

**ÇEMBER PSİKOLOJİK
DANIŞMANLIK VE EĞİTİM
MERKEZİ
ZİNET TUNÇ**

**KVKK
KİŞİSEL VERİ SAKLAMA ve
İMHA POLİTİKASI**

Psikolojik Danışmanlık Merkezi

İçindekiler

1.GİRİŞ

1.1 Amaç

1.2 Kapsam

1.3 Kısaltmalar ve Tanımlar

2.SORUMLULUK VE GÖREV DAĞILIMLARI

3.KAYIT ORTAMLARI

4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

4.1 Saklamaya İlişkin Açıklamalar

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

4.1.2 Saklamayı Gerektiren İşleme Amaçları

4.2 İmhayı Gerektiren Sebepler

5.TEKNIK VE İDARİ TEDBİRLER

5.1 Teknik Tedbirler

5.2 İdari Tedbirler

6.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

6.1 Kişisel Verilerin Silinmesi

6.2 Kişisel Verilerin Yok Edilmesi

6.3 Kişisel Verilerin Anonim Hale Getirilmesi

7. SAKLAMA VE İMHA SÜRELERİ

8. PERİYODİK İMHA SÜRESİ 15

9. POLİTİKA’NIN YAYINLANMASI VE SAKLANMASI

10.POLİTİKA’NIN GÜNCELLENME PERİYODU

11.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN

KALDIRILMASI

12.EKLER

ZİNET TUNÇ KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI
KVKK Veri Yönetimi Kurulu

1.GİRİŞ

1.1 Amaç

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), ZİNET TUNÇ (“Merkez”) gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Merkez; Stratejik Planda belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Merkez çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü 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, Merkez tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 Kapsam

Merkez çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Merkez sahip olduğu ya da Merkez yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 Kısaltmalar ve Tanımlar

Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Çalışan	ZİNET TUNÇ personeli.
Elektronik Ortam	Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar.
Elektronik Olmayan Ortam	Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
Hizmet Sağlayıcı	ZİNET TUNÇ ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
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 kişiler.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
Kanun	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
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 ortam.

Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
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 envanter.
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 işlem.
Kurul	Kişisel Verileri Koruma Kurulu
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	Kişisel Verileri Saklama ve İmha Politikası
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi.
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 sistemi.
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik	28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2.SORUMLULUK VE GÖREV DAĞILIMLARI

Merkezin 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 saklanmasıyla 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 imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Kurul Başkanı	Merkez Sahibi	Çalışanların politikaya uygun hareket etmesinden, Politika’nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanı	Ataması Daha Sonra Yapılacak Kişi	Politika’nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

3.KAYIT ORTAMLARI

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

Tablo 2: Kişisel veri saklama ortamlar

Elektronik Ortamlar

- 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, 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

Elektronik Olmayan Ortamlar

- Kağıt
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri)
- Yazılı, basılı, görsel ortamlar

4.SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Merkez tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler Kanuna 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, Merkezimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.1.1 Saklamayı Gerektiren Hukuki Sebepler

Merkez, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname
- 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 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.

4.1.2 Saklamayı Gerektiren İşleme Amaçları

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

- İnsan kaynakları süreçlerini yürütmek.
- Kurumsal iletişimi sağlamak.
- Merkez güvenliğini sağlamak,
- İmzalanmış sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- Merkez ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

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 Merkez tarafından kabul edilmesi,
- Merkezin, 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 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, Merkez 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 maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Merkez tarafından teknik ve idari tedbirler alınır.

5.1 Teknik Tedbirler

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

- Sızma (Penetrasyon) testleri ile Merkezimizin bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Merkezimizin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme

sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Merkez, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Merkez tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa, evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

5.2 İdari Tedbirler

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

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Merkez tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Kişisel veri işlemeye başlamadan önce Merkez tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Merkez içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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

6.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

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.

6.2 Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Merkez tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt

	kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
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 değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3 Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. SAKLAMA VE İMHA SÜRELERİ

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

- Süreçlere 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 kayıta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Veri Yönetim Kurulu tarafından güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Veri Yönetim Kurulu tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kurul İşlemleri	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmelerin hazırlanması	Sözleşmenin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Merkez İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	Faaliyetin sona ermesini takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip Sistemleri	1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Ziyaretçi ve Toplantı	Etkinliğin sona ermesini	Saklama süresinin bitimini takip eden
Danışanların Kaydı	Takiben 1 Yıl	ilk periyodik imha süresinde
Kamera Kayıtları	1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11 inci maddesi gereğince Merkez, periyodik imha süresini 3 ay olarak belirlemiştir. Buna göre, Merkez her yıl Mart, Haziran, Eylül ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da Veri Yönetimi Kurulu dosyasında saklanır.

10.POLİTİKA'NIN GÜNCELLENME PERİYODU

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

11.POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Merkez yetkilisi tarafından onaylanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Yönetim Kurul Kararı ile Veri Yönetimi Kurulu tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Veri Yönetimi Kurulu tarafından saklanır.

12.EKLER

Politikaya dayanılarak oluşturulan ve uygulanan güncel dökümanlar aşağıdaki gibidir.

Revize edilmesi halinde revizyon numaralarıyla birlikte politikaya işlenecektir.

Ref No: 2021-001 / Veri İhlali Müdahale Planı

Ref No: 2021-002 / Çalışan Aydınlatma Metni

Ref No: 2021-003 / Açık Rıza Formu

Ref No: 2021-004 / KVKK Başvuru Formu

Ref No: 2021-005 / Gizlilik Sözleşmesi

Ref No: 2021-006 / Kamera Kaydı Aydınlatma Metni

Ref No: 2021-007 / Veri Envanteri

VERİ YÖNETİM KURULU

Kurul Başkanı