Revizyon No	Revizyon Tarihi	Sayfa No	Madde No	Revizyon İçeriği
00				İlk Yayın

1. AMAÇ

Gerçek kişilerin kişisel verilerinin Türkiye Cumhuriyeti Anayasası ve insan haklarına ilişkin ülkemizin tarafı olduğu Uluslararası Sözleşmeler ile 6698 Sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**") başta olmak üzere ilgili mevzuata uygun olarak işlenmesi ve işleme şartlarının tamamının ortadan kalkması durumunda silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemek amacıyla işbu politika hazırlanmıştır.

Faaliyetlerimiz sırasında edindiğimiz tüm kişisel verilere ilişkin verinin işlenmesi, saklanması, aktarılmasına ilişkin işlemleri Kişisel Verilerin İşlenmesi ve Korunması Politikasına ("**Politika**") göre gerçekleştirmekteyiz. Kişisel verilerin korunması ve kişisel verileri toplanan gerçek kişilerin temel hak ve hürriyetlerinin gözetilmesi kişisel verilerin işlenmesine ilişkin politikamızın temel prensibidir. Bu nedenle kişisel verinin işlendiği tüm faaliyetlerimizi, özel hayatın gizliliğinin korunması, haberleşmenin gizliliği, düşünce ve inanç özgürlüğü, etkili kanun yollarını kullanma haklarını gözeterek sürdürmekteyiz. Kişisel verilerin korunması için mevzuat ve güncel teknolojiye uygun şekilde ilgili verinin niteliğinin gerektirdiği tüm idari ve teknik koruma tedbirlerini almaktayız. İşbu Politika, ticari veya sosyal sorumluluk ve benzeri faaliyetlerimiz sırasında paylaşılan kişisel verilerin KVKK 'da anılan ilkeler çerçevesinde işlenmesi, saklanması, aktarılması ve silinmesi ya da anonim hale getirilmesine dair izlediğimiz yöntemleri açıklamaktadır.

TANIMLAR

Ağ : Birden fazla bilgisayarın bilgi paylaşımı, yazılım ve donanım paylaşımı, merkezi yönetim ve destek kolaylığı gibi çok çeşitli sebeplerden dolayı birbirine bağlandığı yapıya ağ denir.

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, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek anlamına gelir.

Bulut sistemi : Bulut sistemi, verilerin uzaktan korunması, yönetilmesi için kullanıcıların ağ üzerinden erişebildiği bir sistem modelidir.

DDos : Sisteme kaldırabileceğinden fazla yük yükleyerek cevap veremez hale getiren siber saldırıdır.

DDos Mitigator: DDos saldırısını engellemek üzere verilen hizmet

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 : 24.3.2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

Karartma :Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması 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,

Korelasyon : İki değişken arasındaki ilişkiyi değerlendirme yöntemidir.

Log : Bilgisayarlarda yapılan işlemin kaydedildiği belgelere denir

Maskeleme : Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,

Optik medya : Optik medyalar, içeriği dijital biçimde tutan ve bir lazer tarafından yazılan ve okunan depolama ortamlarıdır.

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Zeroday : Daha önceden bilinmeyen veya tespit edilmemiş ancak ciddi saldırılara yol açacak zafiyetler barındıran yazılım ve donanım kusurlarıdır.

2. KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler **İSTANBUL MARMARA EĞİTİM SAĞLIK KURUMLARI A.Ş.** (bundan böyle **"İSTANBUL MARMARA EĞİTİM KURUMLARI "** olarak ifade edilecektir) tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK 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, yedekleme, e-posta (Exchange), veri tabanı, web, dosya paylaşım, vb.) ✓ Yazılımlar (ofis yazılımları, portal, ERP, pdks) ✓ Bilgi güvenliği cihazları (güvenlik, günlük kayıt dosyası, antivirüs vb.) ✓ Kişisel bilgisayarlar (Masaüstü, dizüstü) ✓ Mobil cihazlar (telefon, tablet vb.) ✓ Optik diskler (CD, DVD vb.) ✓ Çıkartılabilir bellekler (USB, Hafıza Kart vb.) ✓ Yazıcı, tarayıcı, fotokopi makinesi	✓ Kâğıt ✓ Manuel veri kayıt sistemleri (anket formları, Ziyaretçi kayıt defteri) ✓ Yazılı, basılı, görsel ortamlar

