

KİŞİSEL VE ÖZEL NİTELİKLİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

Bu Kişisel Veri Saklama ve İmha Politikası 6698 sayılı Kişisel Verilerin Korunması Kanunu (“Kanun”), Kişisel Sağlık Verileri Hakkında Yönetmelik Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (“Yönetmelik”), ve sair mevzuatlar çerçevesinde Veri Sorumlusu sıfatıyla Diyarlar Sağlık İnşaat Turizm ve Eğitim Ticaret ve Sanayi Limited Şirketi (“Merkez”) tarafından hazırlanmıştır.

1.1. Amaç

Merkez, Kanun hükümleri doğrultusunda öngörülen ilkeler ve sınırlar çerçevesinde; hasta, hasta yakınları, refakatçiler, personel, personel yakınları, personel adayları, personel aday referans kişileri, tedarikçiler, hizmet alınan kişiler ve hissedarlara ait kişisel verileri işlemekte ve bu kişi gruplarının T.C. Anayasası da dahil ancak bununla sınırlı olmamak üzere her türlü mevzuatta öngörülen haklarını etkin bir şekilde kullanmasını hedeflemektedir.

Kişisel Verileri Saklama ve İmha Politikası (“Politika”), Merkez tarafından kişisel ve özel nitelikli kişisel veri işleme süreci sonrası uygulanan saklama ve imha faaliyetlerine ilişkin iş ve işlemlerin usul ve esaslarının belirlemek ve bu sayede ilgili konularda şeffaflığı sağlamak ve bu konuların veri sahipleri için bilinebilir hale getirilmesi amacıyla hazırlanmıştır. Kişisel ve özel nitelikli kişisel verilerin saklanması ve imhasına ilişkin her türlü işlem, İşbu Politika’da belirtilen şekilde gerçekleştirilmektedir.

1.2. Kapsam

Hasta, hasta yakınları, refakatçiler, personel, personel yakınları, personel adayları, personel aday referans kişileri, tedarikçiler, hizmet alınan kişiler ve hissedarlara ait kişisel veriler bu Politika kapsamındadır. Merkezin işlediği ve yönettiği, özel nitelikli kişisel verileri de içerisine alan her türlü kişisel veri bu Politika’da belirtilen sınırlar dahilinde saklanmakta ve imha edilmektedir. İmha faaliyeti kişisel ve özel nitelikli kişisel verilerin silinmesi, anonim hale getirilmesi ile yok edilmesi faaliyetlerini kapsamaktadır. Bu süreçte yine bu Politika’da açıklanan iş ve işlemler uygulanır.

1.3. Hukuki ve Teknik Terimlerin Tanımı

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.
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.
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.
Hasta	Merkez tarafından sunulan sağlık hizmetlerinden faydalanma ihtiyacı bulunan ve bu yönde Merkez'e başvuran gerçek kişiler.
Hasta Yakını	Merkez tarafından sunulan sağlık hizmetlerinden faydalanma ihtiyacı bulunan ve bu yönde Merkez'e başvuran gerçek kişilerce bildirilen yahut Merkez'e gelişlerinde yanlarında bulunan yakınları.
Hissedar	Merkez'de hisse sahibi olan gerçek ve/veya tüzel kişiler.
Hizmet Alınan Kişi	Merkez tarafından ihtiyaç duyulan hizmetlerin temin edildiği üçüncü şahıs gerçek/tüzel kişiler yahut bunların yetkilileri ve çalışanları.
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, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, 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.
Kişisel Verilerin Silinmesi	Kişisel verilerin ilgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kısmi Kimliksizleştirme	Kişisel verilerin bulanıklaştırma, şifreleme, anahtar kodlama ve veri paylaşımı gibi teknolojiler vasıtasıyla açık tanımlayıcılarından sıyrılması ve genelleştirilmesiyle kişiyi belirlenebilir kılan özelliklerinden arındırılmasıdır.
Kurul	Kişisel Verileri Koruma Kurulu.
Maskeleye	İşlenen ve saklanan gizli, hassas ve kişisel verilere erişimi önlemek amacıyla, orijinal verilerin tamamının ya da bir kısmının özel karakter veya farklı yöntemlerle değiştirilerek anlamsız hale getirilmesini sağlayan bir veri güvenlik önlemidir.
Merkez	Diyamar Sağlık İnşaat Turizm ve Eğitim Ticaret ve Sanayi Limited Şirketi
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.
Personel	Merkez'de kısmi/tam zamanlı iş sözleşmesi ile iş görme borcu yüklenen, 4857 ve 5510 sayılı kanunlara tabi hizmet erbabı.
Personel Adayı	Merkez'de kısmi/tam zamanlı iş sözleşmesi ile iş görme borcu yüklenme amacı ile Merkez'e başvuranlar.

