Buse Çolpan
Ağız ve Diş Sağlığı Polikliniği

**BUSE ÇOLPAN ÖZEL SAĞLIK HİZMELERİ SANAYİ ve TİCARET LİMİTED ŞİRKETİ**

**KİŞİSEL VERİ SAKLAMA, İMHA VE GİZLİLİK POLİTİKASI**

## 1. POLİTİKANIN NİTELİĞİ VE AMACI

İşbu Kişisel Veri Saklama ve İmha Politikası (bundan sonra 'Politika' olarak anılacaktır), Buse Çolpan Özel Sağlık Hiz.San.Ve Tic.Ltd.Şti. (bundan sonra 'Klinik' olarak anılacaktır) veri sorumlusu sıfatıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") ve sair mevzuat uyarınca kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin Klinik tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

İşbu Politika, Klinik'in Kişisel Verileri işlediği herhangi bir sürece dahil olan tüm departmanlarını, çalışanlarını, çalışan adaylarını, müşterilerini ve üçüncü kişileri kapsamaktadır.

## 2. TANIMLAR

**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.

**Hizmet Sağlayıcı:** Kişisel Verileri Koruma Kurumu 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.

**Yönetmelik:** 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

**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

**Kişisel Verileri Koruma Komitesi:** Şirket içindeki ilgili kişiler tarafından ve Veri Sorumlusu Başkanlığında oluşturulan komite. Kişisel Verilerin hukuka, Kişisel Veri Saklama ve İmha Politikasına ve Kişisel Veri Envanterine uygun olarak saklanması, imhası ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

**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 işlenme 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.
**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.
**Veri Sorumlusu:** Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
**VERBİS:** Veri Sorumluları Sicil Bilgi Sistemi

## 3. İLKELER

Klinik kişisel verilerin saklanması ve imha edilmesinde Kanun ve işbu politika çerçevesinde, aşağıdaki ilkeler ile hareket etmektedir.

**a)** Kişisel verilerin saklanması, silinmesi, yok edilmesi ve anonim hale getirilmesinde Kanun'un 4. maddesinde sayılan ilkeler ile yine Kanun'un 12. maddesi kapsamında alınması gereken tedbirlerle, ilgili mevzuatlar ve Kurul kararlarına ve işbu politika metnine uygun halde hareket edilmektedir.
**b)** Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ile ilgili tüm işlemler Kanun hükümleri, ilgili mevzuat ve işbu politika çerçevesinde Klinik tarafından kayıt altına alınmakta ve söz konusu kayıtlar diğer hukuki yükümlülükler hariç olarak Yönetmeliğin 7/3.maddesi gereğince 3 yıl süre ile saklanmaktadır.
**c)** Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Klinik tarafından seçilmektedir.
**d)** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde kişisel veriler Klinik tarafından veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.

## 4. TEDBİRLER

Klinik, kişisel verilerin güvenli bir şekilde saklanması ve hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile verilerin saklandığı ve muhafaza edildiği ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

### 4.1. Teknik Tedbirler

Klinik aşağıdaki uygun teknik tedbirleri almaktadır:

- Teknolojik gelişmelere uygun ve güvenli sistemler kullanmaktadır
- Kişisel verilerin tutulduğu ortamlara göre güvenlik sistemleri kullanmaktadır
- Kişisel verilerin tutulduğu ortamlara erişim kısıtlanmaktadır ve sadece yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişimine izin verilir (Veri Sorumlusu ve Kişisel Verileri Koruma Komitesi ve veri sorumlusu tarafından belirlenen diğer personel)
- Kişisel verilerin bulunduğu ortamların/sistemlerin güvenliğini sağlamak için yeterli sayıda personel bulundurmaktadır
- Kişisel verilerin işlendiği sistemlerde, yetki matrisi, yetki kontrolü, erişim logları, şifreleme, güvenlik duvarı, sızma testi ve log kayıtları tedbirlerini kullanmaktadır.

### 4.2. İdari Tedbirler

Klinik aşağıdaki uygun idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Klinik çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.
- Kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli tedbirleri almak için, şirket içi ve dışı ve kurum içi ve dışı denetimler yapılacaktır.
- Kişisel verilerin gereklilik halinde üçüncü kişilere aktarılması halinde, ilgili üçüncü kişilere kişisel verilerin korunması amacıyla protokoller imzalatılır ve bahse konu bu üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- Aydınlatma ve onam metinleri hazırlanmış ve tüm kişisel veri sahiplerine imzalatılmıştır.

- Gizlilik Taahhütnameleri hazırlanmış ve imzalanmıştır.
- Kişisel Veri İşleme Envanteri hazırlanmıştır.
- İşbu Saklama ve İmha Politikası hazırlanmış ve yayınlanmıştır.
- Veri İhlal Politikası hazırlanmıştır.

### 4.3. Şirket İçi Denetim

Kanunun 12. Maddesi, Veri güvenliğine ilişkin yükümlülükleri uyarınca Kanun hükümlerinin ve işbu Politikanın hükümlerinin uygulanmasına ilişkin, güncelleme gerekli olması halinde hemen veya her durumda 6 aylık periyodlarda şirket içi denetimler yapılmaktadır.
Bu denetimler Veri sorumlusu ve Kişisel Verileri Koruma Komitesi tarafından gerçekleştirilir ve bu denetimler sonucunda yükümlülüklere ilişkin bir eksiklik ya da kusur tespit edilirse ve/veya kanun hükümlerine aykırılık tespit edilirse, bu eksiklik ya da kusur derhal giderilir.
Denetim sırasında veya başka bir şekilde Klinik'in sorumluluğu altında bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması halinde bu durum Klinik tarafından en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurulu'na bildirilir.

## 5. KAYIT ORTAMLARI

Klinik, işbu Politika ile Kişisel Veri içeren ve aşağıda sayılmış olan ortamlar ve bunlara ek olarak ortaya çıkabilecek diğer ortamlardaki Kişisel Verileri Politikanın kapsamına dahil etmeyi kabul eder:

- Klinik'in tahsis ettiği ve/veya Klinik adına kullanılan bilgisayarlar/sunucular/sistemler
- Ağ cihazları
- Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
- Bulut Sistemleri
- Mobil telefonlar ve tüm saklama alanları
- Kağıt
- Yazıcı, Parmak izi okuyucu gibi çevre birimleri
- Optik diskler
- Arşiv
- Flash hafızalar
- Kamera kayıtları

## 6. KİŞİSEL VERİLERİN İMHASI

### 6.1. Saklama ve İmha Nedenleri

Kanun'un 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler Klinik tarafından re'sen veya ilgili kişinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.
Kanun'un 5. ve 6. maddelerince sayılan nedenler şu şekildedir:

- Kanunlarda açıkça öngörülmesi
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

### 6.2. İmha Yöntemleri

Klinik, KVKK ve ilgili mevzuata uygun olarak elde ettiği kişisel verileri işbu Politika kapsamında saklayacaktır. Ancak Kanun ve Yönetmelik'te sayılan Kişisel Verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde veya veri sahibi olan ilgili kişinin talebi doğrultusunda, yine Kanun, ilgili mevzuat ve işbu Politikanın belirlediği süreler içerisinde aşağıda da belirtilen teknikler ile re'sen silinir, yok edilir veya anonim hale getirilir. Klinik tarafından kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıdaki gibidir:

#### 6.2.1. Silme Yöntemleri

- Bulut ve yerel dijital ortamda tutulan kişisel veriler için silme yöntemleri ise yazılımdan güvenli olarak silmeden ibarettir. Tamamı veya bir kısmı otomatik olarak işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken, ilgili kullanıcıların hiçbir şekilde erişim ve tekrar kullanımın sağlanmamasına ilişkin yöntemler kullanılır. Kısacası bulut ortamında ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bu şekilde silinen verilere tekrar ulaşılamaz.

  Ancak, kişisel verilerin silinmesi sonucunda diğer verilerinde erişilmesine engel ve bu verileri kullanamamaya yol açacak ise, aşağıdaki koşulların sağlanması halinde kişisel verilerin kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

- Kağıt ortamında bulunan kişisel verileri silme yöntemi karartmadır. Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, amaca yönelik olmayan kullanımı önlemek, ilgili evrak üzerindeki kişisel verilerin mümkün olan durumlarda fiziksel olarak kesilerek belgeden çıkartılması, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi/kapatılması yöntemidir.

