Farmakovijilans Faaliyetlerinde Kişisel Verilerin Korunması Hakkında Kılavuz

TÜRKİYE İLAÇ VE TIBBİ CİHAZ KURUMU
01.08.2019

İçindekiler

BÖLÜM I
Giriş

1.1. Amaç

Bu kılavuzun amacı; farmakovijilans faaliyetleri sırasında kişisel verilerin korunmasını sağlamak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar hakkında bilgilendirme yapmaktır.

Farmakovijilans faaliyetleri 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) kapsamında koruyucu hekimlik ve kamu sağlığının korunması amaçları ile yürütülen faaliyetler olarak değerlendirilmektedir.

1.2. Dayanak

Bu Kılavuz; 6698 sayılı Kanun ve ilgili ikincil düzenlemelere dayanılarak hazırlanmıştır.

1.3. Kapsam

Bu kılavuz kişisel verilerinin işlenmesi için veri sahibinin açık rızasının aranmadığı tüm farmakovijilans faaliyetleri için geçerli olup, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişileri kapsar (Veri işleme; tamamen veya kısmen otomatik olarak ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla yapılabilir).

Bir klinik çalışma kapsamında gerçekleştirilen faaliyetler veya kişisel verilerinin işlenmesi için açık rıza alınan diğer şirket faaliyetleri kapsam dışıdır. 6698 sayılı Kanun'da yer alan istisnaî amaçlar kapsamında olmayan kişisel veri işleme faaliyetleri için açık rıza alınması gerekir.

Bu kılavuz, Türkiye dışındaki ülkelerin kişisel veri koruma mevzuatı ile farmakovijilans verilerinin işlenmesine ilişkin yasal ve idari düzenlemeleri içermez.

1.4 Tanımlar

a) Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

b) Advers olay: İlaç uygulanan bir hastada veya klinik çalışma gönüllüsünde ortaya çıkan istenmeyen ve söz konusu tedavi ile arasında mutlaka bir nedensellik ilişkisi bulunmayan tıbbî olayı,

c) Advers reaksiyon/şüpheli advers reaksiyon: Bir ilaca karşı gelişen zararlı ve amaçlanmayan cevabı,

ç) Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

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

e) Bireysel olgu güvenlilik raporu (BOGR), Advers (ilaç) reaksiyon raporu: Tek bir hastada belli bir zaman noktasında belli bir ilaca karşı gelişen bir veya birden fazla şüpheli advers reaksiyonu bildirirken kullanılan belirli format ve içeriğe sahip raporu,

f) Farmakovijilans: Advers reaksiyonların ve ilaçlarla ilgili diğer sorunların tespit edilmesi, değerlendirilmesi, anlaşılması ve önlenmesine yönelik yürütülen faaliyetler ve bilimsel çalışmaları,

g) Güvenli giriş katmanı (SSL): Sunucu ile istemci arasında akan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikayı,

ğ) İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

h) İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

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

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

j) 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 sağlık verileri üzerinde gerçekleştirilen her türlü işlemi,

k) Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

l) Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

m) Kişisel verilerin silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hâle getirilmesi işlemini,

n) Kurul: Kişisel Verileri Koruma Kurulunu,

o) Kurum: Kişisel Verileri Koruma Kurumunu,

ö) Özel Nitelikli Kişisel Veriler: 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,

p) Raportör: Advers reaksiyon bildirimini yapan kişiyi,

r) Sağlık mesleği mensubu (SMM): Şüpheli advers reaksiyonların bildirilmesi bağlamında; hekim, eczacı, diş hekimi, hemşire ve ebeleri,

s) Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

ş) Şirket: Ruhsat sahibi ve/veya ruhsat sahibinin hizmet aldığı sözleşmeli hizmet kuruluşları (üçüncü kişi hizmet verenleri),

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

u) Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

ü) Veri sorumlusu: Kişisel sağlık verilerinin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.

1.5. Farmakovijilansta kişisel veriler

Şirketler, şüpheli advers reaksiyonların bildirimine ilişkin yasal yükümlülüklere uymak ve hasta güvenliğini sağlamak üzere farmakovijilans faaliyetleri gerçekleştirirken, rutin olarak veri toplarlar. Farmakovijilans verileri; vakaya konu olan hastaya ilişkin kişisel veriler veya özel nitelikli kişisel veriler ile raportöre ilişkin kişisel verileri içerebilir.

