# T.C. KÜLTÜR VE TURİZM BAKANLIĞI
# DÖNER SERMAYE İŞLETMESİ MERKEZ MÜDÜRLÜĞÜ

# KİŞİSEL VERİLERİ
# SAKLAMA VE İMHA
# POLİTİKASI

| | |
|---|---|
| Doküman İçeriği | **Bu politikanın amacı, T.C. KÜLTÜR VE TURİZM BAKANLIĞI DÖNER SERMAYE İŞLETMESİ MERKEZ MÜDÜRLÜĞÜ tarafından, kişisel verilerin saklanması ve imhasına ilişkin yöntem ve süreçlere ilişkin esasları belirlemektir.** |
| Versiyon No | 2025 – 1.0 |
| Dayanak | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| Onaylayan | T.C. KÜLTÜR VE TURİZM BAKANLIĞI DÖNER SERMAYE İŞLETMESİ MERKEZ MÜDÜRLÜĞÜ |

## İÇİNDEKİLER

# T.C. KÜLTÜR VE TURİZM BAKANLIĞI DÖNER SERMAYE İŞLETMESİ MERKEZ MÜDÜRLÜĞÜ VERİ SAKLAMA VE İMHA POLİTİKASI

## 1. AMAÇ

Kişisel Veri Saklama ve İmha Politikası ("Politika") T.C. KÜLTÜR VE TURİZM BAKANLIĞI DÖNER SERMAYE İŞLETMESİ MERKEZ MÜDÜRLÜĞÜ 'nun ("Kurum") veri sorumlusu sıfatıyla işlediği kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

## 2. KAPSAM

Bu Politika, Kurum tarafından kişisel verileri işlenen tüm gerçek kişilere ilişkin kişisel verileri kapsar ve Kurum'un sahip olduğu ya da Kurum tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları hakkında ve tüm veri işleme faaliyetlerinde bu Politika uygulanır. İşbu Politika, Kurum'un faaliyetleri çerçevesinde düzenlenmiş, asılları ve kopyaları dahil tüm elektronik ve elektronik olmayan ortamlarda bulunan belgeleri kapsar.

## 3. HUKUKİ DAYANAK VE YÜKÜMLÜLÜK

Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve ilgili diğer mevzuat gereğince, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in ("Yönetmelik") 5. maddesine dayanarak ve veri sorumlusu Kurumun kişisel veri işleme envanterine uygun olarak hazırlanmıştır.

Bu kapsamda, çalışanların, çalışan adaylarının, vatandaşların ve herhangi bir nedenle Kurum nezdinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri, Kişisel Verilerin Korunması ve İşlenmesi Politikası ile işbu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara ve ilgili diğer mevzuata uygun olarak yönetilmektedir.

Kurumun bütün çalışanları işbu Politika'yı tam olarak anlamak ve uygulamakla yükümlüdür. Politikanın uygulanmasından, ilgili departman yöneticileri, İrtibat Kişisi, Kişisel Verilerin Korunması Komitesi sorumludur.

## 4. TANIMLAR

Bu Politika kapsamında kullanılan terimler aşağıdaki anlamları ifade eder.

| | |
|---|---|
| **Aktif Kayıtlar** | Kurum'un işleyişi, idaresi ve yönetimi için halen kullanılmakta olan kayıtlardır. |
| **Aktif Olmayan Kayıtlar** | Kullanılmayan; ancak işlenmesi sonradan gerekebileceği için saklama süreleri sona ermemiş kayıtlardır. |
| **Elektronik Ortam** | Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlardır. |
| **Elektronik Olmayan Ortam** | Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlardır. |
| **Fiziksel Yok Etme** | Optik veya manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesidir. |
| **İkincil Mevzuat** | Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüşü ifade eder. |
| **İmha** | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir. |
| **Karartma/Maskeleme** | Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması, buzlanması, yıldızlanması gibi işlemleridir. |
| **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 ortamdır. |
| **Periyodik İmha** | Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda bu Politikada belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir. |
| **Silme** | Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. |
| **Veri Kayıt Sistemi** | Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. |
| **VERBİS** | Veri Sorumluları Sicil Bilgi Sistemidir. |

Burada yer verilmeyen terimlerin, Kanun, Yönetmelik ve diğer ikincil mevzuatta yer alan anlamda kullanıldığı kabul edilir.

## 5. SORUMLULUK VE GÖREV DAĞILIMI

Kurum'un tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının 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 tanımları aşağıdaki şekildedir:

| ÜNVANI | GÖREVİ |
|---|---|
| **Veri Sorumlusu İrtibat Kişisi** | Kurum nezdinde Politika'nın yürütülmesinden sorumludur. |
| **Kişisel Verilerin Korunması Komitesi** | Politika'nın hazırlanması, yürütülmesi, yayınlanması, geliştirilmesi ve güncellenmesinden sorumludur. |
| **Birimler** | Görev alanı çerçevesinde Politika'nın uygulanmasından sorumludur. |

## 6. KAYIT ORTAMLARI

Kurum bünyesinde kişisel verilerin kayıt ortamları aşağıda belirtilmiştir:

### 6.1. Elektronik Kayıt Ortamları

Ses kayıtları, fotoğraflar, videolar ve görsel ve işitsel ortamlar dahil birçok ortamda yer alan kişisel veriler; doğru, güncel ve kişisel verileri işlemesi gereken kişilerce erişilebilir olacak şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli elektronik ortamlarda saklanabilir.

Elektronik ortamlar, sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.), yazılımlar (ofis yazılımları, portal vb.), bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit, engelleme, günlük kayıt dosyası, anti virüs vb.), yedekleme kartuşları, kişisel bilgisayarlar (masaüstü, dizüstü), mobil cihazlar (telefon, tablet vb.), optik diskler (CD, DVD vb.), çıkartılabilir bellekler (USB, hafıza kartı vb.) ve yazıcı, tarayıcı, fotokopi makinesi vb. diğer elektronik veri kayıt ortamlarıdır.

### 6.2. Elektronik Olmayan Kayıt Ortamları

- Yazılı, basılı ortamlar ve manuel veri kayıt sistemleri gibi elektronik olmayan kayıt ortamları, fiziksel kayıtlar, kağıt üzerindeki kayıtlar, fotoğraflar ve sözleşmeler gibi kağıt, mikro fiş ve benzeri ortamlarda bulunan kayıtlardan oluşur.
- Aktif kayıtlar ve kolayca erişilmesi gereken kayıtlar Kurum'un ofis ortamında depolanabilir.
- Aktif olmayan kayıtlar Kurum'un arşivlerine gönderilir.

## 7. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER

### 7.1. Saklama ve İmhaya İlişkin Hukuki Sebepler

Kurum kişisel verileri aşağıdaki şartlar gereğince işlemekte, saklamakta ve ilgili şartların gerçekleşmesi durumunda imha yöntemlerini kullanarak silmekte, yok etmekte veya anonim hale getirmektedir:

- Bir Sözleşmenin Kurulması Veya İfasıyla Doğudan Doğruya İlgili Olması Kaydıyla Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması,
- İlgili Kişinin Temek Hak Ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması,
- Kanunlarda Açıkça Öngörülmesi,
- Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması
- İstihdam, İş Sağlığı Ve Güvenliği, Sosyal Güvenlik, Sosyal Hizmetler Ve Sosyal Yardım Alanlarındaki Hukuki Yükümlülüklerin Yerine Getirilmesi İçin Zorunlu Olması

### 7.2. Saklamayı Gerektiren Amaçlar

Kurum, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklamaktadır:

- Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
- Faaliyetlerin Mevzuata Uygun Yürütülmesi

- İletişim Faaliyetlerinin Yürütülmesi
- Fiziksel Mekan Güvenliğinin Temini
- Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi
- Sözleşme Süreçlerinin Yürütülmesi
- Taşınır Mal Ve Kaynakların Güvenliğinin Temini
- İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- İş Sağlığı Ve Güvenliği Faaliyetlerinin Yürütülmesi
- Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- Hukuk İşlerinin Takibi Ve Yürütülmesi
- Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- Görevlendirme Süreçlerinin Yürütülmesi
- Talep / Şikayetlerin Takibi

## 7.3. İmhayı Gerektiren Sebepler

Kişisel veriler aşağıda belirtilen hallerde Kurum tarafından resen veya ilgili kişinin talebi üzerine imha yöntemleri kullanılarak silinir, yok edilir veya anonim hale getirilir:

- 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 Kurum tarafından kabul edilmesi,
- Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verilen cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kuruluna şikayette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

## 8. İDARİ VE TEKNİK TEDBİRLER

- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gizlilik taahhütnameleri yapılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- 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 veriler mümkün olduğunca azaltılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleme önlemi uygulanmaktadır.

- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kişisel veri güvenliğinin takibi yapılmaktadır.
- 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 veriler mümkün olduğunca azaltılmaktadır.
- 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 veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- Şifreleme yapılmaktadır.
- Sızma testi uygulanmaktadır.
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

## 9. SAKLAMA VE PERİYODİK İMHA SÜRELERİ

Kurum, kişisel verileri ilgili mevzuatta belirtilen süre boyunca saklamaktadır. Mevzuatta kişisel verilerin saklanmasına ilişkin herhangi bir süre öngörülmemiş ise, kişisel veriler amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi gereğince işlenmesinin gerektiği ya da işlendikleri amaç için gerekli olan süre kadar işlenmektedir. Bu çerçevede öncelikle ilgili mevzuatta kişisel

verinin saklanması için bir süre öngörülüp öngörülmediği tespit edilmekte, mevzuatta bir süre öngörülmüşse bu süre kadar, yoksa kişisel verinin işlendiği amaç için gereken süre kadar ilgili kişisel veri saklanmaktadır. Saklama sürelerinin sonunda kişisel veri, periyodik imha sürelerine veya veri sahibinin başvurusuna göre ve belirlenmiş olan imha yöntemlerine göre silinmekte, yok edilmekte ya da anonim hale getirilmektedir.

Kurum tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçler ve departmanlara 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 kayıtta yer alır.

