YÖNETMELİK

Sosyal Güvenlik Kurumu Başkanlığından:

SOSYAL GÜVENLİK KURUMU NEZDİNDEKİ VERİLERİN KORUNMASINA VE İŞLENMESİNE İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Yönetmeliğin amacı; Kurumun 16/5/2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanun, 31/5/2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve 15/7/2018 tarihli ve 30479 sayılı Resmî Gazete'de yayımlanan 4 sayılı Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinde belirtilen görev ve yetkileri kapsamında, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde ettiği verilerin işlenmesinde uyulacak usul ve esasları belirlemektir.

Kapsam

MADDE 2 – (1) Bu Yönetmelik, Kurumun görev ve yetkileri kapsamında tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde ettiği verilerin işlenmesinde uyulacak usul ve esaslar doğrultusunda;

a) Kurum personelini,

b) Kişisel verileri işlenen gerçek kişileri,

c) Kişisel verilerin işlenmesine ait bilgi işlem sistemleri yazılım ve donanımı ile dosyalama sistemi gibi hizmetleri sunan gerçek ve tüzel kişileri,

ç) Kurumun faaliyetleri kapsamında mevzuat çerçevesinde kişisel verileri işleyen kamu kurum ve kuruluşları ile özel hukuk gerçek ve tüzel kişileri,

d) Kurum adına kişisel verileri işleyen gerçek veya tüzel kişileri,

e) Veri aktarımının yapıldığı kamu kurum ve kuruluşları ile özel hukuk gerçek ve tüzel kişilerini,

kapsar.

Dayanak

MADDE 3 – (1) Bu Yönetmelik, 16/5/2006 tarihli ve 5502 sayılı Sosyal Güvenlik Kurumuna İlişkin Bazı Düzenlemeler Hakkında Kanunun 35 inci maddesi ile 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu Yönetmelikte geçen;

a) AFYDB: Kurum Aktüerya ve Fon Yönetimi Daire Başkanlığını,

b) Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

c) Anonim veri: Anonim hale getirilen ve kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilemeyen veriyi,

ç) Başkan: Sosyal Güvenlik Kurumu Başkanını,

d) Birim: 4 sayılı Cumhurbaşkanlığı Kararnamesinin 413 üncü maddesinde belirtilen hizmet birimlerini,

e) Birim amiri: 4 sayılı Cumhurbaşkanlığı Kararnamesinin 413 üncü maddesinde belirtilen hizmet birimlerinin en üst amirini, taşra teşkilatında ise sosyal güvenlik il müdürlerini,

f) Genel sağlık sigortalısı: 5510 sayılı Kanunun 60 ıncı maddesinde sayılan kişileri,

g) Genel sağlık sigortası: Kişilerin öncelikle sağlıklarının korunmasını, sağlık riskleri ile karşılaşmaları halinde ise oluşan harcamaların finansmanını sağlayan sigortayı,

ğ) HSGM: Kurum Hizmet Sunumu Genel Müdürlüğünü,

h) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

ı) 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,

i) Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,

j) Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

k) 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

l) Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini,

m) Kişisel verilerin yok edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

n) Kurul: Kişisel Verileri Koruma Kurulunu,

o) Kurum: Sosyal Güvenlik Kurumunu,

ö) MEDULA: Sağlık hizmeti kullanım verisi toplamak ve bu verilere dayanarak faturalama işlemini gerçekleştirmek amacıyla Kurum tarafından uygulanan ve işletilen elektronik bilgi sistemini,

p) Mevzuat birimi: Emeklilik Hizmetleri Genel Müdürlüğü, Sigorta Primleri Genel Müdürlüğü, Genel Sağlık Sigortası Genel Müdürlüğü, Rehberlik ve Teftiş Başkanlığı, Aktüerya ve Fon Yönetimi Daire Başkanlığı ile Strateji Geliştirme Başkanlığını,

r) Sağlık hizmeti: Genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilere 5510 sayılı Kanunun 63 üncü maddesi gereği finansmanı sağlanacak tıbbi ürün ve hizmetleri,

s) Sağlık hizmeti sunucusu: Sağlık hizmetini sunan ve/veya üreten; gerçek kişiler, kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerini ve bunların tüzel kişiliği olmayan şubelerini,

ş) Sigortalı: Kısa ve/veya uzun vadeli sigorta kolları bakımından adına prim ödenmesi gereken veya kendi adına prim ödemesi gereken kişiyi,

t) Sosyal sigortalar: 5510 sayılı Kanunda tanımlanan kısa ve uzun vadeli sigorta kollarını,

u) Taşra birimi: Sosyal güvenlik il müdürlükleri ile sosyal güvenlik il müdürlüklerine bağlı sosyal güvenlik merkezlerini,