Diğer verilerle eşleştirildiğinde ilgili kişiyi ve ilgili kişiye ait sağlık verilerini gösterme niteliğini hâiz durumlarda söz konusu veriler özel nitelikli kişisel veriler olarak kabul edilmektedir. Bildirimde bulunan kişiye ilişkin adı ve soyadı bilgisi, meslek bilgisi ile iletişim bilgileri ise kişisel veri olarak değerlendirilmektedir.

Advers reaksiyon bildirimlerinde; güvenlilik verisinin etkin bir şekilde analiz edilebilmesi için hastanın yaşı/yaş grubu, cinsiyeti, kilosu, boyu, tıbbî geçmişi ve mevcut durumunu bilmek gerekir.

Bir hastanın adı ve soyadının baş harfleri veya atanmış bir numara ve/veya doğum tarihi, mükerrer bildirimlerin belirlenmesi için önem taşır. Ayrıca eksiksiz ve doğru verilerin toplanmasını sağlamak üzere etkin bir takip gerçekleştirmek için bildirimde bulunan kişinin ismi ve iletişim bilgileri de gerekir.

Şirketler farmakovijilans faaliyetleri sırasında kişisel verileri işlediklerinde 6698 sayılı Kanuna uymalı ve kişisel verilerin korunmasını sağlamak için şeffaf ve güvenilir süreçler uygulamalıdır. Veri sorumluları tarafından alınması gereken teknik ve idari tedbirler için 6698 sayılı Kanunun 12 nci maddesi birinci fıkrası uyarınca KVKK tarafından hazırlanan "Kişisel Veri Güvenliği Rehberi" dikkâte alınmalıdır. Buna ilâveten 6698 sayılı Kanun'un 6 ncı maddesinin dördüncü fıkrası uyarınca Kurul tarafından 2018/10 sayılı Karar ile belirlenen yeterli önlemler de göz önünde bulundurulmalıdır. Veri sorumluları ile veri işleyen sıfatını hâiz taraflarca alınması gereken teknik ve idari tedbirler ile yeterli önlemler yukarıda anılan düzenlemelerle sınırlı olmayıp, ileride gündeme gelebilecek Rehber ve Kararlarda yer alan tedbir ve önlemlerin de alınması gerekmektedir.

BÖLÜM II
Farmakovijilans verilerinin alınması ve takibi

2.1. Farmakovijilans verilerinin alınması

Bir advers olay ilaç şirketine bildirildiğinde "tanımlanabilir bir hasta" ve "tanımlanabilir bir raportör"ün olmasına ilişkin farmakovijilans gerekliliklerinin yerine getirilebilmesi için bazı kişisel verilerin toplanması gerekir.

Farmakovijilans mevzuatı; şirketlerin, bireysel olgu güvenlilik raporlarının asgari kriterleri içerecek bilgiyi sağlamalarını garanti etmelerini şart koşmaktadır. Ayrıca, hasta ile ilgili bilginin mümkün olduğunca tam olması gerekmektedir. Hasta ile ilgili bilgilerin tam olması gerekliliği, hastaya ait kimlik bilgilerinin birebir olduğu şekilde bildirilmesi anlamına değil; advers reaksiyon bildirimi için gerekli tüm alanların mevzuat hükümlerine uygun bir şekilde doldurulması anlamına gelir. Kanun'un 4 üncü maddesinin ikinci fıkrasında, kişisel verilerin işlenmesinde uyulması gereken ilkeler arasında "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi de yer alır. Bu kapsamda şirketler; advers reaksiyon bildirimi yapan SMM'lerden, hastanın açık rızası olmadan açık adını ve iletişim bilgilerini talep edemezler.

Kişisel verilerin işlenebilmesi için açık rıza ve istisnaî haller olmak üzere iki farklı hukuki sebep bulunmaktadır. Kişisel veriler için söz konusu istisnaî haller 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasında, özel nitelikli kişisel veriler için ise Kanunun 6 ncı maddesinin üçüncü fıkrasında yer almaktadır. İstisnaî hallerden herhangi birinin varlığı halinde açık rıza alınmasına gerek bulunmamaktadır.

Farmakovijilans kapsamında, özel nitelikli kişisel veriler dışında kalan ad soyad, iletişim bilgileri vb. gibi kişisel veriler, 6698 sayılı Kanunun 5 inci maddesi kapsamında; kanunlarda açıkça öngörülmesi, veri sorumlusu olan ilaç şirketinin hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması nedeniyle veri sahibinin açık rızası aranmaksızın işlenebilir.

