

YÖNETMELİK

Sağlık Bakanlıđından:

KİŞİSEL SAĞLIK VERİLERİ HAKKINDA YÖNETMELİK
BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Yönetmeliğın amacı; 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri kapsamında, Sağlık Bakanlıđının merkez ve taşra teşkilatı birimleri ile bunlara bağılı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağılı ve ilgili kuruluşları tarafından yürütölen süreç ve uygulamalarda uyulacak usul ve esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Bu Yönetmelik, kişisel sağlık verisi işleyen özel hukuk gerçek ve tüzel kişileri ile kamu hukuku tüzel kişilerinin, Sağlık Bakanlıđı tarafından yürütölmekte olan süreç ve uygulamalara ilişkin faaliyetlerini kapsar.

Dayanak

MADDE 3 – (1) Bu Yönetmelik, 7/5/1987 tarihli ve 3359 sayılı Sağlık Hizmetleri Temel Kanunu ile 10/7/2018 tarihli ve 1 sayılı Cumhurbaşkanlıđı Teşkilatı Hakkında Cumhurbaşkanlıđı Kararnamesinin 378 inci maddesinin altıncı fıkrası ve 508 inci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu Yönetmelikte geçen;

- Açık veri: Ücretsiz olarak veya hazırlanma maliyetini geçmeyecek şekilde internet üzerinden herkesin erişimine sunulan, üzerinde herhangi bir fikri mülkiyet hakkı bulunmayan ve herhangi bir amaçla serbestçe kullanılabilen, makineler tarafından okunabilen ve böylelikle diğer veriler ve sistemlerle birlikte çalışabilen, anonim hale getirilmiş veriyi,
- Açık sağlık verisi: Açık veri haline getirilen sağlık verisini,
- Anonim hale getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliğı belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- Bakanlık: Sağlık Bakanlıđım,
- e-Nabız: İlgili kişilerin sağlık verilerine kendilerinin, hekimlerin veya yetki verdikleri üçüncü kişilerin erişimini sağlayan, e-Devlet uygulamalarına uygun olarak Bakanlıkça kurulan sistemi,
- Genel Müdürlük: Sağlık Bilgi Sistemleri Genel Müdürlüğüüü,
- İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
- 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 kişileri,
- KamuNET: Kamu kurum ve kuruluşları arasındaki veri iletişiminin sağlanması, bu veri iletişiminin internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılması, siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlarıyla Ulaştırma ve Altyapı Bakanlıđı tarafından geliştirilen projeyi,
- Kanun: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununu,
- Kimliksizleştirme: Kişisel verilerin; kimliğı belirli veya belirlenebilir gerçek kişiyle ilişkilendirilememesi için teknik ve idari tedbirlerin alınması şartıyla ve farklı bir ortamda muhafaza edilen diğer verilerle bir araya getirilmeksizin ilgili kişiyle ilişkilendirilemeyecek şekilde işlenmesini,
- Kişisel veri: Kimliğı belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
- Kişisel sağlık verisi: Kimliğı belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,
- Kişisel verilerin imha edilmesi: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,
- Kişisel verilerin işlenmesi: 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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlemi,
- Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi işlemini,
- Kişisel verilerin yok edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hâle getirilmesi işlemini,
- Kurul: Kişisel Verileri Koruma Kurulunu,
- Kurum: Kişisel Verileri Koruma Kurumunu,
- Maskeleme: Kişisel verilerin belirli alanlarının, kimliğı belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,
- Merkezi sağlık veri sistemi: Bakanlık tarafından oluşturulan kişisel sağlık verilerinin toplandığı veri sistemini,
- Sağlık hizmeti sunucusu: Sağlık hizmetini sunan veya üreten gerçek kişiler ile kamu hukuku ve özel hukuk tüzel kişilerini,
- Veri sorumlusu: Kişisel sağlık verilerinin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.
- Bu Yönetmelikte yer almayan tanımlar için Kanundaki tanımlar ile Kurum tarafından yapılan ikincil düzenlemelerde yer verilen tanımlar geçerlidir.

İKİNCİ BÖLÜM
Genel İlke ve Esaslar

Genel ilke ve esaslar

MADDE 5 – (1) Kişisel verilerin işlenmesinde Kanunun 4 üncü maddesinde yer alan genel ilkeler başta olmak üzere, Kanunda yer alan bütün esaslara riayet edilir.

(2) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütölmesi maksadıyla, Bakanlık ile bağılı ve ilgili kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla Bakanlık tarafından, bağılı ve ilgili kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemleri kurulabilir.