### 6.2.2. Yok Etme Yöntemleri

Matbu ortamda tutulan kişisel verileri yok edebilmek için fiziksel olarak evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok etmek gerekir.
Dijital ve bulut ortamda tutulan kişisel verileri yok etmek için kullanılabilecek yöntemler aşağıdaki gibidir:
**Fiziksel yok etme:** Bu yöntem, kişisel verileri barındıran optik ve manyetik medya aracının eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel yok etmeden ibarettir. Bahse konu medyanın eritilmesi, yakılması, toz haline getirilmesi veya metal öğütücüden geçirilmesi, kişisel veriyi erişilmez hale getirir.
**De-manyetize etme:** Manyetik medyanın daha yüksek manyetik alanlara maruz bırakılarak, özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Ancak bu yöntem başarısız olur ve medyanın üzerindeki veriler hala okunabilir halde olur ise, medya fiziksel olarak yok edilebilir ve yok etme işlemi tamamlanmış olur.
**Üzerine yazma:** Bu yöntem, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkansızlaştıran veri yok etme yöntemidir.
**Yazılımdan güvenli bir şekilde silme:** bu yöntemde ise kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir.

### 6.2.3. Anonim Hale Getirilmesi

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.
Klinik'in kişisel verilerin anonim hale getirilmesi tekniklerine ilişkin usul ve esaslar aşağıda sayılmıştır:

- Değişkenleri çıkarma yöntemi ile betimleyici nitelikteki verilerin yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden "yüksek dereceli betimleyici" olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir. Örneğin kişisel verilerin bulunduğu ortamdan (evrak, tablo vb.) kişisel verilerden yüksek derecede betimleyici olan veri gruplarının çıkartılması ile anonimleştirme sağlanabilecektir.
- Bölgesel gizleme yönteminde kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
- Alt ve üst sınır kodlama yöntemi ile belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Örneğin, bir işyerinde çalışan personelin işyerindeki çalışma yılının 5 yıldan az, 5 ila 10 yıl arasında veya 10 yıldan çok olmasına göre 'çok deneyimli', 'deneyimli' ya da 'deneyimsiz' olarak birleştirilerek anonim hale getirilebilir.
- Genelleştirme yöntemi ile birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgilerin kaldırılarak istatistik veri haline getirilmesi işlemidir.
- Veri karma ve bozma yöntemi ile kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karşılaştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmelerini sağlar.

**6.3. Saklama Süreleri**

Klinik, Kişisel Veri Envanterinde, işbu Politikada ve ilgili mevzuatta belirtilen yasal saklama ve imha sürelerini dolduran fiziksel ve dijital veriler, periyodik olarak imha edilir. Klinik, Kişisel Veri Envanteri, Kanun, ilgili mevzuat ve işbu Politika uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

| VERİ SAHİBİ | VERİ KATEGORİSİ | SAKLAMA SÜRESİ |
|---|---|---|
| Çalışan | İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen, hizmet süresine ve ücrete dair bildirimlere esas özlük veriler | Hizmet akdinin devamında ve hitamından itibaren de 10 yıl müddetle muhafaza edilir |
| Çalışan | İşyeri kişisel sağlık dosyası içeriğindeki veriler | Hizmet akdinin devamında ve hitamından itibaren de 10 yıl müddetle muhafaza edilir |
| Çalışan Adayı | İşe başvuru formunda yer alan kişisel sağlık verileri | Başvurunun alınmasından itibaren 5 yıl süre ile saklanır. |
| Çalışan Adayı | Çalışan adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler | Başvurunun alınmasından itibaren 5 yıl süre ile saklanır. |
| Çalışan | Ceza mahkumiyeti, çalışanın şirket aleyhine ya da şirketin çalışan aleyhine açtığı davalara ilişkin kişisel veriler | Çalışanın iş sözleşmesinin sona erdiği tarihten itibaren 10 yıl süre ile saklanır. |
| Çalışan | Faaliyet/İşin yerine getirilmesi için(vize, otel, sözleşme, vs.)alınan kişisel veriler | Çalışanın iş sözleşmesinin sona ermesinden itibaren 10 yıl süre ile saklanır. |
| Ziyaretçi | Klinik'e ait binaya girişte alınan Ziyaretçi'ye ait ad, soyad, TCKN, kamera görüntüleri telefon aramalarında alınan ses kayıtları | 3 ay süre ile saklanır |
| Hasta/Hasta Yakını | Hasta'ya ait kayıt formu ile elde edilen ad, soyad, TCKN, iletişim bilgileri, kimlik bilgileri gibi kişisel verileri ve laboratuvar tahil sonuçları, tıbbi anamnez sonuçları, kullanılan ilaç bilgisi gibi özel nitelikli verileri | Hasta ile yapılan hizmet sözleşmesinin sona ermesinden itibaren 10 yıl süre ile saklanır. |
| Hasta | Hasta'ya ait ad, soyad, TCKN, iletişim bilgileri, ödeme bilgileri ve yöntemleri, telefon aramalarında alınan ses kayıtları , hasta talep ve şikayetleri, işlem geçmişi, elektronik ortamda yazışmalar, imza beyannamesi bilgileri | Müşteri'nin satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunum. 146 ile Türk Ticaret Kanunu md. 82 uyarınca 10 yıl süre ile saklanır |