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ise, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

Veri sahibinin advers olayı yaşayan kişi veya advers olayı bildiren kişi (örn; bir sağlık mesleği mensubu (SMM) veya hasta yakını) olmasından bağımsız olarak;

- Farmakovijilans amacıyla veri sahibine ilişkin kişisel verilerin işlenmesi için veri sahibinden rıza alınması şart değildir.
- Bu kılavuzun giriş bölümünde belirtildiği üzere özel nitelikli kişisel veri olarak değerlendirilebilecek farmakovijilans verilerinin, yine farmakovijilans amacıyla sır saklama yükümlülüğü altında bulunan kişiler tarafından işlenmesi, 6698 Sayılı Kanunun 6 ncı maddesinin üçüncü fıkrası uyarınca kamu sağlığının korunması ve koruyucu hekimlik faaliyetleri kapsamında değerlendirilmektedir. Ancak, açık rızanın gerekmemesi, Kanun hükümlerinden muafiyet anlamına gelmemekte olup, başta aydınlatma yükümlülüğü ile veri güvenliğine ilişkin yükümlülükler olmak üzere diğer tüm yükümlülüklerin yerine getirilmesi gerekmektedir.

Ancak, 6698 sayılı Kanunun 10 uncu maddesinde düzenlenmekte olan aydınlatma yükümlülüğü kapsamında veri sahiplerinin (bir advers olay yaşayan ve farklı olmaları durumunda advers olay bildirimini yapan kişilerin) kendilerine ait kişisel verilerin hangi amaçlarla işleneceği, veri sorumlusunun kim olduğu, işlenen verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile veri sahibinin 6698 Sayılı Kanunun 11 inci maddesinde sayılan hakları konularında bilgilendirilmeleri gerekir. Verilerin aktarılabileceği tarafların ismen belirtilmesi zorunlu olmayıp, kategori olarak belirtilmeleri (örn; Sağlık Bakanlığı) yeterli olacaktır. Bu bilgiler kolaylıkla anlaşılabilen Veri Koruma Aydınlatma Metni (VKAM) içeriğinde net bir şekilde yazılmış olmalıdır.

Farklı kanallardan ulaşan, farklı türdeki advers olay bildirimleri, şirketin farklı VKAM metinleri kullanmasını gerektirebilir (bkz. Ek). Şirketin, bir SMM tarafından veya veri sahibinin kendisi dışında aile üyesi, yakını gibi kişiler tarafından yapılan advers olay bildirimlerinde, veri sahibine doğrudan VKAM sunması mümkün değildir. Bu gibi durumlarda veri sahibinin VKAM'a ne şekilde ulaşabileceği SMM'ye veya advers olay bildiriminde bulunan kişiye aktarılır, VKAM'a şirketin internet sitesinde yer verilir. Şirket, VKAM'a farklı mecralardan ulaşılabilmesi için de gerekli önlemleri alır. VKAM, 6698 sayılı Kanunun 10 uncu maddesi ile Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun olarak hazırlanır.

2.2. Farmakovijilans verilerinin takibi

Bildirimde bulunan kişiyle gerçekleştirilen iletişimler, daha önce bu kişiye bir aydınlatma yapılmamış olması halinde bir VKAM gerektirir; Ek'de yer alan metin, bildirimde bulunan kişiye gönderilen şirket takip talep formlarına veya advers olay formlarına eklenebilir.

İlk raporlayıcının hasta veya hasta yakını olduğu durumlarda, hastaların SMM'leri ile takip gerçekleştirebilmek için hastalardan her zaman rıza alınmalıdır.

BÖLÜM III
Veri girişi, işlenmesi ve aktarılması

3.1. Veri girişi – hukuka ve dürüstlük kurallarına uygun işleme

6698 sayılı Kanunun 12 nci maddesinin birinci fıkrası uyarınca şirketler; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

3.2. Kişisel veri güvenliğine ilişkin idari tedbirler

3.2.1. Kişisel veri işleme envanteri hazırlanması, mevcut risk ve tehditlerin belirlenmesi

Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek uygun tedbirlerin alınması gerekmektedir.

3.2.2. Çalışanların eğitilmesi ve farkındalık çalışmaları

Kişisel verilerin işlenmesi sırasında aşağıda belirtilen ihlâllerin yapılması veri güvenliğini tehdit etmektedir:

1. Kişisel verilerin hukuka aykırı olarak açıklanması veya paylaşılması,
2. Siber saldırılara maruz kalınması:
    a. Kötü amaçlı yazılım içeren elektronik posta eki gönderilmesi ve kullanıcıların dikkatsizlik, dalgınlık ya da tecrübesizlik sonucu bu eki açmaları,
    b. Elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması,
3. Kişisel verilerin izinsiz veya yasalara aykırı işlenmesi,
4. Kişisel verilerin kazara kaybı, imhası veya hasar görmesi.

Şirketler, yukarıda belirtilen tehditlere karşı uygun önlemleri almalıdırlar. Bu önlemlere, kişisel verilere erişimi olan çalışanların güvenilir olmasını sağlamak üzere makul adımların atılması da dâhil edilmelidir.

Çalışanların kişisel verilerin korunması ve yasalara uygun şekilde işlenmesine ilişkin eğitim alması ve bu konudaki farkındalıklarının sağlanması gerekmektedir. Ayrıca; çalışanların sınırlı bilgileri olsa dahi kişisel veri güvenliğini zedeleyecek saldırılar ve siber güvenliğe ilişkin ilk müdahaleyi yapmaları da büyük önem taşımaktadır:

- Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımında belirlenmelidir.
- Kişisel veri içeren ortamlara erişim hakkı verilirken "Yasaklanmadıkça her şey serbesttir." prensibi değil, "İzin verilmedikçe her şey yasaktır." prensibine uygun hareket edilmelidir.
- Çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik taahhütnamesi imzalanmalıdır.
- Çalışanların güvenlik politika ve süreçlerine uymaması durumunda devreye girecek bir disiplin süreci de mutlaka olmalıdır.
- Kişisel veri güvenliğine ilişkin politika ve süreçlerde önemli değişikliklerin meydana gelmesi durumunda; yapılacak yeni eğitimler ile bu değişikliklerin, çalışanların bilgisine sunulması ve kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerin güncel tutulması sağlanmalıdır.
- Veri girişi veya diğer işleme faaliyetlerinde kişisel verilerin üçüncü kişilerle paylaşılması durumunda, uygun güvenlik önlemlerinin alınması şirketin sorumluluğundadır.
- Şirketler ile veri işleyen sıfatını hâiz taraflar arasında, kişisel verilerin yalnızca şirket talimatları doğrultusunda işlenmesini ve kişisel verilerin işlenmesine yönelik uygun güvenliğin sağlanmasını zorunlu kılan bir yazılı sözleşme imzalanması gerekmektedir.

3.2.3. Kişisel veri güvenliği politikalarının ve süreçlerinin belirlenmesi

- Kişisel veri güvenliğine ilişkin doğru ve tutarlı politika ve süreçler belirlenmeli, söz konusu politika ve süreçler veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir.
- Bu kapsamda düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yapıldıktan sonra da düzenli olarak kontrollere devam edilmelidir.
- Her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlâllerinin nasıl yönetileceği de açıkça belirlenmelidir.

3.2.4. Kişisel verilerin mümkün olduğunca azaltılması

6698 sayılı Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, doğru ve gerektiğinde güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Şirketler, işledikleri verileri neden belirli bir süre boyunca saklamaları gerektiğini de gerekçelendirilebilmelidir (bkz. Bölüm 5.6). Veri Sorumluları Sicili'ne kayıt olmakla yükümlü olanlar söz konusu sürelere, hazırlayacakları kişisel veri imha politikasında yer vermelidirler.

Bunun yanında, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmekte ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

3.2.5. Veri işleyenler ile ilişkilerin yönetimi

Veri sorumlularının bilgi teknolojileri ihtiyaçlarını karşılamak için veri işleyenlerden hizmet alması durumunda veri işleyenlerin kişisel veriler konusunda en az veri sorumluları tarafından sağlanan güvenlik seviyesinin sağlandığından emin olması gerekmektedir. Zira 6698 sayılı Kanunun 12 inci maddesinin ikinci fıkrası gereği veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusuyla müştereken sorumludur. Veri işleyen ile yazılı bir sözleşme imzalanmalı ve sözleşmede aşağıdaki hükümler de yer almalıdır:

- Veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile Kişisel Veri Saklama ve İmha Politikasına uyumlu şekilde hareket edeceği,
- Veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tâbi olacağı,
- Herhangi bir veri ihlâli olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna; veri sorumlusunun da derhal Kişisel Verileri Koruma Kurulu'na ve ilgili kişiye bildirme yükümlülüğü olacağı,
- Sözleşmenin niteliğinin elverdiği ölçüde, veri sorumlusu tarafından veri işleyene aktarılan kişisel veri kategori ve türlerinin de ayrı bir maddede belirtilmiş olması gerekeceği.

Bununla birlikte veri sorumlusu, kişisel veri içeren sistem üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir.

Veri sorumluları tarafından alınabilecek idari tedbirler Tablo I'de özet olarak gösterilmiştir:

Tablo I. İdari tedbirler

İdari Tedbirler
Kişisel veri işleme envanteri hazırlanması
Eğitim ve farkındalık faaliyetleri (Bilgi güvenliği ve Kanun)
Kurumsal politikalar (Erişim, Bilgi güvenliği, Kullanım, Saklama ve imha vb.)
Sözleşmeler (Veri sorumlusu -Veri sorumlusu, Veri sorumlusu - Veri işleyen arasında)
Gizlilik taahhütnameleri
Kurum içi periyodik ve/veya rastgele denetimler
Risk analizleri
İş sözleşmesi, Disiplin Yönetmeliği (Kanuna uygun hükümler ilâve edilmesi)
Kurumsal iletişim (Kriz yönetimi, Kurul ve ilgili kişiyi bilgilendirme süreçleri, itibar yönetimi vb.)
Veri sorumluları sicil bilgi sistemine (VERBİS) bildirim

3.3. Kişisel veri güvenliğine ilişkin teknik tedbirler

3.3.1. Siber güvenliğin sağlanması

Siber güvenliğin sağlanmasında tavsiye edilen yaklaşım, birçok prensip dâhilinde tamamlayıcı niteliğe sahip ve düzenli olarak kontrol edilen birtakım tedbirlerin uygulanmasıdır. Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler aşağıda sıralanmıştır:

- Kullanılmakta olan ağa derinlemesine nüfuz etmeden ihlâllerin durdurulabilmesi için güvenlik duvarı oluşturulması,
- Çalışanların, kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önlemek için internet ağ geçidi kullanılması,
- Kötü amaçlı yazılımlardan korunmak için bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması ve güncel tutulması,
- Güvenlik açıkları olan yazılımlarla, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması,
- Yama yönetimi ve yazılım güncellemeleri yapılması,
- Kişisel veri içeren sistemlere erişimin sınırlı olması,
    - Çalışanlara yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınması ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanması,
    - Farmakovijilansta kullanılan kişisel verileri içeren veri tabanlarının, veride yapılan değişiklerin saptanabilmesine olanak sağlayacak şekilde tam olarak valide edilmiş veya test edilmiş olması ve bu veri tabanlarına erişimin sadece belirlenmiş kişilerle sınırlı olması,
    - Şifreler oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi,
    - Veri sorumlularının erişim yetki ve kontrol matrisi oluşturmaları ve ayrı bir erişim politika ve süreçleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve süreçlerin uygulamaya alınması,
    - Kaba kuvvet algoritması kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayılarının sınırlandırılması,
    - Düzenli aralıklarla şifrelerin değiştirilmesinin sağlanması,

- Yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması,
- Veri sorumlusuyla ilişikleri kesilen çalışanlar için derhal hesabın silinmesi ya da girişlerin kapatılması,
- Veri sorumluları tarafından farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi.

3.3.2. Kişisel veri güvenliğinin takibi

Veri sorumlusunun sistemlerine yapılabilecek saldırıların önlenmesi ya da siber suçlara veya kötü amaçlı yazılımlara maruz kalınmaması için aşağıdaki tedbirleri alması gerekmektedir:

- Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
- Bilişim ağlarında sızma veya beklenmeyen hareketler olup olmadığının belirlenmesi,
- Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
- Güvenlik sorunlarının bildirilmesi için resmi bir raporlama sürecinin oluşturulması,
- Güvenlik sorunlarının veri sorumlusuna mümkün olduğunca hızlı bir şekilde raporlanması.

Alınan tedbirlere rağmen; bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlâller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

3.3.3. Kişisel veri içeren ortamların güvenliğinin sağlanması

- Kişisel veriler, veri sorumlularının yerleşkelerinde ya da dışında yer alan cihazlarda, elektronik ya da kağıt ortamlarda saklanıyor ise, çalınma veya kaybolma gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması, ayrıca fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş ve çıkışların kontrol altına alınması,
- Farmakovijilans verilerini içeren belgelerin gözetimsiz bırakılmaması, şirketlerin farmakovijilans belgeleri için temiz masa politikasını benimsemesi,
- Kişisel veriler elektronik ortamda ise; ağ bileşenleri arasında erişimin sınırlandırılması veya bileşenlerin ayrılması,
- Elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi,
- Çalışanların şahsi elektronik cihazlarının bilgi sistem ağına erişimi sırasında yeterli güvenlik tedbirlerinin alınması,
- Kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş ve çıkış kayıtlarının tutulması gibi fiziksel güvenliğin artırılmasına ilişkin önlemlerin alınması,
- Kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması, şifre anahtarının sadece yetkili kişilerin erişebileceği ortamda saklanması ve yetkisiz erişimin önlenmesi,
- Kağıt ortamındaki evrakların kilitli şekilde sadece yetkili kişilerin erişebileceği ortamlarda yangın önleyici dolaplar/arşivler gibi emniyetli ve sağlam alanlarda saklanması ve yetkisiz erişimin önlenmesi,

- Hangi şifreleme yöntemi kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunması ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanımının tercih edilmesi gerekmektedir.

3.3.4. Kişisel verilerin bulutta depolanması

- Kişisel verilerin bulutta saklanabilmesi için bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının veri sorumlusu tarafından kontrol edilmesi,
- Bulutta depolanan kişisel verilerin ayrıntılı olarak bilinmesi, yedeklenmesi, senkronizasyonunun sağlanması ve gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün yapılması,
- Depolanma ve kullanım sırasında şifrelemenin kriptografik yöntemlerle yapılması, verilerin buluta şifrelenerek atılması ve hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarlarının kullanılması,
- Bulut bilişim hizmet ilişkisi sona erdiğinde; şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekmektedir.
- Bulut hizmeti alınan firmanın sunucularının ülkemizde veya Kurum tarafından açıklanan güvenilir ülkeler listesinde yer alan ülkelerden birinde bulunması gerekmektedir. Veri sahibinden açık rıza alınması halinde bu kural geçerli değildir.

3.3.5. Bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı

- Veri sorumlusu tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimlerinin göz önüne alınması,
- Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontrollerin yapılması, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmalarının yerleştirilmesi,
- Uygulamaların, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanması,
- Arızalanan veya bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi,
- Bakım ve onarım için dışarıdan personel gelmesi durumunda verilerin kopyalanarak kurum dışına çıkarılmaması için gerekli tedbirlerin alınması gerekmektedir.

3.3.6. Kişisel verilerin yedeklenmesi

- Yedeklenen kişisel verilere sadece sistem yöneticisinin erişebilmesi, veri seti yedeklerinin mutlaka ağ dışında tutulması,
- Tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunması gerekmektedir.

Veri sorumluları tarafından alınabilecek teknik tedbirler Tablo II'de özet olarak gösterilmiştir:

Tablo II. Teknik tedbirler

Teknik Tedbirler
Yetki matrisi

Yetki kontrol
Erişim logları
Kullanıcı hesap yönetimi
Ağ güvenliği
Uygulama güvenliği
Şifreleme
Sızma testi
Saldırı tespit ve önleme sistemleri
Log kayıtları
Veri maskeleme
Veri kaybı önleme yazılımları
Yedekleme
Güvenlik duvarları
Güncel anti-virüs sistemleri
Silme, yok etme veya anonim hale getirme
Anahtar yönetimi

3.3.7. Verilerin yurtdışına aktarılması

Farmakovijilans verilerinin şirketin Türkiye dışındaki ana farmakovijilans sistemine veya Türkiye dışından erişilebilen bir veri tabanına girilmesi, veri koruması mevzuatı çerçevesinde kişisel verilerin yurtdışına aktarımı anlamına gelmektedir.

Eğer kişisel verilerden oluşan farmakovijilans verileri Türkiye dışındaki ana sistemde barındırılıyorsa veya burada yedeklenmişse, farmakovijilans verileri Türkiye dışında görülebilir olmasa bile bu durum kişisel verilerin yurtdışına aktarımı olarak değerlendirilir.