(3) Hiç kimse, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dokümanı sunmaya veya göstermeye zorlanamaz.

(4) Sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirler alınır.

(5) Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmi kimliksizleştirme veya maskeleme tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır.

(6) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili olarak Kanunun 11 inci maddesinde yer alan hakları kullanabilir.

(7) Veri sorumlusuna başvuruda, Kanunun 13 üncü maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete’de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümlerine riayet edilir.

(8) Aydınlatma yükümlölüğünün yerine getirilmesinde, Kanunun 10 uncu maddesi ile Kurum tarafından hazırlanarak 10/3/2018 tarihli ve 30356 sayılı Resmî Gazete’de yayımlanan Aydınlatma Yükümlölüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine riayet edilir.

ÜÇÜNCÜ BÖLÜM
Kişisel Sağlık Verilerine Erişim

Sağlık personelinin verilere erişimi

MADDE 6 – (1) Sağlık hizmeti sunumunda görevli kişiler; ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereğı ile sınırlı olmak kaydıyla erişebilir.

(2) e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanır. İlgili kişiler, gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilir. Gizlilik tercihi ve geçmiş sağlık verilerinin görütölenememesi nedeniyle sağlık hizmeti sunumunda meydana gelebilecek aksaklık ve zararlardan Bakanlık sorumlu olmaz.

(3) e-Nabız hesabı bulunmayan kişilerin sağlık verilerine ise Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan istisnai amaçlarla sınırlı olmak üzere ancak;

- Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırlı olmaksızın,
- Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağılantılı işlemler sonlanana kadar,
- Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla,
- Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar, erişilebilir.

(4) Üçüncü fıkraa yer alan erişim kuralları, Bakanlıđın sağlık hizmeti sunumu ihtiyaçlarına göre ve Kanunun 6 ncı maddesinin üçüncü fıkrası kapsamında Genel Müdürlük tarafından yeniden değeriendirilebilir. Böyle bir durumda aydınlatma yükümlölüğü kapsamında gereklilikler sağlanır.

(5) Geçmiş sağlık verilerinin herhangi bir kimse tarafından erişilmesini istemeyen kişilere ilgili gizlilik tercihi e-Nabız üzerinden sunulur. Bu gizlilik tercihini kullanan kişilerin geçmiş sağlık verilerine ancak kişinin kendisi tarafından beyan edilen telefon numarasına gönderilecek olan kodun hekim ile paylaşılmısı ve hekim tarafından sisteme giriilmesi halinde erişilebilir.

(6) Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görölmesi ve bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verileri Bakanlıkça belirlenir ve sağlık personelinin bu verilere erişimine ölçülü kısıtlar getirilebilir.

Bakanlık birimlerinin verilere erişimi

MADDE 7 – (1) Sağlık hizmeti sunucuları tarafından merkezi sağlık veri sistemine kimliksizleştirilerek gönderilen sağlık verilerini, ilişkisel veri tabanı aracılığı ile ait oldukları kişilerle eşleştirmeye yetkili kişileri Bakanlıđın birim amirleri ayrı ayrı belirler ve Genel Müdürlükten bu kişilerin yetkilendirilmesini talep eder. Her birimin amiri, kendi biriminden en fazla üç kişinin yetkilendirilmesini talep edebilir.

(2) Birim amirinin talebi üzerine Genel Müdürlükçe yetkilendirilen kullanıcılar bu yetkiyi, yalnızca sağlık hizmetleri ile finansmanın planlanması ve yönetimi ile denetleme ve düzenleme görevleri kapsamında, kişisel veri koruma mevzuatı ilkelerine uygun olarak kullanabilirler.

(3) Sağlık hizmetleri ile finansmanın planlanması ve yönetimi amacının sınırları, yasal ve idari düzenlemelerde ilgili birime verilen görevler üzerinden belirlenir.

Çocukların sağlık verilerine erişim

MADDE 8 – (1) Ebeveynler, çocuklarına ilişkin sağlık kayıtlarına herhangi bir onaya ihtiyaç duymaksızın e-Nabız üzerinden erişebilir. Ayırt etme gücüne sahip çocuklar, sağlık geçmişlerine ebeveynlerinin erişimini e-Nabız üzerinden izne tabi tutabilir.