3. KİŞİSEL VERİLERİN SAKLANMASI

3.1. Kişisel Verilerin Saklandığı Ortamlar

Kurum, 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 aşağıda yer alan ortamlarda saklamaktadır:

Elektronik Ortam:

- ✓ Fiziksel ve Sanal Sunucular
- ✓ Yazılımlar

- ✓ Bilgi Güvenliği Cihazları
- ✓ Kurum Bilgisayarı Dâhili Diski
- ✓ Mobil Cihazlar
- ✓ Harici Bellek (USB, Harici Harddisk vb.)
- ✓ Yazıcı, Tarayıcı, Fotokopi Makinası

Fiziksel Ortam:

- ✓ Basılı Doküman / Kopya / Belge
- ✓ Ofis İçi Alan
- ✓ Ortak Arşiv

3.2. Kişisel Verilerin Saklandığı Ortamların Güvenliğinin Sağlanması

Kurum, kişisel verilerin güvenli ortamlarda saklanması ve hukuka aykırı amaçlarla yok edilmesini, kaybolmasını veya değiştirilmesini önlemek için teknolojik imkânlar ve uygulama maliyetine göre gerekli teknik ve idari tedbirleri almaktadır.

3.2.1. İdari ve Teknik Tedbirler

Veri Güvenliği Tedbiri
Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
Çalışanlar için yetki matrisi oluşturulmuştur.
Erişim logları düzenli olarak tutulmaktadır.

Veri Güvenliği Tedbiri
Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
Gerektiğinde veri maskeleme 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 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.

Veri Güvenliği Tedbiri
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.
Sızma testi uygulanmaktadır.
Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.
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 HUKUKİ VE TEKNİK SEBEPLER

4.1. Kişisel Verilerin Saklanmasını Gerektiren Sebepler

4.1.1. Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler

Kişisel veriler Kurum tarafından;

- ✓ Kurumun doğmuş ya da doğabilecek yasal sorumluluklarını yerine getirebilmesi amacı ile ve kanunlarda öngörülen ölçülere ve/veya emredilen sürelere 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 veriler ise işleme amacı ortadan kalkmasından itibaren derhal ve en geç bir sonraki periyodik imha tarihine kadar,

Saklanmaya devam edecektir.

Kurum 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,
- ✓ 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- ✓ 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- ✓ 4982 Sayılı Bilgi Edinme Kanunu,
- ✓ 5115 Sayılı Kimlik Bildirme Kanunu,
- ✓ 5580 Sayılı Özel Eğitim Kurumları Kanunu,
- ✓ 4857 sayılı İş Kanunu,
- ✓ 2004 Sayılı İcra ve İflas Kanunu,
- ✓ 5434 sayılı Emekli Sağlığı Kanunu,
- ✓ 2828 sayılı Sosyal Hizmetler Kanunu
- ✓ 25369 sayılı İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- ✓ 24015 sayılı Arşiv Hizmetleri Hakkında Yönetmelik
- ✓ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- ✓ Diğer mevzuatlar

Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.2. Kişisel Verilerin İmhasını 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 Kurum tarafından kabul edilmesi,
- Kurumun, 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, Kurum tarafından re'sen veya ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

4.2.1. Kişisel Verilerin İmhasını Gerektiren Hukuki Sebepler

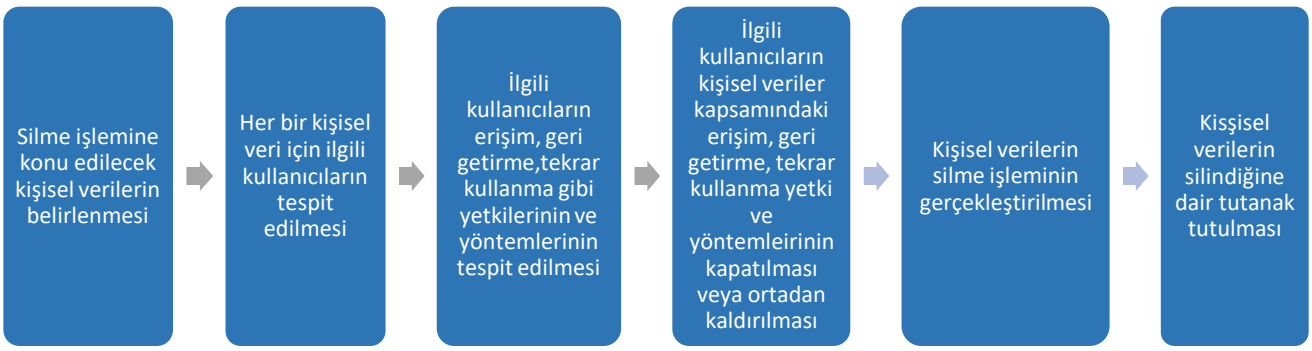
Kişisel veriler kurum tarafından;