| | | |
|---|---|---|
| Hasta/Hasta Yakını | Kamera görüntüleri ve Klinik'in binasına girişinde alınan hasta/hasta yakını bilgileri | 3 ay süre ile saklanır |
| Klinik'in işbirliği içinde olduğu Kurum/Firmalar (Tedarikçi, Tıbbi destek ve malzeme temin edilen, firmalar vb.) | Klinik'in işbirliği içinde olduğu Kurum/Firmalar ile Klinik arasındaki ticari ve hizmet ilişkilerinin yürütülmesine dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, Kurum/Firma çalışanı verileri | Klinik'in işbirliği içinde olduğu Kurum/Firmaların, Klinik ile olan iş/ticari, ilişkisi sürecine ve sona ermesinden itibaren 10 yıl süre ile saklanır. |
| Ortaklar Kurulu İşlemleri | Ortaklar Kurulu işlemleri sürecinde alınan kimlik bilgileri, elektronik alanda yapılan yazışmalarda bulunan kişisel veri bilgileri, telefon aramalarında alınan ses kayıtları, Kurul üyelerine dair veriler | 10 yıl süre ile saklanır |

### 6.4. İmha Süreleri

Klinik, Kişisel Veri Envanteri, Kanun, ilgili mevzuat ve işbu Politika uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir.

Kişisel verileri işlenen ilgili kişi, Kanunun 13. Maddesince Klinik'e başvurarak kendisine ait kişisel verilerin silinmesi veya yok edilmesini talep edebilir.

Eğer ilgili kişi böyle bir talepte bulunursa ve kişisel verileri işleme şatlarının tamamı ortadan kalkmış ise, Klinik talebi aldığı günden itibaren 30 gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Ancak kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Klinik tarafından Kanunun 13. Maddesinin üçüncü fıkrasınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç 30 gün içinde yazılı olarak veya elektronik ortamda bildirecektir.

Klinik işleme şartları ortadan kalkmış olan kişisel verileri işbu Politikada belirtilen ve tekrar eden aralıklarla re'sen gerçekleşecek olan bir işlemle siler, yok eder veya anonim hale getirir. Periyodik imha süreçleri ilk kez 31 Ocak 2021 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

## 7. GİZLİLİK POLİTİKASI

Klinik, Kişisel Verileri faaliyet amaçları doğrultusunda ve bu amacın ifası için gerekli olan süre ve iş ortağı/tedarikçi/danışman/denetçi ya da üçüncü kişi ile arasındaki ticari ilişkinin devamı süresince ve/veya mevzuatta belirtilen süre ile sınırlı olarak Klinik nezdinde saklayacağını, söz konusu amacın ifası için üçüncü kişi konumundaki sağlayıcıların hizmetlerini kullanması halinde Kişisel Verileri üçüncü kişilere aktarabileceğini ancak bu halde söz konusu üçüncü kişilerin, Kanun hükümlerine riayet etmesini sağlayacağını bildirir.

Klinik, personeli ya da üçüncü kişi tarafından Kişisel Verilere yetkisiz erişilmesini ve Kişisel Verilerin aktarımı amacı dışında kullanılmasını engelleyecek şekilde, Kanun ve Yönetmeliğe uygun olarak teknik ve idari tedbirleri almakla yükümlüdür.

## 8) YÜRÜRLÜK

İşbu Politika, yayınlandığı tarihten itibaren yürürlüğe girecektir.

Klinik bünyesinde, Kanun'a uyum için gerekli aksiyonların takibi ve yönetilmesi amacıyla bir Kişisel Verilerin Korunması Komitesi kurulmuştur.

Ofis Yönetimi, Hekimler, Muhasebe ve Finans Departmanı ile İnsan Kaynakları Departmanından seçilecek çalışanlar olmak üzere en az iki (2) kişiden oluşur.