Personel Adayı Referans Kişisi	Personel adayının mesleki deneyimi ve yetisi ile ilgili bilgi sahibi olan, personel adayı tarafından bilgisine başvurulması için Merkez'e bildirilen gerçek kişi.
Personel Yakını	Merkez'de kısmi/tam zamanlı iş sözleşmesi ile iş görme borcu yüklenen, 4857 ve 5510 sayılı kanunlara tabi hizmet erbabı olan kimselerce bildirilen yakınları.
Politika	Kişisel Verileri Saklama ve İmha Politikası.
Refakatçi	Merkez tarafından sunulan sağlık hizmetlerinden faydalanma ihtiyacı bulunan ve bu yönde Merkez'e başvuran gerçek kişilere Merkez'de süren tedavileri süresince eşlik eden gerçek kişiler.
Tedarikçi	Merkez tarafından ihtiyaç duyulan hizmetlerin tedarik edildiği üçüncü şahıs gerçek/tüzel kişiler yahut bunların yetkilileri ve çalışanları.
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	Diyamar Sağlık İnşaat Turizm ve Eğitim Ticaret ve Sanayi Limited Şirketi (Merkez)
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

Merkez'in tüm birimleri ve çalışanları, politika kapsamında alınan teknik ve idari tedbirlerin sorumlu birimlerce gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, takibi ve denetimi ile kişisel ve özel nitelikli kişisel verilere hukuka aykırı olarak erişilmesinin ve işlenmesinin önlenmesi, mevcut kişisel ve özel nitelikli kişisel verilerin hukuka uygun olarak saklanmasının sağlanması, veri sahiplerinin aydınlatılması amacıyla lazım gelen tüm teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel ve özel nitelikli kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki şekildedir;

Unvan	Birim	Görev
Mesul Müdür	Sağlık Hizmetleri	Özel nitelikli kişisel verileri Politika'ya ve mevzuata uygun olarak işlemek ve aktarmak ile sorumludur.
İşletme Müdürü	Yönetim	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Başhemşire	Sağlık Hizmetleri	Görevlerine uygun olarak Politika'nın yürütülmesinden sorumludur.

3. KAYIT ORTAMLARI

İşlenen kişisel ve özel nitelikli kişisel veriler, Merkez tarafından aşağıda sıralanan ortamlarda hukuka uygun ve güvenli şekilde saklanır.

Elektronik Ortamlar:

- Sunucular (Etki Alanı, yedekleme, elektronik posta, veritabanı, web, dosya paylaşımı, vb.)
- Yazılımlar (Mavi Nokta Yazılım)
- 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.)
- Çıkarılabilir bellekler (USB, hafıza kartı vb.)
- Yazıcı, tarayıcı, fotokopi makinesi

Elektronik Olmayan Ortamlar:

- Kağıt
- Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri, personel bilgi formu, iş başvuru formu, Merkez nezdinde tutulan her türlü sağlık formları vb.)
- Yazılı, basılı, görsel ortamlar
- Arşiv
- Dolaplar

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Merkez; hasta, hasta yakınları, refakatçi, personel, personel adayı, tedarikçi, hissedarlar, hizmet alınan kişiler ve diğer üçüncü kişilere ait kişisel ve özel nitelikli kişisel verileri Kanun ve ilgili ikincil mevzuatta

uygun bir şekilde saklamakta ve imha etmektedir. Saklama ve imha etme iş ve işlemleri aşağıda detayları açıklandığı şekilde gerçekleştirilmektedir.

