

KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ – GİZLİLİK POLİTİKASI

GİRİŞ

Bu Politika ile kişisel verilerin işlenmesi ve korunması konusunda RFM ANKARA RENAL TEDAVİ HİZMETLERİ

A.Ş. tarafından benimsenecek ve uygulama noktasında dikkate alınacak ilkeler ortaya konulmaktadır. Bu Politika ile RFM RENAL tarafından yerine getirilecek hususlar ortaya konulmakta, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("KVKK") öngörülen düzenlemelere nasıl uyacağına ilişkin temel ilkeler belirlenmektedir.

AMAÇ

Bu Politika RFM RENAL düzeyinde kişisel verilerin işlenmesi ve korunması konusunda KVKK'ya uyum sağlamak amacıyla ilgili tüm grup şirketleri özelinde yürütülecek uyum faaliyetlerinin en üst düzeyde yönetilmesini ve eşgüdümün sağlanmasını temin etmek hedefiyle hazırlanmıştır.

RFM RENAL , tarafından belirlenen ilkeler doğrultusunda iç işleyişlerini uyum için gerekli düzenlemeleri yapacak çalışanlarının ve iş ortaklarının farkındalığının oluşması için gerekli sistemi oluşturacaktır.

I. KİŞİSEL VERİLERİN İŞLENMESİNDE UYGULANACAK İLKELER

Bu Politika, RFM RENAL 'nin KVKK ve ilgili mevzuat tarafından ortaya konulan kuralları somut olarak nasıl uygulayacaklarına ilişkin yol gösterici bir nitelik taşımaktadır.

RFM RENAL bu Politikayı rehber edinerek kendi bünyelerinde gerçekleştirdikleri kişisel veri işleme faaliyetlerini analiz edecek, bu Politikaya uyum için gerekli aksiyonları belirleyecek ve her türlü teknik ve idari önlemi alacaklardır. Belirlenen aksiyonlar hayata geçirildikten sonra iç denetim mekanizmaları işletilerek Politikaya uygunluğun devamlılığı sağlanacaktır.

RFM RENAL bünyesinde bu Politikaya uyumluluğun sağlanması amacıyla çalışanların farkındalığının sağlanması için çalışmalar yapılacak, yeni başlayan çalışanlar için gerekli uyum süreçleri işletilecek ve RFM RENAL nin iş ortakları ile ilişkilerinde gerekli düzenlemeler yapılacaktır.

KVKK'ya uyumluluğun sağlanması için RFM RENAL tarafından kişisel veriler mevzuatta öngörülen genel ilke ve hükümlere uygun olarak işlenmelidir. Bu kapsamda, RFM RENAL tarafından tüm kişisel veri işleme faaliyetlerinde dikkate alınması gereken ilke ve şartlar bu bölümde ele alınacaktır.

Kişisel verilerin işlenmesi sırasında dikkate alınacak ilkeler aşağıda başlıklar halinde incelenmektedir.

1.1. Hukuka ve Dürüstlük Kuralına Uygun Kişisel Veri İşleme Faaliyetlerinde Bulunma

RFM RENAL kişisel verilerin işlenmesi faaliyetleri kapsamında hukuka ve dürüstlük kurallarına uygun hareket etmelidir. Bu kapsamda RFM RENAL , kişisel verilerin işlenmesinde orantılılık ve gereklilik prensiplerini uygulamaya koyarak sadece gerektiği kadar kişisel veriyi, veri işleme amaçlarına uygun düşecek seviyede işlemelidirler.

1.2. Kişisel Verilerin Doğru ve Gerekliğinde Güncel Olmasını Sağlama

RFM RENAL, işlemekte oldukları kişisel verilerin doğru ve güncel olmasını sağlamalı ve bu doğrultuda gerekli tedbirleri almalıdır. Örneğin, RFM RENAL kişisel veri sahiplerinin kişisel verilerini düzeltmelerine ve güncelleştirmelerine imkân verecek sistemleri geliştirmelidir.

1.3. Belirli, Açık ve Meşru Amaçlarla İşleme

RFM RENAL , kişisel verileri belirli, açık ve hukuka uygun sebeplerle işlemelidir. Bu kapsamda RFM RENAL kişisel verilerin hangi amaçla işleneceğini belirlemeli ve bu amaçları kişisel verileri işlenmeden önce veri sahiplerinin bilgisine sunmalıdır. Kişisel veriler, belirtilen amaçlar dışında işlenmemelidir. RFM RENAL tarafından belirlenen veri işleme amaçları meşru ve hukuka uygun olmalıdır.