- ✓ Kişisel Verilerin işlenmesini gerektiren amaçların ve saklanmasını gerektiren sebeplerin ortadan kalkması, ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- ✓ Kişisel Verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- ✓ İlgili kişinin, KVKK' nın 11. maddesinde belirtilen haklarını kullanarak kişisel verilerinin imha edilmesini talep etmesi ve yapılan başvurunun kurum tarafından kabul edilmesi,
- ✓ Kişisel Verilerin saklanmasını gerektiren azami sürenin geçmiş olması,
- ✓ Kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması halinde kişisel verileriniz imha edilir.

5. KİŞİSEL VERİLERİN SİLİNMESİ

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 almakla yükümlüdür.

5.1. Kişisel Verilerin Silinmesi Süreci



5.2. Kişisel Verilerin Silinmesi

5.2.1. Kayıt Ortamlarına Göre Silme Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır.

a) Hizmet Olarak Uygulama Türü Bulut Çözümleri

Kurum tarafından Bulut sisteminde bulunan veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken kurum ilgili kullanıcılarının Bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

b) Kâğıt Ortamında Bulunan Kişisel Veriler

Kâğıt ortamında bulunan kişisel veriler Kurum tarafından karartma yöntemi kullanılarak silinmelidir. 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 Ofis Dosyaları

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

ç) Taşınabilir Medyada Bulunan Kişisel Veriler

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

d) Veri Tabanları

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile silinmesi gerekir. Anılan işlem gerçekleştirilirken kurum ilgili kullanıcısının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

5.3. 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 almaktadır.

5.3.1. 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 kurum tarafından belirlenerek kullanılabilir.

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

***ii*) 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 gerekir.

***iii*) 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

Kurum veri kayıt ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:

***i*) Ağ cihazları (switch, router vb.):** Söz konusu cihazların 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 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'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

***iii*) Manyetik bant**: Verileri esnek bant 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 gerekir.

***iv*) 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 gerekir.

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

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

***vii*) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre a'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

***viii*) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri:** Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. a'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c) Kâğıt ve Mikro fiş 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 anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre a'da 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 kurumun hizmet aldığı 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.

Yukarıdaki ortamlara ek olarak; kurumun 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'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

gerekir.

6. ANONİM HALE GETİRİLMESİ

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. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye 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. Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, 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.

6.1. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

6.1.1. 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.

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

6.1.2. Değer düzensizliği sağlayan anonim hale getirme şekilleri

Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır.

- ✓ Mikro Birleştirme
- ✓ Veri Değiş Tokuşu
- ✓ Gürültü Ekleme

6.1.3 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 türetilebilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir.

- ✓ K-Anonimlik
- ✓ L-Çeşitlilik
- ✓ T-Yakınlık

7. SAKLAMA VE İMHA

7.1. Saklama ve İmha Süresi Tablosu

Veri Kategorisi	Veri Saklama Süresi
1-Kimlik Kişisel Veri	101 Yıl
2-İletişim Kişisel Veri	101 Yıl
4-Özlük Kişisel Veri	101 Yıl
5-Hukuki İşlem Kişisel Veri	10 Yıl
6-Müşteri İşlem Kişisel Veri	10 Yıl
7-Fiziksel Mekan Güvenliği Kişisel Veri	21 Gün
8-İşlem Güvenliği Kişisel Veri	2 Yıl

Veri Kategorisi	Veri Saklama Süresi
9-Risk Yönetimi Kişisel Veri	5 Yıl
10-Finans Kişisel Veri	10 Yıl
11-Mesleki Deneyim Kişisel Veri	101 Yıl
12-Pazarlama Kişisel Veri	2 Yıl
13-Görsel Ve İşitsel Kayıtlar Kişisel Veri	30 Yıl
16-Felsefi İnanç, Din, Mezhep Ve Diğer İnançlar Özel Nitelikli Kişisel Veri	101 Yıl
17-Kılık Ve Kıyafet Özel Nitelikli Kişisel Veri	101 Yıl

Veri Kategorisi	Veri Saklama Süresi
21-Sağlık Bilgileri Özel Nitelikli Kişisel Veri	101 Yıl
23-Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri Özel Nitelikli Kişisel Veri	101 Yıl

7.2 Periyodik İmha

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; kurum 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.

