

T.C.  
AFYONKARAHİSAR SAĞLIK BİLİMLERİ ÜNİVERSİTESİ  
YÖNETİM KURULU KARARI

TOPLANTI SAYISI : 16

KARAR TARİHİ : 29.07.2024

**KARAR 2024/122**

Üniversitemiz Bilgi İşlem Daire Başkanlığının 17.07.2024 tarihli ve 266407 sayılı yazısı okunarak değerlendirildi. Yapılan değerlendirme sonucunda; “Afyonkarahisar Sağlık Bilimleri Üniversitesi Kişisel Veri Saklama ve İmha Politikası”nın aşağıdaki şekliyle kabulüne katılanların oy birliği ile karar verildi.

**AFYONKARAHİSAR SAĞLIK BİLİMLERİ ÜNİVERSİTESİ  
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

**1. AMAÇ**

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), 6698 Sayılı Kişisel Verileri Koruma Kanunu (KVK Kanunu) ve ilgili mevzuat esas alınarak **Afyonkarahisar Sağlık Bilimleri Üniversitesi** (“Üniversite” veya “AFSÜ”) tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

**Tanımlar**

**Ağ:** Birden fazla bilgisayarın bilgi paylaşımı, yazılım ve donanım paylaşımı, merkezi yönetim ve destek kolaylığı gibi çeşitli sebeplerle birbirine bağlandığı yapıdır.

**Ağ cihazları:** Ağ yapılarını oluşturmak için kullanılan cihazlardır.

**Anonim hale getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

**Bilgi güvenliği:** Bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme ve ortadan kaldırılmasını önlemek anlamına gelir.

**AFSÜ/Üniversite:** Afyonkarahisar Sağlık Bilimleri Üniversitesi’ni ifade eder.

**Bulut sistemi:** Bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır.

**Doğrudan tanımlayıcılar:** Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

**Dolaylı tanımlayıcılar:** Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

**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 gerçek veya tüzel kişileri,

**İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

**KVKK:** 24.03.2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nu,

**KVK Komisyonu:** Afyonkarahisar Sağlık Bilimleri Üniversitesi KVK Komisyonu'nu,

**Karartma:** Kişisel verilerin bütünü, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması (flu hale getirilmesi) gibi işlemleri,

**Kayıt ortamı:** Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

**Kişisel veri saklama ve imha politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı ifade eder.

**Korelasyon:** İki değişken arasındaki ilişkiyi değerlendirme yöntemidir.

**Kurul:** Kişisel Verileri Koruma Kurulu'dur.

**Log:** Bilişim sistemlerinde yapılan işlemlere ilişkin elektronik ortamdaki izlerdir.

**Manyetik medya:** Manyetik veri ortamlarıdır.

**Maskeme:** Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde boyanması ve yıldızlanması (\*) gibi işlemleri ifade eder.

**Optik medya:** İçeriği dijital biçimde tutan ve bir lazer tarafından yazılan ve okunan depolama ortamlarıdır.

**Veri kayıt sistemi:** Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

## 2. KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından aşağıdaki tabloda listelenen ortamlarda başta KVK Kanunu hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır.

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
Sunucular (Etki alanı (LDAP), yedekleme, e-posta, veri tabanı, web vb.)	✓ Kâğıt
✓ Yazılımlar (ofis yazılımları, portal vd. otomasyonlar)	✓ Manuel veri kayıt sistemleri (formlar vb.)
✓ Bilgi güvenliği araçları (günlük kayıt dosyası, antivirüs vb.)	✓ Yazılı, basılı, görsel ortamlar
✓ Bilgisayarlar (masaüstü, dizüstü)	✓ Ofis içi alan
✓ Dosya paylaşımları	✓ Arşiv
✓ Manyetik diskler (harddisk vb.)	
✓ Mobil cihazlar (telefon, tablet vb.)	
✓ Optik diskler (CD, DVD vb.)	
✓ Taşınabilir bellekler (USB, Hafıza Kartı vb.)	
✓ Yazıcı, tarayıcı, fotokopi makinesi	

### 3. KİŞİSEL VERİLERİN SAKLANMASI

#### 3.1. Kişisel Verilerin Saklandığı Ortamlar

Afyonkarahisar Sağlık Bilimleri Üniversitesi tamamen otomatik veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlediği kişisel verileri, hukuka uygun olarak 2. Bölüm 'de belirtilen elektronik ve elektronik olmayan ortamlarda saklamaktadır.

#### 3.2. Kişisel Verilerin Saklandığı Ortamların Güvenliğinin Sağlanması

Afyonkarahisar Sağlık Bilimleri Üniversitesi, kişisel verilerin saklandığı elektronik veya elektronik olmayan ortamların güvenliğini sağlamak için teknolojik imkânlar ve uygulama maliyetleri doğrultusunda gerekli teknik ve idari tedbirleri almaktadır.