1.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

RFM RENAL , kişisel verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işlemeli ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin

işlenmesinden kaçınmalıdır. Örneğin, kişisel veriler elde edildikten sonra ortaya çıkan yeni bir amacın gerçekleştirilmesine yönelik kişisel veri işleme faaliyeti yürütülmemelidir.

1.5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Etme

RFM RENAL kişisel verileri yalnızca kanunlarda öngörülen süreler ile veya işlendikleri amaç ile sınırlı olarak muhafaza etmelidir. Bu kapsamda, ilgili mevzuatta kişisel verilerin saklanması için bir süre belirlenmişse bu süreye uygun davranmalıdır. Bir süre belirlenmemişse, kişisel veriler işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

II. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Kişisel veriler kural olarak, KVKK'nın 5 numaralı maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı olarak işlenmelidir. Bu kapsamda RFM RENAL kişisel veri işleme faaliyetlerinin bu şartlardan birinin kapsamına girip girmediğini değerlendirmeli ve bu şartlardan birine dayanmayan kişisel veri işleme faaliyetleri durdurulmalıdır.

KVKK'da özel nitelikteki kişisel verilerin işlenmesi için özel önlemler getirilebileceği düzenlenmiştir. Bu kapsamda özel nitelikli kişisel veriler işlenirken Kurul tarafından belirlenecek önlemler alınmalıdır.

Kişisel verilerin yurt içinde veya yurt dışında üçüncü kişilere aktarılması konusunda, KVKK'nın 8 ve 9 numaralı maddelerinde öngörülen düzenlemelere uygun hareket etmeye yönelik gerekli organizasyonel sistemler kurgulanmalıdır. Kişisel veriler aktarılırken işleme amaçları doğrultusunda gerekli güvenlik önlemleri alınmalıdır.

Kişisel verilerin hukuka aykırı işlenmesinin önüne geçilmesi adına şirketler içerisinde gerekli sistemler kurgulanmalı ve kurum içi farkındalık yaratılmalıdır.

III. RFM RENAL'İN YÜKÜMLÜLÜKLERİ

3.1. Kişisel Veri Sahibini Aydınlatma Yükümlülüğü

RFM RENAL , kişisel verilerin elde edilmesi sırasında verileri işlenecek kişileri, verilerinin ne şekilde işleneceği konusunda aydınlatılmalıdır. KVKK'da, bilgilendirmede yer alması gereken asgari hususlar sayılmıştır. Bu bilgiler aşağıdaki gibidir:

- (1) Veri sorumlusu olarak RFM RENAL 'nin ve varsa temsilcisinin kimliği,
- (2) Kişisel verilerin hangi amaçla işleneceği,
- (3) Kişisel verilerin kimlere ve hangi amaçla aktarılacağı,
- (4) Kişisel veri toplamanın yöntemi ve hukuki sebepleri,
- (5) Kişisel veri sahibinin sahip olduğu haklar.

Bu kapsamda, RFM RENAL tarafından öncelikle kişisel veri toplama kanalları tespit edilmeli ve her kanal özelinde aydınlatma noktaları ve metinleri belirlenmelidir.

3.2. Kişisel Veri Sahiplerinin Başvurularını Yanıtlandırma Yükümlülüğü

Kişisel veri sahipleri, yazılı olarak veya Kurul'un belirleyeceği diğer yöntemlerle başvuruda bulunarak kendi verilerine ilişkin KVKK'da yer alan haklarını kullanabilirler.

Bu kapsamda, RFM RENAL , kişisel veri sahiplerinin haklarının yerine getirilmesi için KVKK'nın 13 numaralı maddesi kapsamındaki yükümlülüklerini yerine getirmek için gereken idari ve teknik önlemleri almalıdır.

KVKK kapsamında kişisel veri sahipleri aşağıdaki haklara sahiptir:

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Kişisel veri sahiplerinin yalnızca yazılı olarak RFM RENAL ye iletilen talepleri işleme alınmalıdır. İleride Kurul tarafından farklı başvuru yöntemleri belirlenebilecektir. RFM RENAL talebin niteliğine göre ilgili talebi en kısa sürede ve en geç otuz gün içinde yanıtlandırmalıdır. Değerlendirme sonucunda RFM RENAL başvuruları kabul ederek gereken aksiyonları alabilecekleri gibi başvuruları gerekçeli olarak reddedebilirler.