ü) Ticari sır niteliğindeki veri: Bir ticari işletme veya şirketin kendisine veya muvafakati çerçevesinde gerçek veya tüzel kişilere verilme durumları hariç olmak üzere; herkes tarafından bilinmeyen ve elde edilemeyen, başta rakipleri olmak üzere üçüncü kişilere ve kamuya açıklanması halinde ilgili ticari işletme veya şirketin zarar görme ihtimali bulunan ve ticari işletme veya şirketin ekonomik hayattaki başarı ve verimliliği için ticari önem atfettikleri veriyi,

v) Veri: Kurum nezdinde üretilen, işlenen veya arşivlenen her türlü bilgi ve belgeyi,

y) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

z) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği Kurum veri kayıt sistemlerini,

aa) Veri paylaşım metodu: Talep edilen verilerin Kurum tarafından uygun bulunan Elektronik Belge Yönetimi Sistemi (EBYS) ortamında CD, DVD, sabit disk, taşınabilir bellek gibi elektronik-manyetik kayıt ortamlarında veya web servis, SFTP veya Kurumda kullanılan diğer yazılımlar gibi elektronik ortamlar üzerinden şifrelenerek paylaşım metotlarını,

bb) Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

ifade eder.

İKİNCİ BÖLÜM

Kişisel Veriler, Kişisel Sağlık Verileri ile Ticari Sır Niteliğindeki Veriler

Kişisel veriler, kişisel sağlık verileri ile ticari sır niteliğindeki verilerin işlenmesi

MADDE 5 – (1) Kurum; 5502 sayılı Kanun, 5510 sayılı Kanun ve 4 sayılı Cumhurbaşkanlığı Kararnamesi ile kendisine verilen görevleri yerine getirmek amacıyla kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin işlenmesinde aşağıdaki ilkelere uymak zorundadır:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

(2) Kurumla sözleşmeli sağlık hizmeti sunucuları, Kurum adına işledikleri kişisel sağlık verilerini Kurum veri kayıt sistemine aktarmakla yükümlüdür.

(3) Sağlık hizmeti sunucuları, sözleşme kapsamında Kurum adına işledikleri kişisel sağlık verilerini, Kurum veri kayıt sistemi dışında hiçbir yere kopyalayamaz veya aktaramaz.

(4) Kurum adına kişisel verileri, kişisel sağlık verilerini ve ticari sır niteliğindeki verileri işleyen veya görevi gereği bu verilere erişen herkes, sır saklama yükümlülüğü altında olup veri gizliliğinin sağlanması amacıyla Kurum ve Kurul tarafından belirlenen önlemlere uymakla yükümlüdür.

(5) Kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin işlenmesinde ayrıca Kurul tarafından yapılan düzenlemelere uyulması zorunludur. Ancak veri aktarımında 5502 sayılı Kanunun 35 inci maddesi hükmü saklıdır.

(6) Kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin bulunduğu Kurum veri kayıt sistemine erişim izni verilebilmesi için, yetkilendirme dahilinde kullanıcı tanımlanması gerekir. Kullanıcı tanımlama ve yetkilendirmeye ilişkin her türlü işlem kayıt altına alınır ve bu kayıtlar muhafaza edilir. Yetkilendirme, kayıt altına alma ve verilerin muhafazasına ilişkin hususlar veri sorumlusu tarafından belirlenir.

Veri sorumlusunun görev ve yükümlülükleri

MADDE 6 – (1) Veri sorumlusu, bu Yönetmelik kapsamındaki verilerin hukuka aykırı olarak işlenmesini ve bu verilere, hukuka aykırı bir şekilde erişilmesini önlemek, bu verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, tedbirlerin alınması hususunda veri işleyenler ile birlikte müştereken sorumludur.

(3) Veri sorumlusu Kurul tarafından belirlenen düzenlemelerin uygulanmasını sağlamak amacıyla Kurumda gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Kişisel verileri, kişisel sağlık verileri ile ticari sır niteliğindeki verileri işleyen kişiler, bu verilere erişen kişiler ve veri sorumluları; öğrendikleri kişisel verileri, kişisel sağlık verilerini ve ticari sır niteliğindeki verileri 6698 sayılı Kanun ve 5502 sayılı Kanun ile bu Yönetmelik hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) Bu Yönetmelik kapsamında işlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin tespiti hâlinde veri sorumlusu, bu durumu gecikmeksizin ve en geç 72 saat içinde Kurula, söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde bildirir.