##### 3.2.1. Teknik Tedbirler

Üniversitemizde uygulanan veri güvenliği tedbirleri aşağıda belirtilmiştir:

- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Kullanılması halinde bulutta depolanan kişisel verilerin güvenliğinin sağlanması.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Erişim logları düzenli olarak tutulmaktadır.
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
- Gerekğinde veri maskeleyme önlemi uygulanmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmaktadır.İlgili 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.

- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- 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.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

#### **4. KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN SEBEPLER**

Kişisel veriler Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından;

- ✓ Afyonkarahisar Sağlık Bilimleri Üniversitesi'nin doğmuş ya da doğabilecek yasal sorumluluklarını yerine getirebilmesi amacı ile ve kanunlarda öngörülen ölçülere ve/veya emredilen sürelerle uygun olarak,
- ✓ Silinmesi ve/veya anonimleştirilmesi öngörülen veriler ise; iş sürekliliği, veri kaybının önlenmesi ve veri koruma amacıyla yedek/arşiv ve benzeri ortamlarda erişime hazır ("canlı") olmayan şekilde,
- ✓ Silme, yok etme veya anonimleştirme yolu ile imha edilecek verilerin saklama ve imha işlemleri ise işleme amacının ortadan kalkmasından itibaren derhal veya kamu kurumlarınca tabi olunan arşiv mevzuatına göre ilgili Komisyonların denetiminde gerçekleştirilir.

Afyonkarahisar Sağlık Bilimleri Üniversitesi faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler ilgili yasal mevzuat ve bağlayıcı düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

#### **5. KİŞİSEL VERİLERİN SİLİNMESİ**

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

##### **5.1. Kişisel Verilerin Silinmesi Süreci**

Afyonkarahisar Sağlık Bilimleri Üniversitesi'nde uygulanan kişisel veri silme süreci aşağıdaki gibidir:

- Silme işlemine konu edilecek kişisel veriler belirlenir.
- Söz konusu kişisel verinin tutulduğu ortamlar tespit edilir.
- KVK Komisyonunun yönlendirmesiyle, yetkili üst makam, verinin tutulduğu ortamların birim sorumlularını, ilgili verinin silinmesi konusunda talimatlandırır. Birim sorumluları, dijital ortamlarda, otomasyonlarda yetkili personel; fiziki ortamlarda ise birim "Ayıklama ve İmha Komisyon"larıdır.

- Kişisel verinin silme işlemleri gerçekleştirilir.
- Kişisel verilerin silindiğine dair tutanak tutulur.

## 5.2 Kayıt Ortamlarına Göre Silme Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir:

### a) Hizmet Olarak Uygulama Türü Bulut Çözümleri

Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından kullanılması durumunda bulut sisteminde bulunan veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken Afyonkarahisar Sağlık Bilimleri Üniversitesi ilgili kullanıcılarının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

### b) Kâğıt Ortamında Bulunan Kişisel Veriler

Kâğıt ortamında bulunan kişisel veriler Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin okunması mümkün olmayacak şekilde üzerinin çizilmesi/ boyanması şeklinde yapılır.

### c) Sunucu ve Bilgisayarlarda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından kaldırılması (silinmesi-erişimin engellenmesi) gerekir.

### ç) Taşınabilir Ortamda Bulunan Kişisel Veriler

Taşınabilir saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

### d) Veri Tabanları

Kişisel verilerin bulunduğu veri tabanı tablosundaki ilgili satır ve sütun (hücre)'lerin veri tabanı komutları ile silinmesi gerekir.

## 6. KİŞİSEL VERİLERİN YOK EDİLMESİ

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

### 6.1 Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

#### a) Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı Afyonkarahisar Sağlık Bilimleri Üniversitesi tarafından belirlenerek kullanılabilir.

**i) De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

**ii) Fiziksel Yok Etme:** İlgili verinin bulunduğu donanım/ medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. İlgili verinin bulunduğu

donanım/medyanın eritilmesi, yakılması, toz haline getirilmesi ya da bir metal öğütücüden geçirilmesi gibi işlemlerle verilerin erişilmez kılınması sağlanır.

**iii) Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir.

## **b) Çevresel Sistemler**

Afyonkarahisar Sağlık Bilimleri Üniversitesi veri kayıt ortam türüne bağlı olarak kullanılabilir yok etme yöntemleri aşağıda yer almaktadır:

**i) Ağ cihazları (switch, router vb.):** Söz konusu donanımlar içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. “a” bendinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle ilgili verinin bulunduğu donanım/medyanın yok edilmesi gerekir.

