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, Rehberli 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.