4.1. Saklamaya İlişkin Açıklamalar

Merkez, kişisel ve özel nitelikli kişisel veri işlemenin sınırını Kanun'un 3. maddesinde tanımlandığı şekilde uygulamakta, aynı Kanun'un 4. maddesindeki kişisel verilerin *belirli, açık ve meşru amaç* ile ve bu amaçla *bağlantılı, sınırlı ve ölçülü* olarak, *işlendikleri amaç için gerekli olan süre kadar muhafaza etme* ilkelerini benimsemektedir. Merkez aynı zamanda Kanun'un 5. ve 6. maddelerindeki kişisel ve özel nitelikli kişisel verilerin işleme şartlarına da riayet etmektedir.

4.1.1. Saklamayı Gerektiren Hukuki Sebepler

Kişisel ve özel nitelikli kişisel verileri saklamayı gerektiren hukuki sebepler aşağıdaki gibidir;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 4721 Sayılı Türk Medeni Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 5237 sayılı Türk Ceza Kanunu,
- 4857 sayılı İş Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 213 sayılı Vergi Usul Kanunu,
- 6502 sayılı Tüketicinin Korunması Hakkında Kanun,
- 2219 sayılı Hususi Hastaneler Kanunu,
- 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname,
- Diyaliz Merkezleri Hakkında Yönetmelik,
- Hasta Hakları Yönetmeliği,
- Sağlıkta Kalitenin Geliştirilmesi ve Değerlendirilmesine Dair Yönetmelik,
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Yataklı Tedavi Kurumları İşletme Yönetmeliği,
- Kişisel Sağlık Verileri Hakkında Yönetmelik,
- Özel Hastaneler Yönetmeliği,
- Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik,
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler ve sair mevzuat hükümleri.

4.1.2. Saklamayı Gerektiren İşleme Amaçları

Kişisel ve özel nitelikli kişisel verilerin işlenmesindeki amaçlar her bir veri konusu kişi grubu özelinde aşağıda belirtilmektedir;

Hastalar

- Sosyal Güvenlik Kurumu ile Merkez arasında yapılan sözleşme ve Merkez tarafından sunulan sağlık hizmetlerinin düzenlendiği sair mevzuat hükümleri çerçevesinde yasal yükümlülüklerin yerine getirilmesi,
- Kamu sağlığının korunması,
- Sağlık hizmetlerinin sunulması, geliştirilmesi ve iyileştirilmesi,
- Sağlık hizmetleri kullanımının analiz edilmesi,
- Sunulan hizmetler karşılığında fatura tanzim edilmesi,
- Düzenleyici ve denetleyici kurumlar ile resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temininin sağlanması,
- Merkez'de en uygun tedavi hizmetinin sunulabilmesi, bu hizmetin ifasının, planlamasının ve finansmanının gerçekleştirilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi, yasal ve düzenleyici gereksinimlerin yerine getirilmesi,
- T.C. Sağlık Bakanlığı ve diğer kamu kurum ve kuruluşları ile edinilen verilerin paylaşılması ve taleplere ilişkin yanıt verilmesi,
- Saklanması gerekli sağlık verilerine ilişkin bilgilerin muhafaza edilmesi

Hasta Yakını ve Refakatçiler

- Hasta sağlığının korunması ve tedavisinin gerçekleştirilmesi için gerekli olan hallerde iletişim sağlanması.

Personel ve Personel Adayları

- Sosyal Güvenlik Kurumu ile Merkez arasında yapılan sözleşmede yer alan hukuki yükümlülüklerin yerine getirilmesi,
- Kamu sağlığının korunması,
- Merkez'in sistem ve uygulamalarının veri güvenliğini sağlamak adına tüm gerekli idari ve teknik tedbirlerin alınması,
- Düzenleyici ve denetleyici kurumlarla, resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temininin sağlanması,
- Merkez iç politikası ve prensiplerine uyum sağlanması,
- Hukuki işlemlerin yerine getirilmesi,
- Merkez'in iç işleyişi ile günlük operasyonların planlanması ve yönetilmesi, risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Yasal ve düzenleyici gereksinimlerin yerine getirilmesi,
- Yetkili kamu kurum ve kuruluşları ile edinilen bilgilerin paylaşılması ve yanıt verilmesi,
- İlgili mevzuat gereği saklanması gereken verilere ilişkin bilgilerin muhafaza edilmesi
- İş akdi ve mevzuat kaynaklı yükümlülüklerin yerine getirilmesi,
- Eğitim faaliyetlerinin planlanması ve yürütülmesi,