Kişisel verilerin saklanma ve imha süreleri aşağıdaki tabloda gösterilmiştir.

| VERİ KATEGORİSİ | SAKLAMA SÜRESİ | İMHA SÜRESİ |
|---|---|---|
| **Kimlik** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **İletişim** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Mesleki Deneyim** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Özlük** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Finans** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Görsel ve İşitsel Kayıtlar** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Ceza Mahkumiyeti ve Güvenlik Tedbirleri** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Sağlık Bilgileri** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Hukuki İşlem** | 101 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **Diğer(İmza)** | 10 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

| | | |
|---|---|---|
| **Fiziksel Mekan Güvenliği** | 30 Gün | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| **İşlem Güvenliği** | 1 Yıl | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

Kurum, periyodik imha süresini 6 ay olarak belirlemiştir. Politika bağlamında, saklama takvimi kaydın oluşturulduğu takvim yılının sonunda başlar. Saklama süresi dolmuş kayıtlar Kurumda her yıl Haziran ve Aralık aylarında olmak üzere iki kez gerçekleştirilen periyodik imhaya tabi tutulur. Bir kişisel verinin işleme amacının ortadan kalktığı tarih bu iki dönemden hangisine daha yakınsa o dönemde İmha edilir.

## 10. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

Kurum tarafından KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenen kişisel veriler, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, Kurum tarafından resen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak silinerek, yok edilerek veya anonim hale getirilerek imha edilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde;

- İlgili mevzuatta kişisel verilerin işlenmesinde uyulması gerekli görülen genel ilkelere,
- Veri sorumlularının veri güvenliğine ilişkin yükümlülükleri kapsamında alınması gereken idari ve teknik tedbirlere,
- Kişisel Verileri Koruma Kurulu kararlarına,
- Kişisel verilerin saklanması ve imhası politikasına uygun hareket edilmektedir.

### 10.1. Kişisel Verilerin Silinmesi

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

Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri alır.

Silme işlemi için öncelikle silme işlemine konu teşkil edecek kişisel veriler belirlenmekte ve her bir kişisel veri için ilgili kullanıcılar tespit edilmektedir. Bunu takiben ilgili

kullanıcıların erişim, geri getirme ve tekrar kullanma gibi yetkileri ve kullandıkları yöntemler tespit edilerek işbu yetkiler ortadan kaldırılmaktadır.

Verilerin silinmesi ile ilgili aşağıdaki yöntemler kullanılır:

**a) Hizmet Olarak Uygulama Türü Bulut Çözümleri**

Bulut sisteminde veriler silme komutu verilerek silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilir.

**b) Kağıt Ortamında Bulunan Kişisel Veriler**

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.

**c) Merkezi Sunucuda Yer Alan Kişisel Veriler**

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması sağlanır. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına da dikkat edilir.

**d) Taşınabilir Medyada Bulunan Kişisel Veriler**

Taşınabilir medyalarda taşınan veriler şifreli olarak saklanmakta ve bu araçlarda gizli seviyede hiçbir veri taşınmamaktadır. Taşınabilir ortamda olan kişisel veriler, söz konusu donanıma uygun yazılımlar ile silinir.

**e) Veri Tabanları**

Kişisel verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

## 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. Kurum, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri alır.

Kişisel veriler, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilir.

**a) Yerel Sistemler**

Yerel sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılır.

- **De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
- **Fiziksel Yok Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi sağlanır.
- **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

**b) Çevresel Sistemler**

Ortam türüne bağlı olarak kullanılan yok etme yöntemleri aşağıda yer almaktadır:

- **Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanlarının, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da Yukarıda 'Yerel Sistemler' için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.

● **Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yukarıda 'Yerel Sistemler' için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi sağlanır.

● **Veri kayıt ortamı çıkartılabilir olan yazıcı çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre Yukarıda 'Yerel Sistemler' için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

● **Veri kayıt ortamı sabit olan yazıcı gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Yukarıda 'Yerel Sistemler' için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi sağlanır.

● **Bulut Sistemler:** Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi sağlanır.

## 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 alıcı grupları 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. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiyi işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek

bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Kurum, kişisel verilerin silinmesi veya yok edilmesi yerine anonim hale getirilmesi sürecinde gerekli her türlü teknik ve idari tedbirleri alır. Kişisel verilerin anonim hale getirilmesi, Kişisel Verilerin Silinmesi Yok edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte belirtilen esaslara ve Kişisel Verileri Koruma Kurumunun konuya ilişkin yayınladığı rehberdeki yöntemlere uygun olarak yapılır.

Kurum, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmek için aşağıdaki şartların yerine getirilmesini arar ve işbu şartların yerine getirilmiş olmasını sağlar:

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulmaması,
- Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturmaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

## 11. POLİTİKANIN YÜRÜRLÜĞÜ

Kurum tarafından kişisel verilerin saklanması ve imhasında uygulanmak üzere yürürlükteki mevzuatla uyumlu olarak hazırlanan bu Politika, Kurum görevlendirme ve kararları ile yürürlüğe konulmuştur.

Bu politika Kurumun internet sayfasında yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur. Bu Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.