

**UZ.DR. SAVAŞ DEMİRPENÇE KLİNİĞİ**  
**KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

**MADDE 1- AMAÇ**

Kişisel verileri saklama ve imha politikası Uz.Dr. Savaş Demirpençe kliniği (ve tüm çalışanları) tarafından işlenen kişisel verilerin saklanması ve imhasına yönelik iş ve işlemler konusundaki usulleri ve esasları belirlemek amacıyla hazırlanmıştır.

**MADDE 2- KAPSAM**

Şirket çalışanlarına, çalışan adaylarına, stajyerlere, ürün ve hizmet alanlara, potansiyel müşterilere, ortaklara, ziyaretçilere, tedarikçilere ve diğer üçüncü kişilere ait kişisel veriler bu politika kapsamındadır.

Şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.

**MADDE 3- TANIMLAR**

<b>Alıcı grubu</b>	: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
<b>Açık rıza</b>	: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
<b>Anonim Hale Getirme</b>	: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
<b>Çalışan</b>	: Şirket personeli
<b>Elektronik ortam</b>	: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
<b>Elektronik olmayan ortam</b>	: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
<b>Hizmet sağlayıcı</b>	: Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
<b>İlgili kişi</b>	: Kişisel verisi işlenen gerçek kişi
<b>İlgili kullanıcı</b>	: 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

<b>İmha</b>	: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
<b>Kanun</b>	: 6698 Sayılı Kişisel Verilerin Korunması Kanunu
<b>Kayıt ortamı</b>	: 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
<b>Kişisel veri</b>	: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
<b>Kişisel veri işleme envanteri</b>	: 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
<b>Kişisel verilerin işlenmesi</b>	: 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
<b>Kurul</b>	: Kişisel Verileri Koruma Kurulu
<b>Özel nitelikli kişisel veri</b>	: 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
<b>Periyodik imha</b>	: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi

<b>Politika</b>	: Kişisel Verileri Saklama ve İmha Politikası
<b>Şirket</b>	: Uz.Dr. Savaş Demirpençe Kliniği
<b>Veri işleyen</b>	: Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi
<b>Veri kayıt sistemi</b>	: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
<b>Veri sorumlusu</b>	: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi
<b>Veri sorumluları sicil bilgi sistemi</b>	: Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi
<b>VERBİS</b>	: Veri Sorumluları Sicil Bilgi Sistemi
<b>Yönetmelik</b>	: 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

#### **MADDE 4- SORUMLULUK VE GÖREVLER**

Şirketin tüm çalışanları ve birimleri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması konusunda sorumlu birimlere tam ve aktif destek verir. Politika kapsamında alınan idari ve teknik tedbirlerin uygulanmasında, birim çalışanlarının eğitilmesinde, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesinde ve kişisel verilerin hukuka uygun olarak muhafazasında tüm çalışanlar ve birimler, sorumlu birimlere destek olur.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım EK TABLO: 1’de gösterilmiştir.

#### **MADDE 5- KAYIT ORTAMLARI**

Kişisel veriler, kliniğimiz tarafından EK TABLO: 2’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

#### **MADDE 6- SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER**

Kliniğimizde, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

- a. Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,

- b. Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması
- c. Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla şirketin meşru menfaatleri için saklanmasının zorunlu olması
- d. Kişisel verilerin şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması
- e. Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi
- f. Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması

#### **MADDE 7- SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI**

Şirket aşağıdakiler dahil olmak ancak bununla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir:

- a. İnsan kaynakları süreçlerini yürütmek
- b. Hasta letişimi sağlamak
- c. Klinik güvenliğini sağlamak
- d. İstatistiksel çalışmalar yapabilmek
- e. İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek
- f. Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak
- g. Klinik ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak
- h. Yasal raporlamalar yapmak
- i. Çağrı merkezi süreçlerini yönetmek
- j. İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirmek
- k. Klinik hukuk işlerinin icrası/takibini yapmak

#### **MADDE 8- İMHAYI GEREKTİREN HUKUKİ SEBEPLER**

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re'sen şirket tarafından silinir ya da yok edilir:

- a. Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması
- b. Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması
- c. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması

- d. Kanunun 11 inci maddesi geređi ilgili kiřinin hakları çerçevesinde kiřisel verilerinin silinmesi ve yok edilmesine iliřkin yaptıđı bařvurunun veri sorumlusu tarafından kabul edilmesi
- e. Kiřisel verilerin saklanması gerektiren azami sürenin geçmiř olması ve kiřisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir řartın mevcut olmaması

## **MADDE 9- TEKNİK TEDBİRLER**

řirket tarafından, iřlediđi kiřisel verilerle ilgili olarak alınan teknik tedbirler ařađıdadır:

- a. Kurulan sistemler kapsamında gerekli iç kontrolleri yapar
- b. Kurulan sistemler kapsamında bilgi teknolojileri risk deđerlendirmesi ve iř etki analizinin gerçekteřtirilmesi süreçlerini yürütür
- c. Verilerin řirket dıřına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluřturulmasını sađlar
- d. Düzenli olarak ve ihtiyaç oluřtuđunda sızma testi hizmeti olarak sistem zafiyetlerinin kontrolünü sađlar
- e. Bilgi teknolojileri birimlerinde çalıřanların kiřisel verilere eriřim yetkilerinin kontrol altında tutulmasını sađlar
- f. Kiřisel verilerin yok edilmesi geri dönüřtürülemeyecek ve denetim izi bırakmayacak řekilde sađlanır
- g. Kanun'un 12. maddesi uyarınca, kiřisel verilerin saklandıđı her türlü dijital ortam, bilgi güvenliđi gereksinimlerini sađlayacak řekilde řifreli veyahut kriptografik yöntemler ile korunur

## **MADDE 10- İDARİ TEDBİRLER**

řirket tarafından, iřlediđi kiřisel verilerle ilgili olarak alınan idari tedbirler ařađıdadır:

- a. Saklanan kiřisel verilere řirket içi eriřimi iř tanımı geređi eriřmesi gerekli personel ile sınırlandırır. Eriřimin sınırlandırılmasında verinin özel nitelikli olup olmadıđı ve önem derecesi de dikkate alınır.
- b. İřlenen kiřisel verilerin hukuka aykırı yollarla bařkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgisine ve Kurul'a bildirir.
- c. Kiřisel verilerin paylařılması ile ilgili olarak, kiřisel verilerin paylařıldıđı kiřiler ile kiřisel verilerin korunması ve veri güvenliđine iliřkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliđini sađlar.
- d. Kiřisel verilerin iřlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kiřisel verilerin korunması mevzuatı ve veri güvenliđi kapsamında gerekli eđitimleri verir.

- e. Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

#### **MADDE 11- KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ**

Kişisel veriler EK TABLO: 3'te belirtilen yöntemlerle silinir.

#### **MADDE 12- KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ**

Kişisel veriler EK TABLO: 4'te belirtilen yöntemlerle yok edilir.

#### **MADDE 13- SAKLAMA VE İMHA SÜRELERİ**

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş ise bu süreye riayet edilir.

#### **MADDE 14- PERİYODİK İMHA SÜRESİ**

Şirket her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

#### **MADDE 15- POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ**

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuoyuna ilan edilir. Basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

#### **MADDE 16- YÜRÜRLÜK**

Politika, şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile şirket tarafından saklanır.

#### **EK TABLO: 1 Saklama ve imha süreçleri görev dağılımı**

UNVANI	GÖREVİ
Veri Sorumlusu	Çalışanların politikaya uygun davranmasından sorumludur.
	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
	Politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.
--	--

### EK TABLO: 2 Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel bilgisayarlar Mobil Cihazlar Optik diskler Yazıcılar, tarayıcılar, fotokopi makineleri Çıkarılabilir ve taşınabilir bellekler Sunucular Yazılımlar Bilgi güvenliği cihazları Google Drive	Kağıtlar Yazılı ve basılı ortamlar Görsel kayıtlar Manuel veri kayıt sistemleri

### EK TABLO: 3 Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik ortam	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel ortam	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 medya	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.

**EK TABLO: 4 Kişisel Verilerin Yok Edilmesi Yöntemleri**

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel ortam	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medya	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 değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.