

ATATÜRK ORMAN ÇİFTLİĞİ
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ
- 1.1 Amaç
- 1.2 Kapsam
- 1.3 Kısaltmalar ve Tanımlar
2. SORUMLULUK VE GÖREV DAĞILIMLARI
3. KAYIT ORTAMLARI
4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR
- 4.1 Saklamaya İlişkin Açıklamalar
- 4.1.1 Saklamayı Gerektiren Hukuki Sebepler
- 4.1.2 Saklamayı Gerektiren İşleme Amaçları
- 4.2 İmhayı Gerektiren Sebepler
5. TEKNİK VE İDARİ TEDBİRLER
- 5.1 Teknik Tedbirler
- 5.2 İdari Tedbirler
6. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ
- 6.1 Kişisel Verilerin Silinmesi
- 6.2 Kişisel Verilerin Yok Edilmesi
- 6.3 Kişisel Verilerin Anonim Hale Getirilmesi
7. SAKLAMA VE İMHA SÜRELERİ
8. PERİYODİK İMHA SÜRESİ
9. POLİTİKANIN YAYIMLANMASI VE SAKLANMASI
10. POLİTİKANIN GÜNCELLENME PERİYODU
11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

1. GİRİŞ

1.1. Amaç

Kişisel Verileri Saklama ve İmha Politikası, Atatürk Orman Çiftliği Müdürlüğüne gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Veri Sorumlusu sıfatıyla Atatürk Orman Çiftliği Müdürlüğü çalışanlarının, hizmet alımı sözleşmesi ile çalışanların, stajyerlerin, müşterilerin, potansiyel müşterilerin, tedarikçilerin, kiracıların, kiraya verenlerin, iş ortaklarının hissedarları/yetkilileri/çalışanlarının, ziyaretçilerin, işbirliği içinde olunan özel hukuk ve kamu tüzel kişilerin çalışanları/hissedarları/yetkililerinin ve Müdürlükle irtibat halinde olan kişilerin verilerinin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, bu Politikaya uygun olarak gerçekleştirilir.

1.2. Kapsam

Müdürlük çalışanlarının, hizmet alımı sözleşmesi ile çalışanların, stajyerlerin, müşterilerin, potansiyel müşterilerin, tedarikçilerin, kiracıların, kiraya verenlerin, iş ortaklarının hissedarları/yetkilileri/çalışanlarının, ziyaretçilerin, işbirliği içinde olunan özel hukuk ve kamu tüzel kişilerin çalışanları/hissedarları/yetkililerinin ve Müdürlükle irtibat halinde olan kişilerin verileri bu Politika kapsamında olup Müdürlüğün sahip olduğu ya da Müdürlük tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. Tanımlar ve Kısaltmalar

- Alıcı Grubu** : Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,
- Açık Rıza** : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- Anonim Hale Getirme** : Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
- Çalışan** : Atatürk Orman Çiftliği Müdürlüğü kadrolu personeli ile hizmet alımı sözleşmesi ile çalışanları,
- EBYS** : Elektronik Belge Yönetim Sistemini,
- Elektronik Ortam** : Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,
- Elektronik Olmayan Ortam** : Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamları,
- İlgili Kişi** : Kişisel verisi işlenen gerçek kişiyi,
- 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,

İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
Kanun	:	6698 sayılı Kişisel Verilerin Korunması Kanununu,
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	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
Kişisel Veri İşleme Envanteri	:	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
Kurul	:	Kişisel Verileri Koruma Kurulunu,
Kurum Müdürlük	:	Kişisel Verileri Koruma Kurumunu, Atatürk Orman Çiftliği Müdürlüğünü,
Müşteri	:	Müdürlükten mal veya hizmet alan gerçek veya tüzel kişi ve kurumlar ile bunların yetkilileri, çalışanları, ortakları ve temsilcilerini,
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 verilerini,
Periyodik İmha	:	Kanunda 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,
Politika	:	Kişisel Verileri Saklama ve İmha Politikasını,