(6) Bu Yönetmelik kapsamında kişisel veri işleyen veri sorumluları Kurul tarafından çıkarılacak düzenlemelere uymakla yükümlüdür.

Kişisel veriler, kişisel sağlık verileri ile ticari sır niteliğindeki verilere erişimler

MADDE 7 – (1) Kuruma verilen görevlerin yerine getirilebilmesi için kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personelinin kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere erişimleri; üçüncü kişilere verilmemek, açıklanmamak ve veri güvenliğine ilişkin Kurum ve Kurul tarafından belirlenen yükümlülüklere uyulmak kaydıyla veri aktarımı olarak değerlendirilmez.

(2) Bu Yönetmelik kapsamındaki kişisel verilere;

a) Sağlık hizmetlerine ilişkin fatura bedellerinin incelenmesi ve ödenmesi,

b) Kurumun alacaklarının takip ve tahsili,

c) Denetim, teftiş ve kontrol,

ç) Verilerin işlenmesi,

d) Kurum mevzuatında yer alan sağlık ve sosyal sigorta hizmetlerine ilişkin kontrol parametrelerinin Kurum veri kayıt sistemine aktarılması ve takibi,

e) Sağlık ve sosyal sigorta hizmetlerinin izlenmesi, değerlendirilmesi, istatistik üretilmesi ve risk analizi yapılması,

f) Sağlık ve sosyal sigorta politikalarının belirlenmesi,

g) HSGM'de yazılım geliştirilmesi, sistem işletimi ve verilerin hazırlanması,

amacıyla bu işlemlerde görevlendirilen ve 5 inci maddenin altıncı fıkrası kapsamında kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personeli tarafından erişilebilir.

(3) Kullanıcı tanımlaması ve yetkilendirmesi yapılan Kurum personeli, kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere;

a) Kurum veri kayıt sisteminde yer alan verilere şifre ile doğrudan erişim yetkisi verilmesi,

b) Kurumsal Raporlama ve İstatistik Sistemi, MEDULA gibi kişisel veriler, ticari sır niteliğindeki veriler ile kişisel sağlık verilerine ulaşılan uygulamalara şifre ile erişim yetkisinin verilmesi,

yoluyla erişebilir.

(4) Kullanıcı tanımlaması ve yetkilendirmesi yapılmaksızın Kurum personelinin görevi kapsamında talep ettiği kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere;

a) İlgili mevzuat biriminin onayı sonrasında HSGM tarafından uygun veri paylaşım metodu ile personelin bağlı olduğu ilgili birime iletilmesi,

b) Kurum personelinin görevi kapsamında talep ettiği kişisel veriler, kişisel sağlık verileri ve ticari sır niteliğindeki verilere birimi içerisinde hazırlanması ve iletilmesi,

yöntemiyle erişebilir.

(5) İkinci fıkranın (c) bendi kapsamında yapılan veri talepleri doğrudan HSGM'ye yapılır ve HSGM tarafından karşılanır. Üçüncü fıkranın (a) bendi kapsamında verilere erişim yetkileri, personelin görev yaptığı birim tarafından Başkanlık Makamından alınan onaya istinaden HSGM tarafından verilir. Üçüncü fıkranın (b) bendi kapsamında verilere erişim yetkileri, personelin görev yaptığı birimin talebine istinaden Kurumun yetkilendirme işlemleri çerçevesinde

HSGM tarafından verilir. Dördüncü fıkranın (a) bendi kapsamında yapılacak veri talepleri ilgili birim tarafından doğrudan mevzuat birimine yapılır ve bu talepler hakkında 20 nci maddenin bir ila yedinci fıkrası hükümleri uygulanır.

(6) Verilere erişim yetkileri, personelin görev süresi ve kapsamı ile sınırlı olup, erişim yetkisinin sona ermesini gerektirecek bir durumun meydana gelmesi halinde yetkinin kaldırılması ile ilgili gerekli işlemler personelin görev yaptığı birim tarafından derhal yapılır.

(7) Personelin verilere erişim yetki düzeyleri, personelin görev süresi ve kapsamı ile yapılacak çalışmanın niteliğinin gerektirdiği erişim ihtiyacı dikkate alınarak talebi yapan ilgili birimce belirlenir ve bu talep ilgili mevzuat biriminden alınacak onay ile HSGM'ye iletilir.

Kurumun iş ve işlemlerinin yürütülmesine ilişkin hususlar

MADDE 8 – (1) Veri işleyenler tarafından hizmetin gereği olarak veri kayıt sistemlerinden yapılan sorgular, veri aktarımı olarak değerlendirilmez.

Genel sağlık sigortası ile sosyal sigortalara yönelik iş ve işlemlerin paydaşlar ile yürütülmesi

MADDE 9 – (1) Kuruma verilen görevlerin yerine getirilebilmesine yönelik iş ve işlemlerin diğer kamu kurum ve kuruluşları ile üniversite, enstitü, oda, dernek gibi paydaşlar ile birlikte gerçekleştirilmesi amacıyla;

a) Kurumca imzalanan işbirliği protokolü, hizmet alım sözleşmesi/protokolü kapsamındaki çalışmalarda,

b) Genel sağlık sigortası ile sosyal sigortalar uygulamalarına ilişkin iş ve işlemlerin yürütülmesine yönelik olarak oluşturulan komisyonlarda,

Kurum dışından görev alan kişilerin kişisel verilere, kişisel sağlık verilerine ve ticari sır niteliğindeki verilere erişimlerine izin verilmez. Bu kişilerin anonim verilere erişimleri, veri aktarımı olarak değerlendirilmez.

(2) Kurum, bu madde kapsamında görevlendirilen kişiler ile ilgili olarak, bu Yönetmelik ve 6698 sayılı Kanunun 12 nci maddesi kapsamında veri güvenliğine ilişkin teknik ve idari tedbirleri almak, ilgili mevzuat hükümlerine uygun hareket edilmesini sağlamak zorundadır.

Kişinin kendisine ait kişisel veriler ile kişisel sağlık verilerine ilişkin talepleri

MADDE 10 – (1) Herkes, Kuruma başvurarak kendisiyle ilgili kişisel verileri ile kişisel sağlık verilerinin;

a) İşlenip işlenmediğini öğrenme,

b) İşlenmişse buna ilişkin bilgi talep etme,

c) Silinmesini, yok edilmesini isteme,

ç) İşlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

d) Yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri bilme,

e) Eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

f) İşlenenlerinin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

g) Mevzuata aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,

ğ) (c) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

haklarına sahiptir.

(2) Kişilerin kişisel verileri ile kişisel sağlık verilerinin silinmesi veya yok edilmesi taleplerinde, kişisel verilerin işlenme şartlarının tamamının ortadan kalkıp kalkmadığı yönünde ilgili mevzuat birimince değerlendirme yapılarak silme, yok etme veya anonim hâle getirme işlemlerinden hangisinin uygulanacağına karar verilir. Uygulanan yöntem ve gerekçesi en geç 30 gün içinde ilgili mevzuat birimi tarafından ilgili kişiye yazılı olarak veya elektronik tebligat adresine bildirilir.

(3) Kurum, kişinin kişisel verileri ile kişisel sağlık verilerini;

a) Kişinin kendisine veya noter onaylı muvafakatiyle veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izin ile diğer gerçek veya tüzel kişilere,

b) Mahkeme kararı ile kişinin sağlık verilerine erişim izninde yetkilendirilmiş kişilere,

c) Müvekkili tarafından verilen özel vekâletnamede avukatın kişisel veriler ile kişisel sağlık verilerini talep edebileceğine yer verilmiş olması şartıyla ilgili avukatına,

aktarabilir veya gerekçesini açıklayarak veri taleplerini reddedebilir.

(4) Kuruma yapılan talepler, talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırılır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi halinde, Kurulca bu konuda belirlenen tarifedeki ücret alınabilir.

(5) Bu madde kapsamındaki veri talepleri taşra birimine yapılır. Taşra birimi, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemediği verileri 20 nci maddenin iki ila beşinci fıkrası hükümlerine göre temin edebilir.

Kurum veya kuruluşların kişisel veri ile ticari sır niteliğindeki veri talepleri

MADDE 11 – (1) Kurum, işlediği kişisel veri ile ticari sır niteliğinde olan verileri, ilgili kişinin noter onaylı muvafakati veya e-Devlet uygulaması üzerinden kimlik teyidi ile verilen izni ile ve kişiler adına vekâlet ile yetkilendirilenler tarafından, kişisel veri veya ticari sır niteliğindeki veriler hususunda yetkiyi içeren özel vekâletnamenin veya vasi atamaya ilişkin mahkeme kararının Kuruma ibraz edilmesi koşuluyla gerçek veya tüzel kişilere, ilgili mevzuat birim amirinin onayı ile aktarılabilir.