8. İMHA EDİLECEK KİŞİSEL VERİLERİN BELİRLENMESİ

8.1. Periyodik İmha Gerektiren Durumlar

Kurumda kişisel verilerin imhası Kişisel Veriler Envanteri' n de belirlenen sürelerde gerçekleştirilir ve en geç 6 (altı) aylık periyodlarla yapılır. Kişisel verilerin işlenme şartlarını ortadan kaldıran hallerden herhangi birinin gerçekleşmesi durumunda bu kişisel verilere ilişkin kayıtlar için bir sonraki imha periyodunda imha işlemi gerçekleştirilir.

Veri Sorumlusu Kişisel Veriler Envanteri üzerinden imha edilecek kişisel verileri tespit eder ve KVK Komitesi bölüm temsilcilerine bildirir. Bölüm temsilcisi, imha edilecek basılı ve elektronik kayıtları tespit eder.

8.2. Talep Üzerine İmha Gerektiren Durumlar

İlgili kişinin Kanun'dan kaynaklı hakkını kullanarak yaptığı başvurularda veya Kişisel Verileri Koruma Kurumu'nun talebine göre imha işlemi talebinin kurum de ulaşmasından itibaren 30 gün içinde gerçekleştirilerek ilgili kişiye cevap iletilir.

Kişisel veriler Talep Yönetim Süreci aracılığıyla gelen imha talepleri için Veri Sorumlusu, KVK Komitesi bölüm temsilcilerinden oluşturacağı ilgili çalışma grubu ile inceler ve imha edilecek kayıtları talebin kuruma ulaşması tarihinden itibaren en geç 10(on) gün içinde tespit eder.

8.3. İmha Yönteminin Belirlenmesi

Kişisel Veriler Envanterinde, imha edilecek kişisel verinin bulunduğu ortamın türü, kritikliği ve hassasiyetine göre Kişisel Verileri Koruma Kanununda belirtilen imha yöntemlerine göre imha türüne karar verilir. Eğer yok etme işlemi gerçekleştirilecekse, işlemin ardından oluşan fiziksel atıklar, güvenli ve geri döndürülemeyecek şekilde elden çıkarılır.

Silme	Yok Etme	Anonim Hale Getirme
Silinerek	Parçalanarak (Shredding)	Anonimleştirilerek
Formatlanarak	Yakılarak	-
Üzerine yazılarak	-	-
Manyetik alan ile	-	-

Fiziksel İmha Türleri	Dijital İmha Türleri
Parçalanarak (Shredding)	Formatlanarak
Yakılarak	Anonimleştirilerek
Üzerine yazılarak	Üzerine yazılarak
Manyetik alan ile	Silinerek

Ortamlara göre imha yöntemi aşağıda örneklendirilmiştir;

Kişisel Veri İçeren Ortam	İmha Çeşidi	İmha Yöntemi
Kâğıt	Fiziksel İmha	Parçalanarak
CD, DVD, Disket vb.	Fiziksel İmha	Parçalanarak
Taşıyıcı Bellek, SD Kart (USB)	Dijital İmha	Formatlanarak
Veri Tabanı	Dijital İmha	Anonimleştirilerek, Silinerek
Harici/Dahili Disk	Dijital İmha	Formatlanarak, Parçalanarak
Elektronik Yazışma (E-posta vb.)	Dijital İmha	Silinerek

8.4. 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 kayıtlarında imhasını sağlar.

8.5. Tespit Edilen Kişisel Verilerin Tamamının İmha Edildiğinden Emin Olunması

Veri Sorumlusu; Kişisel verilerin tamamının, planlanan zaman aralığında ve tespit edilen kayıtlarla imhayı KVK Komitesi tarafından imha edildiğini kontrol eder. Kişisel verilerin imhasının gerçekleştirilmesinin ardından İmha Ekibi, Veri İmha Formu 'nu doldurur ve Veri Sorumlusu' nun onayını alır. Bu form Veri Sorumlusu tarafından diğer hukuki yükümlülükler saklı kalmak üzere en az 10 (On) yıl süreyle saklanır.

9. SORUMLU KİŞİLER TABLOSU

Birim	Görev Tanımı
IK ve Personel Şefliği	Görevi dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe Müdürlüğü	Görevi dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Güvenlik Birimi	Görevi dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Birimi	Görevi dâhilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi