Tablosu

VERİ KAYIT ORTAMI	AÇIKLAMA
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpmak 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 değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

10.3 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.

Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Bununla birlikte Kurum, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi tekniklerinde Kurum'un yayınlamış olduğu "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'ni" (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf>) dikkate almakta ve bu rehberde yayınlanan örneklerden uygun olanını seçmektedir.

11.SAKLAMA VE İMHA SÜRELERİ

Kurum 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 kayıta;

Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde "Kurum Kişisel Verileri Koruma Komisyonu" tarafından güncellemeler yapılır.

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

Süreç Bazında Saklama ve İmha Süreleri Tablosu

SÜREÇ	SAKLAMA SÜRESİ (birim arşivi + kurum arşivi)	İMHA SÜRESİ
Çalışanlara ait Özlük Dosyalarının Tutulması	Birim Arşivinde Kurumla İlişği Kesilene Kadar + Kurum Arşivinde Son İşlem Tarihi İtibariyle 101 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Emekli ikramiyesi, makam görev tazminatı ve çalışan vefat edince ailesine ölüm yardımı yapılması	50 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Fazla mesai ve puantaj işlemlerinin yürütülmesi	İş Akdi Sona Erdikten Sonra 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Çalışma belgelerinin düzenlenmesi	10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde

Sendikal faaliyetlerinin ve toplu iş sözleşme süreçlerinin yürütülmesi	Toplu İş Akdi Sona Erdikten Sonra 15 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
İcra Müdürlüklerinden gelen maaş haczi taleplerinin işleme alınması	50 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
BES süreçlerinin yürütülmesi	50 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
İş seyahatı kapsamında otel ve uçak rezervasyonlarının gerçekleştirilmesi	10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Çalışanlara gsm hatlarının verilmesi faaliyetinin gerçekleştirilmesi	30 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Tedarikçilerin ve müşterilerin cari hesabının açılması	Sözleşmesel İlişki Sona Erdikten Sonra 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Personel ödemelerin yapılması amacıyla cari kartın oluşturulması	50 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Boru hattı güzergahı üzerinde yapılan kiralama faaliyetlerinin ve zarar ödemelerinin yapılması	Sözleşmesel İlişki Sona Erdikten Sonra 15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Personelin telefon limit aşımının ücretlendirilmesi	İş Akdi Sona Erdikten Sonra Birim Arşivinde 5 Yıl + Kurum Arşivinde 5 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Konaklama hizmetlerin sürdürülmesi kapsamında faturalandırma faaliyet	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
İmza sirküsünün saklanması	imza sirküsü süresinin sona ermesinden itibaren 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Personel kimlik kartının basılması	Personelin kurumla ilişkisi kesilene kadar	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kartvizit basılması süreci	Personelin kurumla ilişkisi kesilene kadar	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Personel araç kartının basılması	Personelin kurumla ilişkisi kesilene kadar	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kurum tanıtım faaliyeti kapsamında Konferans ve fuarlara katılımın gerçekleştirilmesi	Etkinlik tarihinden itibaren 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Talep ve Şikayet yönetiminin yürütülmesi	Süreç Tamamlandıktan Sonra Birim Arşivinde 5 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
İstasyon ve CMT bölgesi konaklama alanları kira	Hukuki İlişki Sona Erdikten Sonra Birim 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde

ödemesinin gerçekleştirilmesi		
Satın alım ve satış süreçlerinin gerçekleştirilmesi	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Alt yüklenici personellerinin kayıtların tutulması	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Alt yüklenici personellerinin hakedişinin yapılması	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
İş ekipmanların temini faaliyeti	İşten ayrılma tarihinden itibaren en az 15 yıl süreyle (Asbest, Mutojen veya Kanserojen Maddeye Maruz Kalan Personel Bakımından 40 yıl)	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Boru hattının geçtiği şehirlerin çevre ve şehircilik il müdürlüklerine periyodik mevzuat gereği aylık raporlama yapılması	10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Atık taşıma süreçlerinin yürütülmesi	Birim arşivinde: 5 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Çevre izleme faaliyetleri	Hukuki İlişki Sona Erdikten Sonra 2 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kampüs çevresi ve içerisinin CCTV sistemi üzerinden izlenmesi ve kaydedilmesi	1 Ay Saklanmaktadır.	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Girişlerde ziyaretçi kabulü ve kayıt işlemleri	Kayıt tarihinden itibaren 2 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Çalışanların giriş çıkış kayıtlarının tutulması	İşlem tarihinden itibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Çalışanların araçları için araç kartı oluşturulması	Hukuki İlişki Sona Erdikten Sonra 2 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Özel güvenlik görevlilerinin özlük işlerinin yürütülmesi	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Hasta kayıt defterlerinin tutulması	5 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Periyodik muayenelerin yapılması ve kayıtların tutulması	İşten ayrılma/iş akdi sona erme tarihinden itibaren 15 yıl süreyle	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Hasta olan çalışanların, Lojmanlarda kalan personel yakınlarının veya misafirlerin muayenelerinin gerçekleştirilmesi ve rahatsızlıkları boyunca	5 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde

teşhis/tedavi/bakım hizmetlerinin yürütülmesi ve takip edilmesi		
İş güvenliği ile ilgili faaliyetlerin yürütülmesi ve eğitimlerin verilmesi	İşten ayrılmasından itibaren 15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
E-Reçete sistemine kurum çalışanlarının sağlık durumları ile reçetelerinin kaydedilmesi	5 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Konaklama faaliyetlerinin gerçekleştirilmesi	İşlem tarihinden Sonra 2 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Lojman konaklama faaliyetlerinin yürütülmesi	Tahsis tarihinden itibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Yemekhane hizmetlerin sürdürülmesi	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Arama Kurtarma Faaliyeti	Kurtarma Faaliyetinin Sonarmesinden itibaren 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Dökme akaryakıt boşaltım formunun tutulması sürecinin yürütülmesi	10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kaza sonuucu yapılan resmi işlemler	10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Araç kullanan şoförler ya da araç tahsisi edilen çalışanlara ait kayıtların tutulması faaliyeti	10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Güncel(yıllık) sağlık raporlarının tutulması faaliyeti	İşten ayrılma tarihinden itibaren 15 yıl süreyle	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
PDKS Personel Devam Kontrol Sistemi	İş Akdi Sona Erdikten Sonra 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Aktif Dizin Hizmeti	Hukuki İlişki/İşlem Sona Erdikten Sonra 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kullanıcı İnternet hareketlerinin kayıt altına alınması	2 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Sistemler üzerinden yetki oluşturup yetki kaldırma	Hukuki İlişki Sona Erdikten Sonra 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Dava Dosyası Kapsamında İşlenen Kişisel Veriler	Birim Arşivinde 5 Yıl + Kurum Arşivinde 35 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde

İcra Takip Dosyası Kapsamında İşlenen Kişisel Veriler	Birim Arşivinde 5 Yıl + Kurum Arşivinde 15 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Arabuluculuk Kapsamında İşlenen Kişisel Veriler	Uzlaşma Sağlanan Dosyalar Birim Arşivinde 10 Yıl, Dava Açılanlar İlgili Dava Dosyasının İçerisine Konulmaktadır.	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Hukuki mütalâa verilmesi faaliyeti kapsamında işlenen kişisel veriler	Birim Arşivinde 5 Yıl + Kurum Arşivinde 25 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kamu Kurumları ile Şirket (BİL) arasındaki hukuki yazışmaların takibi faaliyeti	Adli davalarda 40 yıl İcra dosyalarında 20 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Disiplin işlemlerinin yürütülmesi faaliyeti	30 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Integrity Müdürlük faaliyetleri kapsamında hizmet alım süreçlerinin yürütülmesi	Sözleşmesel İlişki Sona Erdikten Sonra 15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Bakım müdürlüğü bakım süreçlerinin yürütülmesi	Hukuki ilişki sona erdikten sonra 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
SCADA ve Telekom müdürlüğü bakım süreçlerinin yürütülmesi	Hukuki İlişki Sona Erdikten Sonra 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Proje geliştirme süreçlerinin yürütülmesi	15 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kara ve deniz operasyonlarının yürütülmesi	Hukuki İlişki Sona Erdikten Sonra 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Ham petrol boru hattından gelen petrolün analiz edilmesi	Hukuki işlemin sona erme tarihinden itibaren 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Kalite yönetim sistemlerinin belgelendirilmesi, sürdürülmesi ve koordinasyonu	Değişiklikten itibaren 10 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde
Gelen ve giden evrak kayıtlarının yapılması, ilgili birimlere sevki ve arşivlenmesi, kargo takiplerinin yapılması	30 yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresinde

12.PERİYODİK İMHA SÜRESİ

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m.11 gereğince Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Kurumda her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

13.POLİTİKA’NIN YAYINLANMASI VE SAKLANMASI

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

14.POLİTİKA’NIN GÜNCELLENME PERİYODU

Politika Kurum KVK Komisyonu tarafından, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

15.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Kurumun internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika’nın ıslak imzalı eski nüshası Kurum KVK Komisyonu kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 10 yıl süre ile Kurum KVK Komisyonu tarafından saklanır.