(2) Ancak, 5502 sayılı Kanunun 35 inci maddesi uyarınca 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun ekinde yer alan (I), (II), (III) ve (IV) sayılı cetvellerde yer alan kamu idareleri ile Türkiye Cumhuriyet Merkez Bankasının ilgili mevzuatında belirtilen görevleri yapabilmeleri için ihtiyaç duydukları kişisel sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğinde olan veriler aktarılabilir.

(3) Kamu kurum veya kuruluşları tarafından yazılı veya elektronik ortamda talep edilen tek seferlik kişisel veriler ile ticari sır niteliğindeki veriler, ikinci fıkradaki şartları taşıdığının belirlenmesi halinde talep eden kamu kurum veya kuruluşlarının bulunduğu il müdürlüğünce karşılanır. İl müdürlüğü, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemedikleri verileri, 20 nci maddenin bir ila dokuzuncu fıkrası hükümlerine göre temin ederek ilgili merciye teslim eder.

(4) Kamu kurum veya kuruluşları tarafından talep edilen sürekli nitelikteki kişisel veriler ile ticari sır niteliğindeki verilerin aktarılabilmesi için veri talebinde bulunanlar ile Kurum arasında ilgili mevzuat biriminin koordinasyonunda aktarımın usulünü ve diğer gerekli hususları belirleyen protokolün imzalanması zorunludur.

Sağlık Bakanlığının kişisel sağlık verisi talepleri

MADDE 12 – (1) Kurum, kişisel sağlık verilerini; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, verilen sağlık hizmetlerinin uygunluğunun ve yerindeliğinin takibi ve finansmanının planlanması amacıyla talebi hâlinde Sağlık Bakanlığı ile paylaşır.

(2) Sağlık Bakanlığı tarafından yapılan veri taleplerinde, 20 nci maddenin bir ila dokuzuncu fıkrası hükümleri uygulanır.

Sözleşmeli sağlık hizmeti sunucularının sundukları hizmetlere ilişkin veri talepleri

MADDE 13 – (1) Sağlık hizmetlerinin sağlanmasına yönelik olarak Kurumla sözleşme yapmış sağlık hizmeti sunucularınca, Kurum adına işledikleri kişisel sağlık verilerinden mücbir sebep dolayısıyla Kuruma faturalandırılamayan hizmetlere ilişkin verilerin talep edilmesi durumunda bu talepler hakkında 20 nci maddenin bir ila dokuzuncu fıkrası hükümleri uygulanır.

Yargı makamları ve infaz mercilerinin veri talepleri

MADDE 14 – (1) Yargı makamları ve infaz mercileri tarafından talep edilen kişisel veri ile kişisel sağlık verisi talepleri taşra birimine yapılır. Taşra birimi, yetkileri dahilinde Kurum veri kayıt sisteminden temin edemedikleri verileri, HSGM'den temin ederek ilgili merciye teslim eder.

ÜÇÜNCÜ BÖLÜM
Anonim Veriler

Anonim verilerin aktarılması

MADDE 15 – (1) İlgili mevzuat birimleri tarafından belirlenen kişisel verilerin, kişisel sağlık verilerinin ve ticari sır niteliğindeki verilerin anonim hale getirilmesinde, ulusal ve uluslararası kabul görmüş istatistiki yöntemler uygulanır. Bu konuda Kurul tarafından yapılan düzenlemelerde yer alan hükümler uygulanır.

(2) Anonim veriler, bu Yönetmelik hükümlerine uygun olarak ve Kurum tarafından değerlendirilerek uygun görülmesi koşuluyla;

a) Sağlık ile sosyal sigorta alanında stratejilerin ve hedeflerin gerçekleştirilmesi,

b) Genel sağlık sigortası ile sosyal sigorta politika ve uygulamalarının geliştirilmesi,

c) Sağlık ve sosyal sigorta hizmetlerinin finansmanı, yönetimi ve planlanması,

ç) Kişi ve toplum sağlığının korunması ile koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetleri stratejilerinin oluşturulması,

d) Kurumsal önceliklerin gerçekleştirilmesi,

e) Sağlık ve sosyal sigorta istatistiklerinin hazırlanması,

f) Bilimsel ve akademik araştırma ve çalışmaların gerçekleştirilmesi,

g) Kamu alacaklarının takip ve tahsili,

ğ) Kamu kurum ve kuruluşlarının mevzuatla verilen görevlerinin yerine getirilmesinin sağlanması ile denetim görevlerinin gerçekleştirilebilmesi,

h) Kamu kurum ve kuruluşlarının faaliyetlerinde bürokrasinin azaltılması ve işlemlerin sadeleştirilmesi,

amacıyla aktarılabilir.