- Personel adına yan haklar sağlanması,
- Kurumsal iletişim faaliyetlerinin planlanması,
- Aylık ücret ve her türlü ödemenin takibi ve gerçekleştirilmesi,
- İnsan kaynakları süreçlerinin yürütülmesi,
- Personel memnuniyetinin artırılması
- İş sağlığı, güvenliği ve barışının sağlanması

Personel Yakını

- Gerekli olan hallerde iletişimin sağlanması,
- İş mevzuatı kapsamında personel yakınlarına yan haklar sağlanması.

Personel Adayı Referans Kişisi

- Personel adayı tarafından gösterilen referansın teyidinin yapılması,
- Başvurduğu pozisyona uygunluğunun değerlendirilmesi,
- Geçmiş deneyimleri hakkında bilgi edinilmesi ve doğrulanmasıdır.

Merkez Tedarikçileri ve Hizmet Alınan Kişiler

- Merkez'in sistem ve uygulamalarının veri güvenliğini sağlamak adına tüm gerekli idari ve teknik tedbirlerin alınması,
- Düzenleyici ve denetleyici kurumlarla, resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temininin sağlanması,
- Merkez iç politikası ve prensiplerine uyum sağlanması,
- Merkez'in iç işleyişi ile günlük operasyonların planlanması ve yönetilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Yasal ve düzenleyici gereksinimlerin yerine getirilmesi,
- Gerekli iletişimin sağlanması,
- Mevzuat uyarınca T.C. Sağlık Bakanlığı ve diğer kamu kurum ve kuruluşları ile edinilen bilgileri paylaşma ve yanıt verilmesi,
- İlgili mevzuat gereği saklanması gereken verilere ilişkin bilgilerin muhafaza edilmesi
- Mal ve hizmet tedariki için sözleşme yapılması ve tamamlanması
- Yetki tespitinin yapılması

Hissedarlar

- Merkez'in sistem ve uygulamalarının veri güvenliğini sağlamak adına tüm gerekli idari ve teknik tedbirlerin alınması,
- Düzenleyici ve denetleyici kurumlarla, resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temininin sağlanması,
- Merkez iç politikası ve prensiplerine uyum sağlanması,
- Merkez'in iç işleyişi ile günlük operasyonların planlanması ve yönetilmesi,
- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,
- Yasal ve düzenleyici gereksinimlerin yerine getirilmesi,

- Gerekli iletişimin sağlanması,
- Mevzuat uyarınca T.C. Sağlık Bakanlığı ve diğer kamu kurum ve kuruluşları ile edinilen bilgileri paylaşma ve yanıt verilmesi,
- İlgili mevzuat gereği saklanması gereken verilere ilişkin bilgilerin muhafaza edilmesi
- Gerekli resmi müracaatların yapılması,
- Yönetim faaliyetleri ve sözleşme süreçlerinin yürütülmesi

4.2. İmhayı Gerektiren Sebepler

Kişisel ve özel nitelikli kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel ve özel nitelikli kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanun'un 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel ve özel nitelikli kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi,
- Merkez'in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, Merkez'in cevabının ilgili kişi tarafından yetersiz bulunması veya Merkez'in Kanun'da öngörülen süre içerisinde ilgili kişiye cevap vermemesi hallerinde; ilgili kişinin Kurul'a şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel ve özel nitelikli kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel ve özel nitelikli 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. Yukarıda sayılan sebepler ve açıklamalar kişisel ve özel nitelikli kişisel verilerin imhası için de geçerlidir.

5. TEKNİK VE İDARİ TEDBİRLER

Merkez, kişisel ve özel nitelikli kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve kişisel ve özel nitelikli kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ile kişisel ve özel nitelikli kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12. maddesiyle, 6. maddesinin dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde teknik ve idari tedbirler almaktadır.

5.1. Teknik Tedbirler

Kişisel ve özel nitelikli kişisel verilerin belirtilen ortamlarda güvenli bir biçimde saklanması için Merkez tarafından alınan teknik tedbirler;

- Sızma (Penetrasyon) testleri ile Merkez bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemlerin alınması,
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditlerin sürekli olarak izlenmesi,

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesinin erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılması,
- Merkez'in bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemlerin alınması ve güncel anti-virüs sistemlerinin kullanılması,
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için sisteme sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, yangın söndürme sistemi, iklimlendirme sistemi gibi ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınması,
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik risklerin belirlenmesi, bu risklere uygun teknik tedbirlerin alınmasının sağlanması ve alınan tedbirlere yönelik teknik kontrollerin yapılması,
- Merkez içerisinde erişim prosedürleri oluşturularak kişisel ve özel nitelikli kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılması,
- Silinen kişisel ve özel nitelikli kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirlerin alınması,
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmesi ve bilgi sistemlerinin güncel halde tutulması,
- Kişisel ve özel nitelikli kişisel verilerin işlendiği elektronik ortamlarda güçlü parolaların kullanılması,
- Kişisel ve özel nitelikli kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemlerinin kullanılması,
- Kişisel ve özel nitelikli kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programlarının kullanılarak veri kaybının önlenmesi,
- Elektronik olan veya olmayan ortamlarda saklanan kişisel ve özel nitelikli kişisel verilere erişimin, erişim prensiplerine göre sınırlandırılması,
- Merkez internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmesi olarak özetlenebilir.

5.2. İdari Tedbirler

Kişisel ve özel nitelikli kişisel verilerin belirtilen ortamlarda güvenli bir biçimde muhafaza edilmesi için Merkez tarafından alınan tedbirler;

- Mevcut risk ve tehditlerin belirlenmesi,
- Personelin niteliğinin geliştirilmesine yönelik, kişisel ve özel nitelikli kişisel verilerin hukuka aykırı olarak işlenmesinin ve söz konusu verilere hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili diğer mevzuat hakkında eğitimlerin verilmesi,
- *Kişisel Veri Saklama ve İmha Politikası* gibi kurumsal politikalar ve metinler hazırlanması,
- Kişisel veri işlemeye başlamadan önce Merkez tarafından, ilgili kişileri aydınlatma yükümlülüğünün yerine getirilmesi,
- Merkez tarafından yürütülen faaliyetlere ilişkin personel ile gizlilik sözleşmeleri imzalanması,
- Güvenlik politika ve prosedürlerine uymayan personele yönelik uygulanacak disiplin prosedürü hazırlanması,
- Kanun'a uygun olarak kişisel veri işleme envanteri hazırlanması,

- Veri Sorumluları Sicil Bilgi Sistemi'ne VERBİS kaydının yapılması,
- Merkez içi periyodik ve rastgele denetimler yapılması,
- Veri minimizasyonu prensibi benimsenerek bu prensip çerçevesinde kişisel ve özel nitelikli kişisel verilerin mümkün olduğunca azaltılması ve gerekli olmayan, güncelliğini yitirmiş ve bir amaca hizmet etmeyen verilerin toplanılmayıp şayet bu tip veriler uyum sürecinden önceki dönemde toplandıysa söz konusu verilerin Politika'ya uygun bir şekilde imha edilmesi,
- Merkez tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasının önlenmesi ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel ve özel nitelikli kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirlerin alınması,
- Görev değişikliği olan ya da işten ayrılan personelin bu alandaki yetkilerinin derhal kaldırılması ve bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,
- Erişim yetkilerinin sınırlandırılıp yetkilerin düzenli olarak gözden geçirilmesi,
- Kişisel verilerin korunması alanındaki gelişmelerin takip edilmesi ve gerekli, yeterli uygulamaları hayata geçirebilmek için danışmanlık hizmeti alınması,
- Personelin, ilgili mevzuat çerçevesinde esas olanın hastaya bilgilendirme yapılması olduğu ve ancak hastanın yazılı onayının bulunması halinde hasta yakınına bilgi verilebileceği konusunda bilgilendirilmesi,
- Kişisel ve özel nitelikli kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumun ilgili kişiye ve Kurul'a bildirilmesi olarak özetlenebilir.