Önemle belirtmek gerekir ki kişisel veri sahibi, başvurusunun reddedilmesi, verilen cevabı yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde 30 gün içerisinde Kurul'a şikayette bulunabilir. Bu şikayetleri engellemek adına kişisel veri sahiplerine zamanında ve tatmin edici cevaplar verilmesi önem arz etmektedir.

3.3. Kişisel Verilerin Güvenliğini Sağlama Yükümlülüğü

RFM RENAL işlemekte oldukları kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini engellemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almalıdır.

Kurul ileride veri güvenliğine ilişkin yükümlülükler hakkında detaylı düzenlemeler getirebilecektir. Dolayısıyla bu kapsamdaki yükümlülüklere de uyum sağlamak amacıyla makul derecede efor sarf ederek maksimum derecede güvenlik sağlanmalıdır.

RFM RENAL , alacağı teknik ve idari tedbirler bakımından tedbirlerin işleyişi ile ilgili olarak gerekli denetimleri yapmaya ve yaptırmaya yönelik sistemleri kurgulamalıdır. Bu denetim sonuçları RFM RENAL bünyesinde görevli birimlerce incelenmeli ve gerekli aksiyonlar alınmalıdır.

RFM RENAL , işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede ilgili kişisel veri sahibine ve mevzuatın gerektirmesi halinde Kurul'a bildirmekle yükümlüdürler. Bu kapsamda gerekli organizasyonel yapı kurulmalıdır.

RFM RENAL tarafından güvenlik riski teşkil eden durumlar tespit edilirse vakit kaybetmeksizin söz konusu riski ortadan kaldıracak önlemler alınmalıdır.

3.3.1. Hukuka Uygun Veri İşlenmesinin Temini İçin Teknik ve İdari Tedbirlerin Alınması

Kişisel verilerin hukuka uygun işlenmesi için aşağıdaki tedbirler RFM RENAL tarafından alınmalıdır:

RFM RENAL bünyesindeki veri işleme faaliyetlerine ilişkin tüm süreçler iş birimleri bazında analiz edilmeli, bu kapsamda bir "kişisel veri işleme haritası" çıkartılmalıdır.

Kişisel veri işleme haritası uyarınca, hukuka uygunluğun sağlanması için yerine getirilecekler birim bazında belirlenmelidir.

Gerçekleştirilen kişisel veri işleme süreçleri geliştirilecek teknik sistemlerle denetlenmeli ve ilgisine raporlanmalıdır.

RFM RENAL çalışanları, kişisel verilerin hukuka uygun olarak işlenmesi ve hukuka aykırı veri işlemenin yaptırımları konusunda bilgilendirilmeli ve eğitilmelidir.

Çalışanlarda farkındalığın sağlanması için düzenli denetimler yapılmalı ve gerekli idari tedbirler RFM RENAL 'nin iç politikaları ve eğitimleri yoluyla hayata geçirilmelidir.

RFM RENAL ile çalışanları, iştirakleri, iş ortakları, tedarikçileri ve müşterileri arasındaki hukuki ilişkiyi yöneten sözleşme ve belgelere, paylaşılan kişisel verilerin gizliliğine ve ne şekilde işlenmesi ve saklanması gerektiğine ilişkin kayıtlar konulmalıdır.

Kişisel verilere erişim, işleme amacı doğrultusunda görevli çalışanlarla sınırlandırılmalıdır. Çalışanların, görevleri gereği kullanmadıkları kişisel verilere erişimleri sınırlandırılmalıdır.

3.3.2. Kişisel Verilere Hukuka Aykırı Erişimi Engellemek için Teknik ve İdari Tedbirlerin Alınması

Kişisel verilere hukuka aykırı erişimi engellemek için aşağıdaki tedbirler RFM RENAL tarafından alınmalıdır:

Kişisel verilerin saklandığı sistem ve konumlara erişimin engellenmesi için teknolojiye uygun teknik önlemler alınmalı, alınan önlemler periyodik olarak güncellenmelidir.