- Tedarikçi** : Müdürlüğe belirli bir sözleşme çerçevesinde hizmet veya mal sağlayan gerçek veya tüzel kişi ve kurumlar ile bunların yetkilileri, çalışanları, ortakları ve temsilcilerini,
- Veri Kayıt Sistemi** : Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
- Veri Sorumlusu** : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişiyi,
- Veri Sorumluları Sicil Bilgi Sistemi** : Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kurum tarafından oluşturulan ve yönetilen bilişim sistemini,
- VERBİS** : Veri Sorumluları Sicil Bilgi Sistemini,
- Yönetmelik** : Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği,
- Veri İşleyen** : Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- Ziyaretçi** : Müdürlüğü ziyaret eden kişiyi,

ifade eder.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Müdürlüğün 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 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 vermekle yükümlüdürler. Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıda verilmiştir:

UNVAN	BİRİM	GÖREV
Müdür	Atatürk Orman Çiftliği Müdürlüğü	Çalışanların Politikaya uygun hareket etmesinden sorumludur.
Kişisel Verileri Koruma Komisyonu	Atatürk Orman Çiftliği Müdürlüğü	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, uygulamanın denetlenmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi İşlem Birim Sorumlusu	Atatürk Orman Çiftliği Müdürlüğü	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

Bitkisel Üretim Müdürü, Halkla İlişkiler ve Pazarlama Müdürü, Hukuk Müşaviri, Meyvesuyu ve Bal Fabrikası Müdürü, Muhasebe ve Mali İşler Müdürü, Personel ve Destek Hizmetleri Müdürü, Süt Fabrikası Müdürü, Ticaret Müdürü,	Atatürk Orman Çiftliği Müdürlüğü	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
--	-------------------------------------	--

3. KAYIT ORTAMLARI

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<p>Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)</p> <p>Yazılımlar (ofis yazılımları, EBYS, VERBİS, ERP uygulaması, İSG uygulaması vb.)</p> <p>Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)</p> <p>✓ Kişisel bilgisayarlar (masaüstü, dizüstü)</p> <p>✓ Mobil cihazlar (tablet vb.)</p> <p>✓ Optik diskler (CD, DVD vb.)</p> <p>Taşınabilir bellekler (harici diskler, hafıza kart vb.)</p> <p>✓ Yazıcı, tarayıcı, fotokopi makinesi</p>	<p>✓ Kâğıt</p> <p>Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)</p> <p>✓ Yazılı, basılı, görsel ortamlar</p>

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Müdürlük tarafından çalışanların, hizmet alımı sözleşmesi ile çalışanların, stajyerlerin, müşterilerin, potansiyel müşterilerin, tedarikçilerin, kiracıların, kiraya verenlerin, iş ortaklarının hissedarları/yetkilileri/çalışanlarının, ziyaretçilerin, işbirliği içinde olunan özel hukuk ve kamu tüzel kişilerin çalışanları/hissedarları/yetkililerinin ve Müdürlükle irtibat halinde olan ilgili kişilerin kişisel verileri, Kanuna uygun olarak saklanır ve imha edilir.

4.1. Saklamaya İlişkin Açıklamalar

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işlenme şartları sayılmıştır. Müdürlüğümüz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işlenme amaçlarına uygun süre kadar saklanır.

4.1.1. Saklamayı Gerektiren Hukuki Sebepler

Müdürlüğümüz 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,
- 4734 sayılı Kamu İhale Kanunu,
- 657 sayılı Devlet Memurları 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 ve Kontrol Kanunu,
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 sayılı İş Kanunu,
- 5434 sayılı Emekli Sağlığı Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler.

4.1.2. Saklamayı Gerektiren İşlenme Amaçları

Müdürlük kişisel verileri, faaliyetleri çerçevesinde aşağıdaki amaçlar doğrultusunda işler ve saklar.