**ii) Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da **(a)** başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

**iii) Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. **(a)** başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

**iv) Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. **(a)** başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

**v) Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. **(a)** başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

## **c) Kâğıt Ortamları**

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre **(a)** başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

## **ç) Bulut Ortamı**

Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle Afyonkarahisar Sağlık Bilimleri Üniversitesi'nin hizmet aldığı/alacağı 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 gerekir.

## **d) Diğer Ortamlar**

Yukarıdaki ortamlara ek olarak Afyonkarahisar Sağlık Bilimleri Üniversitesi'nin arızalanan ya da bakıma gönderilen cihazlarında yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde

gerçekleştirilir:

- i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesinin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- ii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

## 7. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleyme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Kişisel verilerin anonim hale getirilmesi yöntemleri ve uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde detaylı olarak açıklanmıştır.

### 7.1 Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

#### 7.1.1 Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

- ✓ Değişkenleri Çıkartma
- ✓ Kayıtları Çıkartma
- ✓ Bölgesel Gizleme
- ✓ Alt ve Üst Sınır Kodlama
- ✓ Örnekleme

#### 7.1.2 Değer düzensizliği sağlayan anonim hale getirme şekilleri

Değer düzensizliği sağlayan yöntemlerle, yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma meydana getirilir. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

- ✓ Mikro Birleştirme

✓ Veri Değiş Tokuşu

✓ Gürültü Ekleme

✓ Tekrar Örnekleme

### 7.1.3 Anonim hale getirmeyi kuvvetlendirici istatistiksel yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

✓ K-Anonimlik

✓ L-Çeşitlilik

✓ T-Yakınlık

### 7.2 Anonimlik Güvencesi

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir. Bu şartların yerine getirilmiş olmasını veri sorumluları sağlamalıdır:

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

Bu riskler sebebiyle veri sorumlularının, anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değişikçe kontroller yapmaları ve anonimliğin korunduğundan emin olmaları gerekmektedir.

## 8. SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

KVKK Kanunu 4. maddesinde; işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiştir.

Kurumda, 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 Kanunu,
- 6361 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 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 çerçevesinde, Öngörülen saklama süreleri kadar saklanmaktadır.

## **9. VERİ SAKLAMA SÜRESİ VE İMHA SÜRECİ**

### **9.1 Saklama ve İmha Süresi**

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ayrıca 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; Kurumumuz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

### **9.2 Periyodik İmha**

Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; Afyonkarahisar Sağlık Bilimleri Üniversitesi işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Afyonkarahisar Sağlık Bilimleri Üniversitesi'nde kişisel verilerin saklama ve imha işlemleri, Kişisel Veri Envanterinde belirlenen sürelerde ve kamu kurumlarınca tabi olunan arşiv mevzuatına göre ilgili Komisyonların denetiminde gerçekleştirilir. Kişisel verilerin işleme şartlarını ortadan kaldıran hallerden herhangi birinin gerçekleşmesi durumunda bu kişisel verilere ilişkin kayıtlar için bir sonraki imha periyodunda imha işlemi gerçekleştirilir.

### **9.3 Talep Üzerine İmha Gerektiren Durumlar**

İlgili kişinin kanundan kaynaklı hakkını kullanarak yaptığı başvuruların uygun bulunması halinde veya Kişisel Verileri Koruma Kurumu'nun talimatına istinaden imha işlemi Kurum tarafından gerçekleştirilir.

Veri Sorumlusu, kendisine yapılan başvuruları, KVK Komisyonu ile "Talep Yönetim Süreci Talimatı" na göre yürütür.

### **9.4 İmha Yönteminin Belirlenmesi**

Kişisel Veri Envanterinde, imha edilecek kişisel verinin bulunduğu ortamın türü, kritikliği ve hassasiyetine göre Kişisel Verileri Koruma Kanununda belirtilen imha yöntemlerine göre imha türüne karar verilir.

### **9.5 İmhanın Gerçekleştirilmesi**

İmhası gerçekleştirilecek kişisel veriler,

- ✓ Belirlenen kayıtlar,
- ✓ Ekipler,
- ✓ Takvim ve
- ✓ Yöntem dikkate alınarak gerçekleştirilir.

Veri Sorumlusu, imha edilecek kişisel verileri, veri işleyen taraflara da bildirerek ilgili taraflarda bulunan kayıtların da imhasını sağlar ve kayıt altına alır.

## 10. SORUMLU KİŞİLER

Kişisel verilerin saklama, silme, anonim hale getirme ve imha etme süreçleri Afyonkarahisar Sağlık Bilimleri Üniversitesi KVK Komisyonu tarafından yürütülür.

## 11. GÖZDEN GEÇİRME VE ONAY TABLOSU

Açıklama	Kabul/Revizyon Tarih ve Numarası	Revizyon İçeriği
İlk yayın	.. tarihli ve .. sayılı Yönetim Kurulu Kararı	

ASLI GİBİDİR

Ziya Kutay ERŞEN  
Genel Sekreter