



**DEVLET MALZEME OFİSİ
GENEL MÜDÜRLÜĞÜ
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI**

DEVLET MALZEME OFİSİ GENEL MÜDÜRLÜĞÜ
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

DEVLET MALZEME OFİSİ GENEL MÜDÜRLÜĞÜ
ADRES: Devlet Mahallesi İnönü Bulvarı No:18 06570 Çankaya/ANKARA
TELEFON: 0 (312) 410 30 00 internet sitesi: www.dmo.gov.tr

Bu Politika metninde yer alan tüm içeriklerin, bireysel kullanım dışında izin alınmadan kısmen ya da tamamen kopyalanması, çoğaltılması, kullanılması, yayımlanması ve dağıtılması yasaktır. Bu yasağa uymayanlar hakkında 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca yasal işlem yapılacaktır. Ürünün tüm hakları saklıdır.

İçindekiler

1. GİRİŞ	4
1.1 Amaç	4
1.2 Kapsam.....	4
1.3 Kısaltmalar ve Tanımlar	4
2. SORUMLULUK VE GÖREV DAĞILIMLARI	7
3. KAYIT ORTAMLARI	8
4. SAKLAMA VE İMHA İLİŞKİN AÇIKLAMALAR	8
4.1 Saklamaya İlişkin Açıklamalar	8
4.1.1 Saklamayı Gerektiren Hukuki Sebepler.....	8
4.1.2 Saklamayı Gerektiren İşleme Amaçları.....	9
4.2 İmhayı Gerektiren Sebepler	11
5. TEKNİK VE İDARİ TEDBİRLER	11
5.1 Teknik Tedbirler	12
5.2 İdari Tedbirler.....	13
6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	13
6.1 Kişisel Verilerin Silinmesi	14
6.2 Kişisel Verilerin Yok Edilmesi	14
6.3 Kişisel Verilerin Anonim Hale Getirilmesi.....	15
7. SAKLAMA VE PERİYODİK İMHA SÜRELERİ	15
8. POLİTİKA'NIN YAYINLANMASI, YÜRÜRLÜĞE GİRMESİ VE GÜNCELLENMESİ	16

1. GİRİŞ

1.1 Amaç

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), Devlet Malzeme Ofisi Genel Müdürlüğü tarafından ("DMO") gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

DMO; stratejik planında belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; ilgili kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, DMO tarafından bu doğrultuda hazırlanmış olan Politika'ya uygun olarak gerçekleştirilir.

1.2 Kapsam

İlgili sıfatıyla kişisel verisi işlenen çalışanlar/çalışan adayları, stajyerler, müşteriler (müşteri kurum çalışanı/irtibat kişisi/satın alma sorumlusu/temsilcisi/yetkilisi/harcama yetkilisi), tedarikçiler (istekli çalışan/temsilcisi/yetkilisi ile tedarikçi çalışan/temsilcisi/yetkilisi, eğitmen vb.), ziyaretçiler, bilgi/belge talebinde bulunanlar (gerçek kişiler ile tüzel kişilerin temsilcileri), öğrenciler/öğrenci adayları ve velilere ait kişisel veriler bu Politika kapsamında olup DMO'nun sahip olduğu ya da DMO tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 Kısaltmalar ve Tanımlar

Bu Belge'de geçen;

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	: Devlet Malzeme Ofisi Genel Müdürlüğü personelini,
DMO	: Devlet Malzeme Ofisi Genel Müdürlüğü'nü
EBYS	: Elektronik Belge Yönetim Sistemi'ni,
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,

- Hizmet Sağlayıcı** : Kişisel Verileri Koruma Kurumu ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişiyi,
- 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 Kanunu'nu,
- 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 ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, 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,
- Komisyon** : DMO Kişisel Verileri Koruma Komisyonu'nu,
- Kurul** : Kişisel Verileri Koruma Kurulu'nu,
- Kurum** : Kişisel Verileri Koruma Kurumu'nu,

- 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** : 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** : DMO Kişisel Veri Saklama ve İmha Politikası'nı,
- Veri İşleyen** : Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişiyi,
- Veri Kayıt Sistemi** : Kişisel verilerin belirli ölçütlere göre yapılandırılarak işlendiği kayıt sistemini,
- Veri Sorumlusu** : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında 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, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini,
- VERBİS** : Veri Sorumluları Sicil Bilgi Sistemi'ni,
- Yönetmelik** : 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i,

ifade eder.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

DMO'nun 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 saklanması 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 saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama ve İmha Süreçleri Görev Dağılımı

UNVAN	BİRİM	GÖREV
Genel Müdür Yardımcısı (Veri Sorumlusu Temsilcisi)	Devlet Malzeme Ofisi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
DMO Kişisel Verileri Koruma Komisyonu	Devlet Malzeme Ofisi	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Strateji Geliştirme Daire Başkanı	Strateji Geliştirme Daire Başkanlığı	Politika'nın uygulanmasının takibi ve uygulama sonuçlarının raporlanmasından sorumludur.
Bilgi İşlem Daire Başkanı	Bilgi İşlem Daire Başkanlığı	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve elektronik ortamdaki kişisel verilerin imha süreçlerinin takibinden sorumludur.
Destek Hizmetleri Daire Başkanı	Destek Hizmetleri Daire Başkanlığı	Politika'nın uygulanmasında ihtiyaç duyulan idari çözümlerin sunulmasından ve fiziksel ortamdaki kişisel verilerin imha süreçlerinin takibinden sorumludur.
Birim Amirleri	Merkez ve Taşra Birimleri	Görevlerine uygun olarak Politika'nın yürütülmesinden ve fiziksel ortamdaki kişisel verilerin imha süreçlerinin takibinden sorumludur.

3. KAYIT ORTAMLARI

Kişisel veriler, DMO tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
<ul style="list-style-type: none"> ➤ Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) ➤ Yazılımlar (ofis yazılımları, portal, EBYS, VERBİS.) ➤ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.) ➤ Kişisel bilgisayarlar (Masaüstü, dizüstü) ➤ Mobil cihazlar (telefon, tablet vb.) ➤ Optik diskler (CD, DVD vb.) ➤ Çıkarılabilir bellekler (USB, Hafıza Kart vb.) ➤ Yazıcı, tarayıcı, fotokopi makinesi 	<ul style="list-style-type: none"> ➤ Kâğıt ➤ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ➤ Yazılı, basılı, görsel ortamlar

4. SAKLAMA VE İMHA İLİŞKİN AÇIKLAMALAR

DMO tarafından; çalışanlar/çalışan adayları, stajyerler, müşteriler (müşteri kurum çalışanı/irtibat kişisi/satın alma sorumlusu/temsilcisi/yetkilisi/harcama yetkilisi), tedarikçiler (istekli çalışan/temsilcisi/yetkilisi ile tedarikçi çalışan/temsilcisi/yetkilisi, eğitmen vb.), ziyaretçiler, bilgi/belge talebinde bulunanlar (gerçek kişiler ile tüzel kişilerin temsilcileri), öğrenciler/öğrenci adayları ve velilere ait kişisel veriler Kanun'a uygun olarak saklanır ve imha edilir.

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

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 işleme şartları* sayılmıştır.

Buna göre, DMO faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

DMO'da 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 Kanunu,
 - ◆ 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
 - ◆ 4982 Sayılı Bilgi Edinme Kanunu,
 - ◆ 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
 - ◆ 4857 sayılı İş Kanunu,
 - ◆ 2547 sayılı Yükseköğretim Kanunu,
 - ◆ 5434 sayılı Emekli Sandığı 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,
- çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

DMO, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- ◆ Acil Durum Yönetimi Süreçlerinin Yürütülmesi,
- ◆ Bilgi Güvenliği Süreçlerinin Yürütülmesi,
- ◆ Çalışan Adayı / Stajyer / Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi
- ◆ Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi,
- ◆ Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi,
- ◆ Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi,
- ◆ Denetim / Etik Faaliyetlerinin Yürütülmesi
- ◆ Eğitim Faaliyetlerinin Yürütülmesi,
- ◆ Erişim Yetkilerinin Yürütülmesi,

- ◆ Faaliyetlerin Mevzuata Uygun Yürütülmesi,
- ◆ Finans ve Muhasebe İşlerinin Yürütülmesi,
- ◆ Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi,
- ◆ Fiziksel Mekân Güvenliğinin Temini,
- ◆ Görevlendirme Süreçlerinin Yürütülmesi,
- ◆ Hukuki 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
- ◆ Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi,
- ◆ Organizasyon ve Etkinlik Yönetimi
- ◆ Performans Değerlendirme Süreçlerinin Yürütülmesi,
- ◆ Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi,
- ◆ Risk Yönetimi Süreçlerinin Yürütülmesi,
- ◆ Saklama ve Arşiv Faaliyetlerinin Yürütülmesi,
- ◆ Sosyal Sorumluluk ve Sivil Toplum Aktivitelerinin Yürütülmesi,
- ◆ Sözleşme Süreçlerinin Yürütülmesi,
- ◆ Talep / Şikâyetlerin Takibi,
- ◆ Taşınır Mal ve Kaynakların Güvenliğinin Temini,
- ◆ Ücret Politikasının Yürütülmesi,
- ◆ Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi,

- ◆ Veri Sorumlusu Operasyonlarının Güvenliğinin Temini,
- ◆ Yatırım Süreçlerinin Yürütülmesi,
- ◆ Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi,
- ◆ Yönetim Faaliyetlerinin Yürütülmesi,
- ◆ Ziyaretçi Kayıtlarının Oluşturulması ve Takibi,
- ◆ Çalışanların İSG Sertifikasyon İşlemlerinin Yürütülmesi,
- ◆ Doğabilecek Uyuşmazlıklarda Delil Olarak Kullanılması,
- ◆ İstatistiksel Amaçlarla Katılımcı Sayısının Belirlenmesi,
- ◆ Teknik Şartnameye Uygun Olmayan Malzeme Alımının Önlenmesi,
- ◆ Toplantı ile İlgili Bilgi Sunulması,
- ◆ Toplantıya Katılımın Teyidi.

