

PROF.DR.MUSTAFA LEVENT EMİR

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN GÜVENLİĞİNE İLİŞKİN POLİTİKA

01.02.2021

A. Amaç ve Kapsam

Mefa Plaza, Mustafa Kemal Mah. 2148. Sokak, 1/13, 3. Kat, 06460 Çankaya/Ankara adresinde muayenehane işleten Prof.Dr.Mustafa Levent Emir, kişisel verilerin korunması ve işlenmesine ilişkin olarak, başta 6698 sayılı Kişisel Verilen Korunması Kanunu (“**KVKK**”) olmak üzere, ilgili diğer mevzuat ve Kişisel Verileri Koruma Kurulu (“**Kurul**”) kararlarında belirtilen tüm yükümlülüklerle uyum amacıyla, yeni gelişmeleri takip etmekte, muayenehanesinin bu yöndeki politikalarını ve planlarını güncellemektedir.

Muayehanesindeki faaliyetleri kapsamında, Prof.Dr.Mustafa Levent Emir başta kişilerin sağlığına ilişkin veriler olmak üzere, kişisel veriler işlemektedir. Bu kişisel verilerin nelerden ibaret olduğu ve hangi amaç ve hukuki sebeplerle işlendiği, kimler ile paylaşılabileceği gibi hususlar, KVKK madde 10 “*Veri Sorumlusunun Aydınlatma Yükümlülüğü*” kapsamında hazırlanan KVKK Aydınlatma Metninde açıklanmıştır.

Prof.Dr.Mustafa Levent Emir’un hastalarına ilişkin olarak işlediği sağlık verileri özel nitelikli kişisel veri sayıldığı için, prof.Dr.Mustafa Levent Emir, KVKK’dan doğan genel yükümlüklerinin yanında bir de özel nitelikli kişisel verilerin korunmasına ilişkin yükümlülüklerle uymak için gerekli önlemleri almaktadır.

İşbu Özel Nitelikli Kişisel Verilerin Güvenliğine İlişkin Politika (“**Politika**”), veri sorumlusu Prof.Dr.Mustafa Levent Emir tarafından, Kurulun “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” ile ilgili 31/01/2018 tarihli ve 2018/10 sayılı kararına uyum amacıyla hazırlanmıştır. İlgili kararda belirtilen tüm teknik tedbirler işbu Politika’da da listelenmiştir. Ancak önemli olan işbu Politika’nın sürdürülebilir olmasıdır. Dolayısıyla, Prof.Dr.M.Levent Emir, uygulaması maddi olarak büyük külfet yaratacak teknik tedbirlerden imtina edip bunların yerine uygulaması daha makul olan tedbirler benimseyebilecek,

gerektikçe işbu Politika'da listeli tedbirleri değiştirebilecektir. İşbu Politika'nın sonuna eklenen ekler de, işbu Politika'nın bir parçasını oluşturmaktadır.

İşbu Politika kapsamında, “*kişisel veri*”, “*özel nitelikli kişisel veri*”, “*kişisel verilerin işlenmesi*” ve “*veri ihlali*” kavramlarından ne anlaşılması gerektiği şu şekilde açıklanmaktadır:

- Başta Prof.Dr.M.Levent Emir hastalarına ilişkin bilgiler dahil olmak üzere, KVKK madde 3/1 (d) bendinde ifade edildiği şekliyle, “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*”, işbu Politika kapsamında “*kişisel veri*” ya da “*veri*” tanımını oluşturmaktadır.
- Başta Prof.Dr.M.Levent Emir hastalarına ilişkin sağlık verileri dahil olmak üzere, madde 6/1'de ifade edildiği şekliyle “*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*”, işbu Politika kapsamında “*özel nitelikli kişisel veri*” tanımını oluşturmaktadır.
- KVKK madde 3/1 (e) bendinde ifade edildiği şekliyle “*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 işlemi*”, işbu Politika kapsamında “*kişisel verilerin işlenmesi*” tanımını oluşturmaktadır.

İşbu Politika, kural olarak, Prof.Dr.M.Levent Emir'in'un faaliyetleri kapsamında işlediği özel nitelikli kişisel veriler için uygulanacaktır. Ancak, Prof.Dr.M.Levent Emir'in gerekli görmesi durumunda, işbu Politika'yı, özel nitelikli veri tanımı dışında kalan kişisel veriler için de uygulayabilecektir.