Özel nitelikli kişisel verilerin güvenliğine yönelik yukarıdakilere ek olarak ayrıca bazı idari ve teknik tedbirler belirlenmiştir. Buna göre;

- Özel nitelikli kişisel veri işleme süreçlerinde yer alan personele, verilere erişim yetkisine sahip kullanıcıların yetkilerinin tanımlanması,
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan personele yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmesi,
- Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması ve periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;
 - Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
 - Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
 - Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;
 - Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
 - Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,
- Özel nitelikli kişisel veriler aktarılacaksa;
 - Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

- Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veri aktarımının gerçekleştirilmesi,
- Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın “gizlilik dereceli belgeler” formatında gönderilmesi gerekir.
 - Hiç kimsenin -sağlık hizmeti sunumu için gerekli olan durumlar haricinde- geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanmaması,
 - e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanması ve ilgili kişilerin, gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilmesi olarak özetlenebilir.

6. KİŞİSEL VE ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

Merkez, Yönetmelik’in 7. maddesinde kişisel ve özel nitelikli kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi ile ilgili öngörülen ilkeler çerçevesinde işlem yapmakta ve verileri kayıt altına almaktadır.

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel ve özel nitelikli 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 ve Özel Nitelikli Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi neticesinde ilgili kişiye ait kişisel ve özel nitelikli kişisel veriler, söz konusu verilere ulaşımı olan kişiler için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmektedir.

Bu verilerin silinmesi için kullanılan yöntem aşağıdaki şekildedir:

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel ve özel nitelikli 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 ve özel nitelikli kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı 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 ve özel nitelikli 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 ve özel nitelikli kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel ve Özel Nitelikli Kişisel Verilerin Yok Edilmesi

Kişisel ve özel nitelikli kişisel verilerin yok edilmesi neticesinde ilgili kişiye ait kişisel ve özel nitelikli kişisel veriler hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmektedir.

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel ve özel nitelikli kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırma makineleriyle veya yakılarak veya tamamen yırtılarak geri döndürülemez şekilde yok edilir.
Optik/Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel ve özel nitelikli kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya üzerindeki veriler bozularak, okunamaz hale getirilir.

6.3. Kişisel ve Özel Nitelikli Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel ve özel nitelikli kişisel verilerin anonim hale getirilmesi neticesinde, ilgili kişilere ait verilerin başka verilerle eşleştirilmesi halinde dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmektedir. Merkez, kişisel verileri anonim hale getirmek için aşağıda belirtilen yöntemlerden bir veya birkaçını kullanabilir;

Maskleme (Masking):

Veri maskleme ile kişisel ve özel nitelikli kişisel verinin temel belirleyici bilgisini veri seti içerisinde çikartılarak kişisel ve özel nitelikli kişisel verinin anonim hale getirilmesi yöntemidir.

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkarılarak saklanan veriler anonim hale getirilmektedir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.

Global Kodlama: Veri türetme yöntemi ile kişisel ve özel nitelikli kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel ve özel nitelikli kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/-) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel ve özel nitelikli kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemler Kanun kapsamı dışında olup, kişisel ve özel nitelikli kişisel veri sahibinin açık rızası aranmayacaktır.

7. SAKLAMA VE İMHA SÜRELERİ

Kişisel ve özel nitelikli kişisel veriler, toplandıkları amacı yerine getirmek için gerekli süre boyunca saklanmakta ve bu süreler her bir iş, işlem ya da faaliyet özelinde ayrı ayrı belirlenmektedir.

Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre belirtilmemişse kişisel verilerin imha süreleri belirlenirken aşağıdaki kriterler dikkate alınmaktadır;

- Sağlık sektöründe genel teamül gereği kabul edilen süre,
- Veri sahibiyle tesis edilen hukuki ilişkinin devam edeceği süre,
- Kişisel verileri hukuken saklamak zorunda olunan süre,
- Merkez'in elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
- Verinin saklanması yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
- Verinin doğru ve gerektiğinde güncel tutulmasının gerekliliği ve bunun belirlenen süre için mümkün olup olmadığı,
- Veri sorumlusu tarafından, kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi.