(3) Anonim veri talepleri;

a) Verilerin ayrı veya özel bir çalışma, araştırma, inceleme ya da analiz neticesinde oluşturulabilecek nitelikte olup olmadığı,

b) Verilerin anonim hale getirilme işlemlerinin karmaşıklığı,

c) Verilerin ticari sır niteliğinde olup olmadığı,

gibi ölçütlere göre aktarılabilir.

(4) Anonim veri aktarımı yapılan gerçek ve tüzel kişiler aktarılan verileri aktarım amacı ve Kurum bilgisi dışında kullanamazlar.

Araştırma, planlama ve istatistik amaçlı anonim veri talepleri

MADDE 16 – (1) Kamu idarelerinin, 11 inci maddenin ikinci fıkrası kapsamına girmeyen araştırma, planlama ve istatistik amaçlı anonim veri talepleri veya bilimsel araştırma yapan kamu personelinin, bilimsel derneklerin, kamu kurumu niteliğindeki meslek kuruluşlarının veya üniversitelerin araştırma, planlama ve istatistik amaçlı ihtiyaç duydukları anonim veriler aktarılabilir.

(2) İlgili mevzuat birimleri ile AFYDB'de görevli personel hariç, Kurum personelinin görevi kapsamında yapılacak çalışmalarda kullanılmak üzere, anonim veri talepleri, talep eden personelin bağlı bulunduğu birim amiri tarafından ilgisine göre ilgili mevzuat birim amirine yapılır.

(3) Kurum içi birimler tarafından Kurumsal Raporlama ve İstatistik Sisteminde bulunan istatistik amaçlı veriler talep edilemez.

(4) Bu madde kapsamındaki veri taleplerinde, 20 nci madde hükümleri uygulanır.

(5) Bu madde kapsamında sürekli veya elektronik ortamda yapılacak anonim veri aktarımı, ilgili mevzuat biriminin koordinasyonunda aktarımın usulü ve diğer gerekli hususları belirleyen bir protokol aracılığıyla yapılır.

Tüzel kişilere ait olan anonim verilerin tüzel kişinin kendisine veya diğer kişilere aktarımı

MADDE 17 – (1) Tüzel kişilerin, 5510 sayılı Kanunun 63 üncü maddesinin birinci fıkrasının (f) bendinde belirtilen sağlık hizmetlerinden ruhsat veya satış iznine sahip olduğu ürünlere ait veriler; Kurum tarafından uygun görülmesi halinde tüzel kişiyi temsile yetkili olanların noter onaylı muvafakatlerinin alınması kaydıyla 20 nci maddenin bir ila yedinci fıkrası hükümlerine göre gerçek veya tüzel kişilere aktarılabilir.

(2) Bu madde kapsamında aktarılacak veriler, sağlık hizmeti sunucularının doğrudan ya da dolaylı tanınmasına yol açamaz.

(3) Bu madde kapsamında veri aktarılabilmesi için veri talebinde bulunanlar ile Kurum arasında ilgili mevzuat biriminin koordinasyonu ile aktarımın usulü ve diğer gerekli hususları belirleyen sözleşme/protokol imzalanması zorunludur.

Anonim istatistik yayınları

MADDE 18 – (1) Anonim veriler ile ticari sır niteliğindeki verileri içeren Kurum istatistik bültenlerinin, istatistik yıllıklarının ve faaliyet raporlarının yayımlanması veri aktarımı olarak değerlendirilmez.

(2) Kurum tarafından kamuya açıklanmış istatistik bültenleri, istatistik yıllıkları, faaliyet raporları ve benzeri yayımlarında yer alan anonim verilerin Kurum dışına verilmesi veri aktarımı olarak değerlendirilmez.

Kurum personelinin tezleri

MADDE 19 – (1) Kurum personeli, Kurum mevzuatı gereği hazırlayacakları tezleri için anonim veri talebinde bulunabilir.

(2) Bu madde kapsamında yapılacak anonim veri taleplerinde, 20 nci maddenin birinci, üçüncü ve beşinci fıkraları uygulanır.

DÖRDÜNCÜ BÖLÜM
Genel Hükümler

Verilerin aktarım taleplerine ilişkin genel hükümler

MADDE 20 – (1) Veri aktarım talepleri, ilgili mevzuat birimine yazılı olarak yapılır. İlgili mevzuat birimi gerekli gördüğü durumlarda istenilen veriye ilişkin detaylı veri deseninin hazırlanmasını talep edebilir.