RFM RENAL tarafından, iş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak erişim ve yetkilendirme teknik süreçleri tasarlanmalı devreye

alınmalıdır. Alınan teknik önlemler periyodik olarak ilgisine raporlanmalı, güvenlik riski olan hususlara teknolojik çözüm

üretilmektedir. Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar da dâhil ilgili yazılım ve sistemler kurulmalıdır. RFM RENAL 'nin çalışanları, bu kapsamda alınan teknik tedbirler

konusunda eğitilmeli ve teknik konularda bilgili personel istihdam edilmelidir. RFM

RENAL çalışanlarından, öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak

başkasına açıklamayacakları ve işleme amacı dışında kullanamayacakları konusunda taahhüt alınmalıdır. Bu taahhüt işten ayrılmalarından sonra da devam edecektir. RFM RENAL tarafından kişisel verilerin aktarıldığı kişiler ile akdedilen sözleşmelere, kişisel

verilerin korunması amacıyla gerekli güvenlik tedbirlerinin alınmasına ilişkin hükümler eklenmelidir.

3.4. Veri Sorumluları Siciline Kaydolma Yükümlülüğü

RFM RENAL , veri işlemeye başlamadan önce Kurul tarafından belirlenerek ilan edilecek süre içinde, KVKK'da sayılan başvuru bilgi ve belgelerini sunarak Veri Sorumluları Sicili'ne kayıt olmalıdır. Sunulacak bilgiler aşağıdaki gibidir (Kurul tarafından çıkarılacak ikincil düzenlemeler ile ek bilgi ve belgelerin talep edilmesi mümkündür):

- (1) Veri sorumlusu olarak RFM RENAL 'nin ve varsa temsilcisinin kimlik ve adres bilgileri,
- (2) Kişisel verilerin hangi amaçla işleneceği,
- (3) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- (4) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- (5) Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- (6) Kişisel veri güvenliğine ilişkin alınan tedbirler,
- (7) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

IV. RFM RENAL BÜNYESİNDE ORGANİZASYONEL YAPILANMA

RFM RENAL bünyesinde işbu politika ve bu politikaya bağlı ve ilişkili diğer politikaları yönetmek üzere, üst yönetim tarafından uyum için belirlenen aksiyonların yerine getirilmesinden sorumlu "Kişisel Verilerin Korunması Komitesi" veya bu konuda sorumlu olacak kişi atanmalıdır.

Bu kapsamda Komite veya atanacak kişi tarafından aşağıda sıralanan asgari aksiyonlar alınmalıdır:

Kişisel verilerin işlenmesi ve korunması ile ilgili temel politikaları ve mevzuatla uyum sağlanması için yapılması gerekenleri

belirlemek, Belirlenen temel politika ve aksiyon adımlarını üst yönetimin onayına sunmak; uygulanmasını gözetmek ve koordinasyonunu sağlamak,

Kişisel verilerin işlenmesi ve korunmasına ilişkin politikaların ne şekilde uygulanacağına ve denetimin ne şekilde yapılacağına karar vermek, üst yönetimin onayını aldıktan sonra gerekli görevlendirmelerde

bulunmak, Şirketin kişisel veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini üst yönetimin onayını sunmak, Çalışanların kişisel verilerin korunması ve Şirket politikaları konusunda eğitilmelerini sağlamak, Kişisel veri sahiplerinin başvurularını en üst düzeyde karara

bağlamak, Şirketin KVKK kapsamındaki yükümlülüklerini yerine getirmesi için şirket içinde gerekli düzenlemelerde

bulunmak, Kişisel verilerin korunması konusundaki gelişmeleri takip etmek; bu gelişmeler kapsamında yapılması gerekenler konusunda üst yönetime tavsiyelerde bulunmak,

Kurum ve Kurul ile olan ilişkileri yönetmek.

EK-1 TANIMLAR

Açık Rıza	:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	:	Kişisel verinin, kişisel veri niteliğini kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Ör: Maskeleye, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.
Kişisel Veri Sahibi	:	Kişisel verisi işlenen gerçek kişi. Örneğin; müşteriler ve çalışanlar. Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Veri	:	Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. Örneğin; ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası vb.
Özel Nitelikli Kişisel Veri	:	İrk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.
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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Veri İşleyen	:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir. Örneğin, bir şirketin müşteri verilerini saklayan bilişim firması.
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten kişi veri sorumlusudur.