Merkez tarafından işlenmekte olan kişisel ve özel nitelikli kişisel verilerle ilgili olarak; Faaliyetlere bağlı olarak gerçekleştirilen işlemler kapsamındaki tüm kişisel ve özel nitelikli kişisel verilerle ilgili veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde, veri kategorileri bazında saklama süreleri VERBİS'e kayıttaki, faaliyet bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır. Söz konusu saklama süreleri üzerinde, gerekmesi halinde Merkez tarafından güncellemeler yapılabilmektedir.

Bu doğrultuda, veri sahibine ve veri kategorisine göre belirlenen kişisel veri saklama ve imha süreleri şu şekildedir;

Faaliyet	Veri Saklama Süresi	Veri İmha Süresi
Hasta Randevu Oluşturma ve Randevu Takibi İşlemleri	Hasta Ziyaretinin Tamamlanmasından İtibaren 6 ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hasta Kabul İşlemleri, Tedavi Planlaması, Hasta Kimlik Doğrulaması ve Tedavinin Yürütülmesi İşlemleri	Hasta Tedavisinin Tamamlanmasından İtibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel Özlük Dosyası Oluşturma ve Personel Devam Kontrol Sistemi İşlemleri	İşten Ayrılma Tarihinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ücret ve Prim Ödemeleri ile Personel Eğitimi İşlemleri	İşten Ayrılma Tarihinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Personel Adayı Dosyası Oluşturma	İş Başvuru Tarihinden İtibaren 1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Mal Alım İşlemleri, Hizmet Karşılığı Ödeme, Sunulan Hizmet Karşılığı Fatura Tanzimi ve Hasta Lojistiğinin Sağlanması	Sözleşme İlişkisinin Sona Ermesinden İtibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Merkez Yönetimi İşlemleri	Hissedarlık İlişkisinin Sona Ermesinden İtibaren 10 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuki Süreçlerin Yönetimi İşlemleri	Hukuki İlişkinin Sona Ermesinden İtibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. PERİYODİK İMHA SÜRESİ

Merkez, veri sorumlusu sıfatı ile Yönetmelik'in 11. maddesi uyarınca kişisel ve özel nitelikli kişisel veri saklama ve imha periyodik süresini 6 ay olarak belirlemiştir. Buna göre Merkez'de Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilmektedir. Anılan süre, her hal ve koşulda Yönetmelik'in 11. maddesinde belirtilen azami periyodik imha süresini aşmamaktadır.

9. POLİTİKA'NIN YAYIMLANMASI ve SAKLANMASI

Politika, basılı (ıslak imzalı) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanmakta olup, Merkez'in internet sayfası olan www.diyamardiyaliz.com'da kamuya açıklanmıştır.

Bu politika uyarınca, kişisel veriler üzerinde gerçekleştirilen; silme, yok etme veya anonim hale getirme işlemlerinin tümü kayıt altına alınır ve bu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç (3) yıl süreyle saklanır.

10. POLİTİKA’NIN GÜNCELLENME PERİYODU

Politika, Merkez tarafından ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir. Aynı şekilde zaman içinde değişebilecek mevzuat hükümleri ve kurum politikalarında meydana gelebilecek değişiklikler sebebiyle işbu Politika’da güncellemeler yapılabilecektir. Politika’nın en güncel versiyonu Merkez’in internet sayfası üzerinden yayımlanacaktır.

11. POLİTİKA’NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika Merkez’in internet sitesinde yayımlanması ile yürürlüğe girer. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika’nın ıslak imzalı eski nüshaları İdari İşler tarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 3 (üç) yıl süre ile Merkez bünyesinde saklanır.

12. DİĞER HUSUSLAR

Politika’nın, Kanun veya sair mevzuat ile uyumsuz olması halinde, Kanun ve ilgili mevzuat hükümleri öncelikli olarak uygulanır.

Bu Politika, tüm personel ve yetkililerin bilgisine sunulur ve bu kişiler tarafından okunması sağlanır. Personel, Merkez bünyesinde gerçekleştirdikleri tüm işlemlerde Kanun ve bu Politika’ya uygun hareket edeceklerini kabul, beyan ve taahhüt ederler.