(2) 11 inci maddenin ikinci fıkrasında sayılan kamu kurum ve kuruluşlarının talep ettikleri kişisel sağlık verisi dışındaki kişisel veriler, anonim veriler ile ticari sır niteliğindeki verilerin aktarılabilmesi için talebe ilişkin hukuki dayanağın Kuruma yapılacak yazılı talepte belirtilmesi zorunludur.

(3) Veri taleplerinin değerlendirilmesi sürecinde ihtiyaç duyulması halinde ilgili mevzuat birimince ayrıca bilgi ve belge istenebilir.

(4) Veri taleplerinin kabul edilmesi halinde, veri erişimi ve gizliliğine ilişkin gerekli şartları içeren Protokol ilgili mevzuat biriminin koordinasyonunda veri talebinde bulunanlarca imzalanır.

(5) Veri talepleri, ilgili mevzuat birimi tarafından incelenerek veri formatı ve başlıkları belirlenmiş şekilde verilerin hazırlanması için HSGM'ye iletilir. İlgili mevzuat birimi tarafından veri paylaşımının uygun görülmediği durumlarda veri talebinde bulunanlara ilgili mevzuat birimince bilgi verilir.

(6) Aktarılmak üzere hazırlanan veriler, HSGM tarafından Kurumca belirlenecek format ile uygun veri paylaşım metodu kullanılarak paylaşılır. Paylaşılacak veri, talebi yapan gerçek veya tüzel kişiye yazılı olarak taahhütlü veya iadeli taahhütlü posta ile veya elden teslim edilebilir.

(7) Anonim verilerin kamu kurum ve kuruluşlarına teslimi, talepleri halinde şifrelenmiş dosya ile "gov.tr" uzantılı e-posta adreslerine yapılabilir.

(8) Telefonla veri iletilemez.

(9) Veri talebinde bulunanlar, işledikleri verilerin sonuçlarını Kurum tarafından kontrol edilebilir bir dosya formatında hazırlar ve oluşturulan sonuçlarda bu Yönetmelik hükümlerine aykırı olarak işlenen verilere yer verilemez.

(10) Veri talebinde bulunanların işledikleri verilerin veri işleme süreçlerindeki tüm sonuçlarının bu Yönetmeliğe aykırı biçimde aktarılması sonucunu doğuracak veri içerip içermediği ilgili birim tarafından kontrol edilir. Bu

Yönetmelik hükümlerine aykırı olarak işlenen verileri içeren bölümlerin tespit edilmesi halinde sonuçların kullanılmasına izin verilmez.

(11) Veri talebinde bulunanların hatalı hesaplama sonucu elde ettiği bulgular sadece veri talebinde bulunanları bağlar.

(12) Veri talebinde bulunanlar, çalışmalarında elde ettikleri sonuçları yayımlarken kullandıkları Kurum verilerini kaynak göstermek zorundadır.

(13) Veri talebinde bulunanlar yayımladıkları rapor, makale ve benzeri çalışmalarının bir kopyasını, yayımlarından sonraki 30 gün içerisinde veriyi talep ettiği Kurumun ilgili birimine göndermekle yükümlüdür.

(14) Veri talebinde bulunanlar, aldıkları verileri taleplerinde ifade ettikleri amaç dışında farklı bir amaçla kullanamaz, çoğaltamaz, üçüncü kişilere veremez, satamaz veya devredemez.

Verilerin aktarıldığı kişi, kurum/kuruluşların sorumlulukları

MADDE 21 – (1) Verilere erişen Kurum personeli ile verilere erişen veya veri aktarımı yapılan kamu kurum ve kuruluşlarının personeli de dahil olmak üzere gerçek ve tüzel kişiler, sağlık hizmeti sunucularına ait bilgi işlem sistemlerinin yazılımını ve donanımını sağlayan gerçek ve tüzel kişiler;

a) Veri talebine uygun olarak yaptıkları çalışmaların, kişisel verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar; verilerin istenilen amaç dışında kullanılmaması ve paylaşılmaması için süre ile sınırlandırılmaksızın her türlü önlemi alırlar.

b) Kurum tarafından görüntülenmesi sağlanan ve aktarım yapılan veriler, kişisel verilerin gizliliği ilkesine bağlı kalmak şartıyla ilgili mevzuat, uluslararası anlaşmalar ve kamu hizmetinin gerektirdiği yükümlülüklere göre kullanılır. Aktarılan verilerin; yetkisi olmayan kişi, kurum ve kuruluşların eline geçmemesi için gerekli tüm tedbirler alınır.