B. Özel Nitelikli Kişisel Verilerin İşlendiği Ortam ve Alınacak Tedbirler

1. Elektronik Ortamlar

Prof.Dr.M.Levent Emir'in muayenehanesindeki faaliyetleri kapsamında işlediği özel nitelikli kişisel veriler, muayenehanesindeki bilgisayarlara kaydedilmektedir ve yine bu bilgisayarlarda saklanmaktadır.

Kurulun “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” ile ilgili 31/01/2018 tarihli ve 2018/10 sayılı kararı gereğince, özel nitelikli

kişisel verilerin işlendiği elektronik ortamlara yönelik olarak aşağıdaki tedbirlerin alınması gerekmektedir:

- Kişisel verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- Kişisel veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak Loglanması,
- Kişisel verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- Kişisel 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,
- Kişisel verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması.

2. Fiziksel Ortamlar

Prof.Dr.M.Levent Emir'in muayenehanesindeki faaliyetleri kapsamında işlediği özel nitelikli kişisel veriler, hastaların doldurdukları formlar, test sonuçları gibi kağıt üzerine kaydedilmiş olabilir. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam, yani kâğıt ise aşağıdaki tedbirlerin alınması gerekmektedir:

- Söz konusu kâğıt belgelerin dosyalanarak güvenli bir ortamda saklanması,
- 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.

C. Özel Nitelikli Kişisel Verilerin İşlenmesi Süreçlerinde Yer Alan Kişilere Yönelik Tedbirler

Prof.Dr.M.Levent Emir bünyesinde özel nitelikli kişisel veriler dahil, elektronik ortamda tutulan kişisel verilerin işlendiği bilgisayarlara ancak kullanıcı adı ve şifresi ile giriş yapılabilmektedir. Bu şifreye yalnızca Prof.Dr.M.Levent Emir'e ilişkin kişisel verilerin işlenmesi süreçlerinde görev alan kişiler sahip olacak ve sisteme giriş yaparak, özel nitelikli kişisel veriler dahil, tüm kişisel verilere erişim sağlayabilecektir. Bu yetkiye sahip kişiler, aşağıdaki kişilerden ibarettir:

Ad ve Soyadı	Görevi	Yetkinin Süresi	Yetkinin Kapsamı
Prof.Dr.M.Levent Emir	Doktor	Aksi karar alınıncaya kadar	Muayenehanenin bu konudaki tüm politikalar ile bağlı olmak üzere tam erişim

Yukarıda açıklandığı üzere, Op. Dr. Selçuk Aksoy’a ilişkin özel nitelikli kişisel veriler dahil, kişisel verilerin fiziksel ortamlara da işlenmesi söz konusu olabilecektir. Bu fiziksel ortamlardaki belge ve dosyalara, aşağıdaki yetkisine sahip kişiler aşağıdaki kişilerden ibarettir:

Ad ve Soyadı	Görevi	Yetkinin Süresi	Yetkinin Kapsamı
Prof.Dr.M.Levent Emir	Doktor	Aksi karar alınıncaya kadar	Muayenehanenin bu konudaki tüm politikaları ile bağlı olmak üzere tam erişim

Prof.Dr.M.Levent Emir’e ilişkin özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan bu kişiler ile bir gizlilik sözleşmesi imzalanacaktır. Ayrıca, bu kişilere, KVKK ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi sağlanacaktır.

Prof.Dr.M.Levent Emir, periyodik olarak bu kişilerin yetkilerini kontrol edecek, gerektiği takdirde, bu kişilerin yetkilerini kısıtlayabilecek veya tamamen sonlandırabilecektir. Bu kişilerin, Prof.Dr.M.Levent Emir’e ilişkin kişisel verilerin işlenmesi süreçlerindeki görevleri sona ererse, bu kişilerin yetkileri derhal kaldırılacaktır.

D. Özel Nitelikli Kişisel Verilerin Aktarılması

Prof.Dr.M.Levent Emir hastalarına ilişkin sağlık verileri başta olmak üzere, özel nitelikli kişisel veriler, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla Sağlık Bakanlığı, İl Sağlık Müdürlüğü başta olmak üzere resmi mercilere, kamu hastaneleri ve özel hastanelere, polikliniklere, laboratuvarlara, doktorlara, özel sigorta şirketlerine, bankalara aktarılabilmektedir. Özel nitelikli kişisel veriler aktarılırken aşağıdaki tedbirlerin alınması gerekmektedir:

- 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 veya sFTP yöntemiyle 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,
- Sağlık verilerinin, 21/06/2019 tarihli Resmi Gazete’de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik madde 15 gereği, teknik altyapının uygun olması hâlinde KamuNET üzerinden aktarılması.