(2) Anne ve babanın boşanması hâlinde velâyet hakkı üzerinde bırakılmayan taraf, çocuk ile velinin faydası gözetilmek suretiyle kişisel verilerin korunması mevzuatına uygun şekilde ve Genel Müdürlükçe belirlenen sınırlar çerçevesinde çocuğa ilişkin sağlık verilerine erişebilir.

Sağlık verilerine hasta yakınlarının erişimi

MADDE 9 – (1) Kişisel sağlık verilerinin hasta yakınları ile paylaşımında, Kanun ilkelerine aykırılık teşkil etmeyecek şekilde, 1/8/1998 tarihli ve 23420 sayılı Resmî Gazete’de yayımlanan Hasta Hakları Yönetmeliğinin 18 inci maddesinin üçüncü fıkrasına uygun hareket edilir.

Sağlık verilerine avukatların erişimi

MADDE 10 – (1) Avukatlar, müvekkilinin sağlık verilerini genel vekâletname ile talep edemezler. Müvekkiline ait sağlık verilerinin avukata aktarılması için düzenlenmiş olan vekâletnamede, ilgili kişinin özel nitelikli kişisel verilerinin işlenmesi ve aktarılmasına ilişkin açık rızasını gösteren özel bir hüküm bulunması gerekir.

Ölünün sağlık verilerine erişim

MADDE 11 – (1) Ölmüş bir kişinin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir.

(2) Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır.

DÖRDÜNCÜ BÖLÜM

Kişisel Sağlık Verilerinin Gizlenmesi, Düzeltilmesi, İmha Edilmesi ve Aktarılması

Kişisel sağlık verilerinin gizlenmesi

MADDE 12 – (1) Hakkında gizlilik kararı verilen kişilere ait verilerin gizlenmesi için yargı makamları tarafından gönderilen müzekkerenin gereğı il sağlık müdürlüğü tarafından yerine getirilir. İl sağlık müdürlüğü tarafından tesis edilen işlem doğrudan Kimlik Paylaşım Sistemine de yansır. Gizlilik kararlarının sadece görevi gereğı bilmesi gereken kişiler tarafından bilinmesini sağlamak üzere gerekli her türlü teknik ve idari tedbirler alınır.

Kişisel sağlık verilerinin düzeltilmesi

MADDE 13 – (1) İlgili kişi, kendisi hakkında sehven oluşturulan sağlık verilerinin düzeltilmesi hususunda sağlık verisinin oluşturulduğu sağlık hizmeti sunucusunun bağılı bulunduğu il sağlık müdürlüğüne başvurur. İl sağlık müdürlüğü, ilgili sağlık hizmeti sunucusunda yapacağı araştırma neticesinde sağlık verisinin sehven oluşturulduğu bilgisine ulaşırsa resmî yazı ile Genel Müdürlüğe başvurur ve sehven oluşturulan sağlık verisinin düzeltilmesini ister.

(2) Genel Müdürlük tarafından tesis edilecek işlem, sağlık hizmeti sunucusunun kendi veri tabanında da gerçekleştirilir.

(3) Genel Müdürlük, sağlık hizmeti sunucuları tarafından oluşturulan sağlık verilerinin kendileri tarafından düzeltilileceğı tarihi belirler ve bu tarihi ihtiyaca göre günceller. Genel Müdürlükçe belirlenen bu tarihten sonra oluşturulan sağlık verileri ilgili sağlık hizmeti sunucusu tarafından; bu tarihten önce oluşturulan sağlık verileri ise ilgili il sağlık müdürlüğünün talebi üzerine Genel Müdürlükçe düzeltilir.

Kişisel sağlık verilerinin imha edilmesi

MADDE 14 – (1) Kişisel verilerin imha edilmesinde, Kanunun 7 nci maddesi ile Kurum tarafından hazırlanarak 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine riayet edilir.

Kişisel sağlık verilerinin aktarılması

MADDE 15 – (1) Kişisel sağlık verilerinin yurtiçinde aktarımında Kanunun 8 inci maddesine, yurtdışına aktarımında ise Kanunun 9 uncu maddesine riayet edilir.

(2) Kişisel sağlık verilerinin, Kanunun 8 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası ve 28 inci maddesi kapsamında kamu kurum ve kuruluşlarına aktarılması için protokol düzenlenir. Düzenlenen protokole, kişisel veri koruma mevzuatının genel ilkeleri ile veri güvenliğine ilişkin hükümlere ve protokol kapsamında hangi verilerin aktarılaacağına yer verilir. Verilerin aktarımı, teknik altyapının uygun olması hâlinde KamuNET üzerinden gerçekleştirilir.

(3) Kişisel sağlık verilerinin aktarımı talepleri, talep edilen sağlık verilerinin ilgili olduğu Bakanlık birimi tarafından Kanun ve ilgili diğer mevzuat açısından değeriendirilir, değeriendirme sonucuna göre Genel Müdürlükçe işlem tesis edilir.

BEŞİNCİ BÖLÜM

Bilimsel Amaçlarla İşleme ve Açık Sağlık Verisi

Bilimsel amaçlarla işleme

MADDE 16 – (1) Kanunun 28 inci maddesinin birinci fıkrasının (b) bendi kapsamında veri sorumlusu tarafından anonim hâle getirilen kişisel sağlık verileri ile bilimsel çalışma yapılabilir.

(2) Kanunun 28 inci maddesinin birinci fıkrasının (c) bendi kapsamında kişisel sağlık verileri, ilgili kişilerin özel hayatın gizliliğini veya kişilik haklarını ihlâl etmemek ya da suç teşkil etmemek kaydıyla alınacak teknik ve idari tedbirler çerçevesinde, bilimsel amaçlarla işlenebilir.

Açık sağlık verisi

MADDE 17 – (1) Genel Müdürlük tarafından, Bakanlıđın merkez ve taşra teşkilatı ile bağılı ve ilgili kuruluşlarında kullanılan sistemlerde yer alan verilerin, veri mahremiyeti ile veri güvenliğine ilişkin düzenlemeler göz önünde bulundurularak, sağlık sisteminde jeffaflığı ve hesap verilebilirliğı temin etmek, sağlık hizmeti sunumuna ilişkin politika ve stratejilere yön vermek, sağlık alanında yapılacak bilimsel araştırmalara destek olmak ve sağlığa ilişkin irtin ve hizmetlerin geliştirilmesini sağlamak amaçlarıyla, bu konuya özel olarak tahsis edilen bir internet sitesi üzerinden herkesin erişimine açılmasına ilişkin usül ve esaslar Bakanlıkça belirlenir.

ALTINCI BÖLÜM

Veri Güvenliğı

Veri güvenliğine ilişkin yükümlölükler

MADDE 18 – (1) Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlölüklere riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliğı Rehberi esas alınır.

(2) İşlenen kişisel verilerin kanunî olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu tarafından Kurula yapılacak bildirimde Kanun hükümleri ile Kurulun bu hususa ilişkin düzenleyici işlemleri esas alınır.

Bilgi güvenliğı

MADDE 19 – (1) Bakanlık merkez birimleri ve taşra teşkilatı ile bağılı ve ilgili kuruluşlarda yürütölen bilgi güvenliğı süreçleri, Genel Müdürlük tarafından hazırlanan Bilgi Güvenliğı Politikaları Yönergesi ile belirlenir.

Yeterli önlemler

MADDE 20 – (1) Özel nitelikli kişisel verilerin işlenmesinde ayrıca, Kanunun 6 ncı maddesinin dördüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (ç) bendi uyarınca Kişisel Verileri Koruma Kurulu tarafından yapılan ikincil düzenlemelerde yer alan yeterli önlemlere riayet edilir.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Yapırım

MADDE 21 – (1) Bu Yönetmelikle korunan kişisel verilere ilişkin suçlar ve kabahatler bakımından Kanunun 17 nci ve 18 inci maddelerine göre işlem yapılır.

(2) Bu Yönetmelik gereklerini yerine getirmeyen kamu görevlileri için bağılı oldukları disiplin amirliğine bildirim yapılır ve varsa yetkileri iptal edilir. Gerçek kişiler ve özel hukuk tüzel kişileri hakkında ilgili mevzuata göre işlem yapılır.

(3) Merkezi sağlık veri sisteminde Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde veri gönderimi yapmayan sağlık hizmeti sunucularına, 3359 sayılı Sağlık Hizmetleri Temel Kanununun Ek 11 inci maddesinin üçüncü fıkrasına göre işlem tesis edilir.

Hüküm bulunmayan hâller

MADDE 22 – (1) Kişisel sağlık verilerinin işlenmesi ile ilgili olarak Bu Yönetmelikte hüküm bulunmayan hâllerde; Kanun ve ilgili ikincil düzenlemeler uygulanır.

Yürürlükten kaldırılan yönetmelik

MADDE 23 – (1) 20/10/2016 tarihli ve 29863 sayılı Resmî Gazete’de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik yürürlükten kaldırılmıştır.

Yürürlük

MADDE 24 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütlme

MADDE 25 – (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.