(2) Bu Yönetmelik hükümlerine göre verilere erişen Kurum personeli dâhil olmak üzere veri aktarımı yapılan gerçek ve tüzel kişiler, sağlık hizmeti sunucularına ait bilgi işlem sistemlerinin yazılımını ve donanımını sağlayan gerçek ve tüzel kişiler;

a) Elde ettikleri verilerin gizliliğini korumak ve güvenliğini sağlamak, verileri yetkisiz kişilerin görmesini, öğrenmesini, eline geçirmesini ve amacı dışında kullanmasını önlemek amacıyla gerekli tedbirleri almak,

b) Verilerin aktarımı ve korunması hususunda mevzuatta yer alan hükümlere uymak,

zorundadır.

(3) Kişisel verilerin güvenliğinin sağlanmasına yönelik Kurul tarafından çıkarılan düzenlemelere uyulur.

Uygulanacak müeyyideler

MADDE 22 – (1) Kişisel verilerin korunması hususu ile ilgili hükümlere aykırı hareket edenler hakkında kabahatler bakımından, 6698 sayılı Kanunun 18 inci maddesi hükümlerinin uygulanmasını teminen durum Kurula bildirilir.

(2) Kurum tarafından kendilerine erişim yetkisi verilen kişilerden, kişisel verileri değiştiren veya bütünlüğünü bozanlar hakkında 5237 sayılı Kanunun ilgili maddeleri uyarınca suç duyurusunda bulunulur.

Verilerin korunmasına ilişkin Kurumca yürütülecek işlemler

MADDE 23 – (1) Kurum, Kurum veri kayıt sisteminde tuttuğu verilerin her türlü tehlikeye karşı güvenliğinin sağlanması amacıyla güvenlik önlemlerinin hazırlanmasını, uygulamaya konulmasını, güncellenmesini ve denetlenmesini sağlamakla yükümlüdür.

(2) Veri aktarım talebinde bulunan gerçek ve tüzel kişilerin Kurum veri kayıt sistemine doğrudan erişimine izin verilmez. Talep edilen verinin aktarımı sağlanır.

(3) HSGM, veri taleplerini karşılarken gerekli güvenlik önlemlerini alır. Kurum veri kayıt sistemine şifre ile erişimler, gerçek kişi (ad-soyad veya domain kullanıcı adı) kullanıcı şifreleri kullanılarak Kurumun belirlediği güvenlik önlem ve uygulamaları çerçevesinde yapılır. Erişimler, HSGM tarafından güvenlik önlemleri çerçevesinde kayıt altına alınır.

(4) Kurum veri kayıt sisteminde sadece test edilmiş ve onaylanmış Kurum uygulamaları aracılığı ile toplanan veriler esas alınır. Hatalar sonucu veya farklı nedenlerle verilerde değiştirilme, silinme, eklenme ihtiyacı oluşursa bu durum ilgili birim ile HSGM'deki yetkilendirilmiş kişiler ile tutanak altına alınmak suretiyle gerekli işlemler yapılır.

(5) Kurumca veriye erişim yetkisi verilmiş personelin Kurumdan ayrılması veya görev yeri değişikliği halinde yetkisiz kullanımın önlenebilmesi amacıyla erişim yetkileri ilgili birim tarafından resmi yazı ile HSGM'ye bildirilir. HSGM tarafından yetkilendirme sona erdirilmeden ayrılış işlemleri yapılamaz. Birim amirleri gerekli bildirim ve iptal etme işlemlerinin yerine getirilmesinden sorumludur. Personelin üzerinde çalıştığı veri ile ilgili sorumluluğu Kurumdan ayrıldıktan sonra da devam eder.

BEŞİNCİ BÖLÜM

Kurum Yazılımları ile Kurum Dışı Yazılımların Entegrasyonu, Entegrasyon Usulü

Kurum yazılımları ile kurum dışı yazılımların entegrasyonu

MADDE 24 – (1) Kurum ve Kurul tarafından belirlenen güvenlik tedbirlerine uyulmak kaydıyla dış paydaşların, Kuruma olan yükümlülüklerini yerine getirebilmek için yazılımlarının Kurum yazılımları ile entegrasyon taleplerini karara bağlamaya Kurum yetkilidir.

Entegrasyon usulü

MADDE 25 – (1) Yazılım entegrasyon ihtiyacı söz konusu olduğunda, Kurum dışı yazılım sahibi gerçek ya da tüzel kişiler HSGM'ye yazılı başvuruda bulunur.

ALTINCI BÖLÜM
Son Hükümler

Yürürlük

MADDE 26 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 27 – (1) Bu Yönetmelik hükümlerini Sosyal Güvenlik Kurumu Başkanı yürütür.