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,
- ◆ Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun DMO tarafından kabul edilmesi,
- ◆ DMO'nun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurum'a şikâyetle 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, DMO 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 Kanunun 12 nci maddesi ile 6 ncı maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde DMO tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

DMO tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- ◆ 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.
- ◆ Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- ◆ Erişim logları düzenli olarak tutulmaktadır.
- ◆ 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 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.
- ◆ Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- ◆ 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.
- ◆ Bilgi sistemleri güncel halde tutulmaktadır.
- ◆ Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmektedir.
- ◆ Hukuka aykırı işleme tespiti halinde ilgili kişiye ve kurula bildirmek için bir sistem ve altyapı oluşturulmaktadır.
- ◆ Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

5.2 İdari Tedbirler

DMO tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- ◆ Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- ◆ Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- ◆ Gizlilik taahhütnameleri yapılmaktadır. Ayrıca görevli personel bilgilerin gizliliği konusunda bilgilendirilmektedir.
- ◆ Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- ◆ İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- ◆ Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta Belgeler kilitli dolaplarda muhafaza edilmektedir.
- ◆ Kanun kapsamındaki ilgili taleplerinin yönetilmesine yönelik süreç ve alt süreçler tanımlanmış ve haritalandırılmıştır.
- ◆ Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- ◆ Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır,
- ◆ Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- ◆ Kişisel veri işleme envanteri oluşturulmuştur.
- ◆ Kişisel veriler mümkün olduğunca azaltılmaktadır.
- ◆ Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- ◆ Mevcut risk ve tehditler belirlenmiştir.
- ◆ Ayrıca;

KAYSİS Hizmet Envanteri ve Devlet Teşkilatı Merkezi Kayıt Sistemine sorumlu personel bilgisi tanımlanırken Dijital Dönüşüm Ofisi Başkanlığı tarafından KAYSİS'e veri girişi yapacak personelin ve yetkilerinin tanımlanması prosedürleri uygulanmaktadır.

TBMM KİT Komisyonu Toplantıları için katılımcı bilgisi paylaşılırken anılan Başkanlıkça belirtilen hazırlama ve gönderim kuralları doğrultusunda işlem yapılmaktadır.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, DMO tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir. İmha işlemleri; kişisel verinin türü ve verinin kaydedildiği ortama göre farklı şekillerde gerçekleştirilir.

İmhanın fiilen gerçekleştirilmesinden sorumlu birim "uygulama sorumlusu", imha sürecinin yürütülmesinden sorumlu olan birim ise "genel sorumlu" olarak adlandırılır. Genel sorumlu;

periyodik ya da ilgili kişi başvurusu çerçevesinde gerçekleştirilen imha işleminin takibi ve işlem sonucunun raporlanmasından sorumludur.

Genel sorumlu, imha işleminin kurum genelinde ortaklaşa ya da ilgili uygulama birimlerinde ayrı ayrı gerçekleştirilmesine karar verebilir; Politika'da belirtilen periyodik imha sürelerine uygun olarak takvime bağlayabilir.

6.1 Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

DMO'da kişisel verilerin silinmesinde Tablo-3'te verilen yöntemler uygulanır.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Silme Uygulamasının Şekli	Uygulama Sorumlusu	Genel Sorumlu
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.	Bilgi İşlem Daire Başkanlığı	Bilgi İşlem Daire Başkanlığı
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.	Veri Tabanını Yöneten Birim	Bilgi İşlem Daire Başkanlığı
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.	Fiziki Belgeyi Tutan Birim	Destek Hizmetleri Daire Başkanlığı
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.	Bilgi İşlem Daire Başkanlığı	Bilgi İşlem Daire Başkanlığı

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

DMO'da kişisel verilerin yok edilmesinde Tablo-4'te verilen yöntemler uygulanır.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Yok Etme Uygulamasının Şekli	Uygulama Sorumlusu	Genel Sorumlu
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.	Fiziki Belgeyi Tutan Birim	Destek Hizmetleri Daire Başkanlığı
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 değerinde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.	Bilgi İşlem Daire Başkanlığı	Bilgi İşlem Daire Başkanlığı

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.