- Etkinlik yönetimi,
- İş faaliyetlerinin planlanması ve icrası,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Tedarik zinciri yönetimi süreçlerinin planlanması ve icrası,
- Üretim ve/veya operasyon süreçlerinin planlanması ve icrası,
- Bilgi güvenliği süreçlerinin planlanması, denetimi ve icrası,
- Bilgi teknolojileri alt yapısının oluşturulması ve yönetilmesi,
- Finans ve/veya muhasebe işlerinin takibi,
- Lojistik faaliyetlerinin planlanması ve icrası,
- İş ortakları ve/veya tedarikçilerle olan ilişkilerin yönetimi,
- Ürün ve/veya hizmetlerin satış süreçlerinin planlanması ve icrası,
- Müşteri ilişkileri yönetimi süreçlerinin planlanması ve icrası,
- Sözleşme süreçlerinin ve/veya hukuki taleplerin yürütülmesi,
- Müşteri talep ve/veya şikayetlerinin takibi,
- Müdürlüğün sunduğu ürün ve/veya hizmetlere bağlılık oluşturulması ve/veya artırılması süreçlerinin planlanması ve/veya icrası,
- Ürün ve/veya hizmetlerin pazarlama süreçlerinin planlanması ve icrası,
- İnsan kaynakları süreçlerinin planlanması ve yürütülmesi,

- Müşteri memnuniyeti aktivitelerinin planlanması ve/veya icrası,
- Hukuk işlerinin yürütülmesi,
- Müdürlük faaliyetlerinin prosedürlere ve/veya ilgili mevzuata uygun olarak yürütülmesinin temini için gerekli operasyonel faaliyetlerinin planlanması ve icrası,
- Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi,
- Müdürlük denetim faaliyetlerinin planlanması ve icrası,
- Verilerin doğru ve güncel olmasının sağlanması,
- Müdürlük faaliyetlerinin güvenliğinin temini,
- Müdürlüğün fiziksel mekan güvenliğinin sağlanması,
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarının tespit edilmesi, verilen hizmetlerin buna göre düzenlenmesi ve güncellenmesi,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesi.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanununun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Müdürlük tarafından kabul edilmesi,
- Müdürlüğün, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması durumlarında, Müdürlük tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re' sen silinir, yok edilir veya anonim hale getirilir.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanununun 12 nci maddesiyle Kanununun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler ,Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Müdürlük tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

İşlenen kişisel verilerle ilgili olarak Müdürlük tarafından alınan teknik tedbirler aşağıda sayılmıştır.

- Sızma (Penetrasyon) testleri ile Müdürlüğümüz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak takip edilmektedir.

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.
- Müdürlüğün bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Müdürlük içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler, kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Müdürlük, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Müdürlük tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Müdürlük internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması / yaptırılması ve test sonuçlarının kayıt altına alınması sağlanmaktadır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenlik sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerektiğinde şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrlenmekte ve kriptografik anahtar, farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN, IPSEC tunnel kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2. İdari Tedbirler

İşlenen kişisel verilerle ilgili olarak Müdürlük tarafından alınan idari tedbirler aşağıda sayılmıştır.

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ile ilgili mevzuat hakkında eğitimler verilmektedir.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri/ taahhütname imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara disiplin prosedürü uygulanacaktır.
- Kişisel veri işlemeye başlamadan önce Müdürlük tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Müdürlük içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

Kişisel veriler, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda Müdürlük tarafından re 'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler aşağıda belirtilen yöntemlerle silinir.

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler aşağıda belirtilen 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 kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

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.

7. SAKLAMA VE İMHA SÜRELERİ

- İlgili 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 Kişisel Verileri Koruma Komisyonu güncellemeler yapar.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Personel ve Destek Hizmetleri Müdürlüğü tarafından yerine getirilir.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Müdürlük İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kurum İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 101 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı Katılımcılarının Kaydı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	3 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

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

9. POLİTİKANIN 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 Kişisel Verileri Koruma Komisyonu tarafından saklanır.

10. POLİTİKANIN GÜNCELLENME PERİYODU

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

11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Müdürlüğün internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politikanın ıslak imzalı eski nüshaları Müdürlük kararı ile Kişisel Verileri Koruma Komisyonu tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Kişisel Verileri Koruma Komisyonu tarafından saklanır.