E. Veri Güvenliğine İlişkin Ek İdari ve Teknik Tedbirler

21/06/2019 tarihli Resmi Gazete’de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik madde 18 gereği, Prof.Dr.M.Levent Emir, hastalarına ilişkin sağlık verileri başta olmak üzere, özel nitelikli kişisel verilerin güvenliğine ilişkin olarak EK-1’de sunulan ve Kurum tarafından hazırlanan Kişisel Veri Güvenliği Rehberi’nde açıklanan idari ve teknik tedbirler, Prof.Dr.M.Levent Emir’un uygulamalarında esas alınacaktır.

Bunların haricinde, Prof.Dr.M.Levent Emir, özel nitelikli kişisel veriler dahil olmak üzere muayenehane faaliyetleri kapsamında işlenen tüm kişisel verilerin güvenliğine ilişkin olarak EK-2’de listelen teknik ve idari tedbirlerden kendisine uygun olarak alabilecektir.

F. Hukuki Tedbirler

Alınması gereken hukuki tedbirler kapsamında, Av. Doğan Berk Aksoy tarafından gerekli düzenlemeler yapılmaktadır.

G. Sonuç ve Hedefler

İşbu Politika, başta yukarıda sayılan, özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan yetkili kişiler ile paylaşılacak olup; KVKK, ilgili mevzuat ve Kurul kararları ve Prof.Dr.Mustafa Levent Emir politikaları gerektiğinde yenilenecektir.

Politika ile şu hedeflere ulaşılması amaçlanmaktadır:

- Özel nitelikli kişisel verilerin korunmasına ilişkin olarak farkındalığın artırılması,
- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belirlenmiş, yönetilebilir ve sürdürülebilir bir politika ve prosedürün belirlenmesi,

- Prof.Dr.Mustafa Levent Emir’in özel nitelikli kişisel verilerin korunması politikasındaki eksikliklerin tespit edilmesi ve bu eksiklikler üzerinde çalışılarak, Prof.Dr.Mustafa Levent Emir tarafından veri ihlallerini en aza indirecek idari ve teknik önlemlerin alınması.

İşbu Politika, imzalanması ile yürürlüğe girer.

Prof.Dr.Mustafa Levent Emir

Tarih:

İmza

EK-1

Kişisel Verileri Koruma Kurumu Kişisel Veri Güvenliği Rehberi

https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, erişim tarihi: 28.01.2021.

EK-2

Alınabilecek Teknik ve İdari Tedbirler Listesi

- Ağ güvenliği ve uygulama güvenliği sağlanması
- Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılması
- Anahtar yönetimi uygulanması
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınması
- Bulutta depolanan kişisel verilerin güvenliğinin sağlanması
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemesi
- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılması
- Çalışanlar için yetki matrisi oluşturulması
- Erişim loglarının düzenli olarak tutulması
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanması
- Gerekğinde veri maskeleyme önlemi uygulanması
- Gizlilik taahhütnameleri yapılması
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılması
- Güncel anti-virüs sistemleri kullanılması
- Güvenlik duvarları kullanılması
- İmzalanan sözleşmelerin veri güvenliği hükümleri içermesi
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirlerinin alınması ve ilgili evrak gizlilik dereceli belge formatında gönderilmesi
- Kişisel veri güvenliği politikaları ve prosedürleri belirlenmesi
- Kişisel veri güvenliği sorunlarının hızlı bir şekilde raporlanması
- Kişisel veri güvenliğinin takibi yapılması

- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınması
- Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanması
- Kişisel veri içeren ortamların güvenliği sağlanması
- Kişisel verilerin mümkün olduğunca azaltılması
- Kişisel verilerin yedeklenmesi ve yedeklenen kişisel verilerin güvenliğinin de sağlanması
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanması ve bunların takibinin de yapılması
- Kurum içi periyodik ve/veya rastgele denetimler yapılması ve yaptırılması
- Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulması
- Mevcut risk ve tehditlerin belirlenmesi
- Özel nitelikli kişisel veri güvenliğine yönelik protokollerin ve prosedürlerin belirlenmesi ve uygulanması
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmesi
- Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarların kullanılması ve farklı birimlerce yönetilmesi
- Saldırı tespit ve önleme sistemlerinin kullanılması
- Sızma testinin uygulanması
- Siber güvenlik önlemlerinin alınması ve uygulanmasının sürekli takip edilmesi
- Şifreleme yapılması
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler verilerinin şifrelenerek aktarılması
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanması
- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanması
- Veri kaybı önleme yazılımları kullanılması