DMO tarafından işlenen kişisel verilerin saklama süresi sonunda silme veya yok etme yöntemleriyle imha edilmesi öncelikli olarak öngörüldüğünden anonim hale getirilmesine yönelik başkaca bir yöntem tercih edilmemiştir.

7. SAKLAMA VE PERİYODİK İMHA SÜRELERİ

DMO tarafından işlenen kişisel verilere ilişkin saklama sürelerinin yer aldığı belge ve dijital ortamlar aşağıda sayılmaktadır.

- ◆ Tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde yer alır.
- ◆ Veri kategorileri bazında saklama süreleri VERBİS'te mevcuttur.
- ◆ Süreç ve faaliyetler bazında saklama süreleri ise Tablo-5 Kişisel Veri Saklama Süreleri Tablosunda yer almaktadır.

Periyodik imha işlemi güvenlik kamerası kayıtları hariç diğer kişisel veriler için her yıl Ocak ve Temmuz aylarında gerçekleştirilir. Güvenlik kamerası kayıtları ise kayıt tarihinin dolduğu gün itibarıyla otomatik olarak silinir.

8. POLİTİKA'NIN YAYINLANMASI, YÜRÜRLÜĞE GİRMESİ VE GÜNCELLENMESİ

Politika, Yönetim Kurulunca kabulünü müteakip yürürlüğe girer ve kurumsal internet sayfasında yayınlanarak ilgililerin erişimine sunulur.

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümleri güncellenebilir; kabul edildiği usulde yürürlükten kaldırılabilir.

Tablo 5: Süreç Bazında Saklama Süreleri Tablosu

Süreç	Saklama Süresi	Süre Başlangıcı	Süreç	Saklama Süresi	Süre Başlangıcı
Personel Özlük İşlemleri	101 yıl	Personelin kurumla ilişkisini sonlandırması	Hukuk İşlemleri	101 yıl	Son işlem tarihi
İnsan Kaynakları Süreçleri (Mesleki Eğitim, Staj)	10 yıl	Son işlem tarihi	Müşteri Kurum İhtiyacı Mal ve Hizmetlerin Temini (Ön inceleme, Satınalma, Satış, Faturalama, Tedarikçi Ödemeleri, vb.)	10 yıl	İşlemin her ayrı aşaması için son işlem tarihi
İnsan Kaynakları Süreçleri (Hizmet içi Eğitim)	1 yıl	Son işlem tarihi			
İş Sağlığı ve Güvenliği Kapsamındaki İşlemler (Laboratuvar Müdürlüğü Personeli İşe Giriş/Periyodik Muayene)	40 yıl	Muayene tarihi	Muhasebe Süreçleri (Maaş Ödemesi)	10 yıl	Son işlem tarihi
			Güvenlik Personeli Özlük Dosyası Oluş.	10 yıl	İşlem tarihi
İş Sağlığı ve Güvenliği Kapsamındaki Diğer İşlemler (Mesleki Yeterlilik, Eğitim ve Sertifikasyon, İş Kazası Tutanağı, İşe Giriş/Periyodik Muayene) vb.)	15 yıl	Son işlem tarihi	Kreş Öğrenci Kabul İşlemleri	10 yıl	Son işlem tarihi
			Kreş Kayıt Başvuruları, Kreş Görsel ve İhtisat Kayıtları	5 yıl	Başvuru dönemi sonu
Bilgi İşlem Süreçleri (ERP Tedarikçi ve Müşteri Kaydı, Kullanıcı Hesabı Tanımlama, Güvenlik İşlemleri vb.)	10 yıl	İşlem tarihi	Strateji Geliştirme Faaliyetleri (CİMER, Üst Kurumlar ve Yönettikleri Bilgi Yönetim Sistemlerine Veri Girişi, İşbirliği Protokolleri, Görevlendirme ve Kullanıcı Tanımlama hariç İKRY Faaliyetleri)	10 yıl	İşlem tarihi
Bilgi İşlem Süreçleri (Acil Durumda Erişilecek Çalışanlar Listesi, Tedarikçi İletişim Listesi, Bilgi Alışverişi Protokolü)	3 yıl	İşlem tarihi	İç Kontrol ve Risk Yönetimi Faaliyetleri (Görevlendirme ve Kullanıcı Tanımlamaları)	2 yıl	Görevlendirme tarihi
Kurumsal Duyuruların Yayınlanması, Sosyal Medya Paylaşımları	10 yıl	Yayın tarihi	Ziyaretçi ve Toplantı Katılımcılarının Kaydı	2 yıl	Etkinlik tarihi
Personel Devam Sistemi	2 yıl	Kayıt tarihi	Çağrı Merkezi Kayıtları	2 yıl	Görüşme tarihi
Güvenlik Kamera Kayıtları	29 gün	Kayıt tarihi			