

ŞİFA SAĞLIK TESİSLERİ TİC.A.Ş
(PENDİK ŞİFA HASTANESİ)
6698 SAYILI KVKK KAPSAMINDA
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. BÖLÜM: İMHA POLİTİKASI'NIN NİTELİĞİ VE AMACI

GİRİŞ

Bu imha politikası ŞİFA SAĞLIK TESİSLERİ TİC.A.Ş ve PENDİK ŞİFA HASTANESİ olarak, veri sorumlusu sıfatıyla elde ettiğimiz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat gereğince kişisel verilerin silinmesi, yok edilmesi ve/veya anonim hale getirilmesine ilişkin uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Bu kapsamda, çalışanlarımızın, çalışan adaylarımızın, stajyerlerimizin, hastalarımızın, tedarikçilerimizin, ziyaretçilerimizin ve herhangi bir nedenle Şirket bünyesinde kişisel verisi bulunan tüm gerçek kişilerin kişisel verileri Kişisel Verilerin İşlenmesi ve Korunması Politikası ve bu Kişisel Veri Saklama ve İmha Politikası çerçevesinde kanunlara uygun olarak yürütülmektedir.

TANIMLAR

Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi
İlgili kişi	Kişisel verisi işlenen gerçek kişiyi,
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini
Kanun	07.04.2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununu, 28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğini
Yönetmelik	Kişisel Verileri Korunması Komitesi
Kurul / Komite	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı
Kayıt ortamı	https://www.pendiksifa.com.tr/kisisel-verilerin-korunmasi adresinde ve kurum içinde yayımlanan, Şirketin kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı
Kişisel Verilerin İşlenmesi ve Korunması Politikası	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
Veri kayıt sistemi	
Şirket	Şifa Sağlık Tesisleri Tic. A.Ş (Pendik Şifa Hastanesi)

2. BÖLÜM: ORTAMLAR VE GÜVENLİK TEDBİRLERİ

KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

Şifa Sağlık Tesisleri Tic A.Ş (Pendik Şifa Hastanesi) nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun şartlarda ve uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Şirket her durumda veri sorumlusu sıfatıyla hareket etmekte ve Kişisel Verileri Koruma Kanununa, Kişisel Verilerin İşlenmesi ve Korunması Politikasına (KE-03) ve bu Kişisel Veri Saklama ve İmha Politikasına (KVSİ-01) uygun olarak işlemek ve korumaktadır.

Yerel Matbu ortamlar	Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
Yerel dijital ortamlar	Şirket bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi tüm dijital ortamlardır.
Bulut ortamlar	Şirket bünyesinde yer almamakla birlikte, Şirket kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

Bu ortamlar her bir departmanda ayrı ayrı belirlenmiş, departman çalışanlarının görebilecekleri şekilde yazılı olarak asılmıştır.

ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

Şirket kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almakta ayrıca bu konudaki gelişmeleri takip etmektedir.

Bu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun olduğu ölçüde aşağıdaki idari ve teknik tedbirleri kapsar. Bu tedbirler bölüm bazında her bir departman için ayrı ayrı belirtilmiştir.

Teknik Tedbirler

Şirket kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.

İdari Tedbirler

Şirket kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Şirket çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için eğitim ve bilgilendirme çalışmaları yapılmaktadır.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla Gizlilik Sözleşmeleri imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.

Kurum İçi Denetimi

Şirket Kanununun 12. maddesi uyarınca Kanun hükümlerinin ve bu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin düzenli olarak kurum içi denetimler yapılmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik veya kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar en kısa zamanda giderilir.

Denetim sırasında ya da bir şekilde Şirket, sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, bu durumu en kısa sürede ilgisine ve KVK Komitesi Başkanına (72 saat içerisinde) bildirir.

3. BÖLÜM: KİŞİSEL VERİLERİN İMHASI

SAKLAMA VE İMHA NEDENLERİ

Saklama Nedenleri

Şirket bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız (ilgili politika için <https://www.pendiksifa.com.tr/kisisel-verilerin-korunmasi> ziyaret ediniz.) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

İmha Nedenleri

Şirket bünyesinde bulunan kişisel veriler, ilgili kişinin talebi halinde ya da Kanunun 5. ve 6. maddelerinde sayılan nedenlerin ortadan kalkması halinde re'sen bu imha politikası uyarınca silinir, yok edilir veya anonim hale getirilir.

Kanunun 5. ve 6. maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

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 işlenmesinin zorunlu olması,

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması,

İMHA YÖNTEMLERİ

Şirket Kanuna ve ilgili mevzuat ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da bu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir.

Karartma

Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünmez hale getirilmesi şeklinde yapılır.

Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Yazılımdan güvenli olarak silme

Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme

Matbu ortamda tutulan belgeler evrak imha makineleri veya belgenin birleştirilmesi mümkün olmayacak şekilde parçalara ayrılarak tekrar bir araya getirilemeyecek şekilde yok edilir.

Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme

Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

De-manyetize etme (degauss)

Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

Üzerine yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine en az

yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.

Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Yazılımdan güvenli olarak silme

Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da bir kaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabilmesi gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla kullanılabilir.
Bölgesel gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
Genelleştirme	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.
Alt ve üst sınır kodlama / Global kodlama	Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir. Aynı kategori içinde kalan değerler birleştirilir.
Mikro birleştirilme	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olduğundan, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.
Veri karma ve bozma	Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

SAKLAMA VE İMHA SÜRELERİ

Saklama Süreleri

VERİ SAHİBİ

Çalışan

VERİ KATEGORİSİ

İşe alım evrakları ile Sosyal

VERİ SAKLAMA SÜRESİ

Hizmet akdinin sona

	Güvenlik Kurumuna gerçekleştirilen hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	ermesinden itibaren 15 yıl, hukuki bir süreç işliyorsa süreç sona erene kadar muhafaza edilir.
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	Hizmet akdinin sona ermesinden itibaren 15 yıl, hukuki bir süreç işliyorsa süreç sona erene kadar muhafaza edilir
Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin sona ermesinden itibaren 15 yıl, hukuki bir süreç işliyorsa süreç sona erene kadar muhafaza edilir
İş Ortağı/Çözüm Ortağı/Danışman	İş Ortağı/Çözüm Ortağı/Danışman ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	10 yıl süre ile saklanır.
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 1 yıl saklanır.
Stajyer(öğrenci)	Stajyer'e ait staj dosyasında yer alan bilgiler	Stajın sona ermesinden itibaren 15 yıl, hukuki bir süreç işliyorsa süreç sona erene kadar muhafaza edilir
Müşteri	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri	Özel Hastaneler Yönetmeliği gereği en az 20 yıl süre ile saklanır. Hukuki bir süreç işliyorsa süreç sona erene kadar muhafaza edilir.
Müşteri/Hasta/Ziyaretçi/Çalışan vs.	Kamera görüntüleri	Özel Hastaneler Yönetmeliği gereği en az 2 ay süre ile saklanır.
Potansiyel Müşteri	Potansiyel Müşteri ile Şirket arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi,	2 yıl süre ile saklanır.

finansal bilgiler vb. bilgiler

Şirketin İşbirliği İçinde Olduğu Kurum/Firmalar (Tedarikçi, Hizmet Alımı vs.)	Şirketin İşbirliği İçinde Olduğu Kurum/Firmalar ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, Şirketin İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri	Sözleşmenin sona ermesinden itibaren 10 yıl süre ile saklanır. Hukuki bir süreç işliyorsa süreç sona erece kadar muhafaza edilir.
---	--	---

NOT: Kanun ve diğer mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

İmha Süreleri

Şirket, Kanun, ilgili diğer mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve bu Kişisel Verileri Saklama ve İmha Politikası 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.

İlgili kişi, Kanunun 11. ve 13. maddesine istinaden Şifa Sağlık Tesisleri Tic.A.Ş (Pendik Şifa Hastanesi)'ne başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Şirket talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Şirket her halde yapılan işlemle ilgili, ilgili kişiye bilgi verir.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, Şirket tarafından Kanunun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak ret edilebilir ve ret cevabı ilgili kişiye en geç 30 (otuz) gün içinde yazılı olarak ya da uygun yöntemlerle bildirilir.

PERİYODİK İMHA

Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri bu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

Şirket, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve bu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

Teknik Tedbirler

Şirket;

- Bu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
- İmha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- İmha işlemini yapan kişilerin erişim kayıtlarını tutar.
- İmha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder veya gerektiğinde yetkin üçüncü kişilerden hizmet alır.

İdari Tedbirler

Şirket;

- İmha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- Bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- Teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- İmha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklerle uygun olarak yapıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere süresiz saklar.

4. BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI KOMİTESİ

Şirket, bünyesinde bir Kişisel Verilerin Korunması Komitesi kurar. Kişisel Verilerin Korunması Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Saklama ve İmha Politikasına ve KVKK kapsamında hazırlanan diğer Protokollere uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve bu süreçleri denetlemekle, 6698 sayılı yasa kapsamında tüm işleri yürütmekle yetkili ve görevlidir. Bu komite Hastane İçi Görevlendirme ve Atama Formu (FORM444) nda tanımlanmıştır.

Kişisel Verilerin Korunması Komitesi; bir yönetici, bir idari ve bir teknik personel olmak üzere üç kişiden oluşur. Kişisel Veri Komitesinde görevli Şifa Sağlık Tesisleri Tic. A.Ş (Pendik Şifa Hastanesi) çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

Unvan

**Kişisel Veri Komitesi
Yöneticisi**

Görev Tanımı

Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını

yapmak/yaptırmak/yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.

**KVK Personeli
(Teknik ve İdari)**

İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

Toplanma Periyodu: 6 Ayda bir veya gerekli oldukça.

5. BÖLÜM: GÜNCELLEME VE UYUM

Şifa Sağlık Tesisleri Tic. A.Ş (Pendik Şifa Hastanesi) Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca veya sektöründeki veya bilişim alanındaki gelişmeler doğrultusunda Kişisel Verilerin İşlenmesi ve Korunması Politikasında veya bu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.

Bu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişiklikler yayımlandığı tarihte yürürlüğe girer. Bu Politika Şirketimizin internet sitesinde (www.pendiksifa.com.tr) yayınlanır.