Verileri alan ülke veya bölgenin kişisel verilerin işlenmesi hakkında veri sahibi kişilere hakları için yeterli bir koruma sağladığı durumlar haricinde ya da daha genel bir ifade ile 6698 sayılı Kanunun 9 uncu maddesinde yer alan hükümlere uygunluğun sağlanamadığı durumlarda kişisel verilerin yurtdışına aktarımı kural olarak yasaktır.

Kişisel verilerin aktarılacağı ülkede yeterli korumanın bulunmaması durumunda; Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulunun izninin bulunması halinde ilgili kişinin açık rızası aranmaksızın kişisel veriler yurt dışına aktarılabilir. Bu durumda şirket kişisel verilerin işlenmesine yönelik yeterli bir koruma sağlayacak düzenlemeleri devreye sokmalıdır. Ayrıca, KVKK, yurtdışına veri aktarımı için ek düzenlemeler getirebilir.

Türkiye dışında yeterli koruma sağladığı kabul edilen ülkelere, 6698 sayılı Kanunda yer alan sınırlandırmalara uygun olarak ilgili kişinin açık rızası aranmaksızın kişisel veriler yurt dışına aktarılabilir.

Farmakovijilans verilerinin aktarılması için şirketlerin mevcut aktarım çözümlerinin güvenilir olması gerekmektedir. Hâlihazırda uygun bir çözümün olmaması durumunda, veriler yurtdışına aktarılmamalı veya aksi takdirde;

- Aktarımlara limit koyulmalı ve farmakovijilans verilerine yalnızca Türkiye'den erişilmesi sağlanmalıdır veya
- Aktarım öncesinde veriler anonimleştirilmelidir.

Aynı veri koruması ilkeleri Türkiye dışındaki idari otoritelere ve hukuki iş birliği içerisinde bulunulan üçüncü kişi ve kurumlara veri aktarımı gerçekleştirildiğinde de geçerlidir.

Kişisel verilerin anonim hale getirilmesi için Kişisel Verileri Koruma Kurumu tarafından hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'nden istifade edilebilir.

BÖLÜM IV
Erişim, düzeltme ve itiraz hakları

4.1. Kişisel verilere erişim

İlgili kişi (veri sahibi) kendisiyle bağlantılı farmakovijilans verilerine, diğer kişisel verilerine erişim hakkıyla aynı erişim hakkına sahiptir.

4.2. İlgili kişinin erişim talebine cevap verme

İlgili kişi, erişim talebini yazılı olarak veya Kişisel Verileri Koruma Kurulunun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir.

İlgili kişilerin talepleri, 6698 sayılı Kanunun 13 üncü maddesine göre değerlendirilir. Bu kapsamda; veri sorumlusu, başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Veri sorumlusuna başvuru ve işlemin ayrıca bir maliyet gerektirmesi hâlinde alınacak ücret "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" hükümlerine göre yapılır.

Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi hâlinde veri sorumlusunca gereği yerine getirilir.

Bir kişi ancak kendisiyle ilgili kişisel verilere erişim hakkına sahiptir. Bu nedenle şirketlerin talepte bulunan kişinin kimliğini doğrulamak için makul adımlar atması gerekmektedir (Bir kişi bir üçüncü kişi aracılığıyla talepte bulunabilir; bu durumda şirketin üçüncü kişinin ilgili kişi adına hareket etmeye yetkili olduğu konusunda ikna olması gerekir). Farmakovijilans verilerinin kişinin yakınları ve vekili ile paylaşılmasına ilişkin hususlarda 6698 sayılı Kanun, Hasta Hakları Yönetmeliği ve Kişisel Sağlık Verileri Hakkında Yönetmelik hükümlerine riayet edilir.

Sunulan bilgiler talepte bulunan kişi tarafından anlaşılmalı; örneğin, teknik terimler ve kısaltmalar açıklanmalıdır.

Veri sahibinin 6698 sayılı Kanun'un 11 inci maddesinde yer alan haklarını kullanmak istemesi halinde bu başvurunun, şirketin Hukuk Departmanı ve/veya Veri Koruma Görevlisi ya da bu konuda cevap vermeye yetkin bir kişi tarafından yönetilmesi tavsiye edilir.

Hatırlatma: Bildirimlerin bir SMM'den alınması durumunda şirketler bir hastanın tam kimliğine sahip olmaz. Bu gibi bildirimlerde hastanın erişim veya düzeltme talebi SMM aracılığıyla gerçekleştirilmelidir.

4.3.Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi 6698 sayılı Kanunun 7 nci maddesi ile "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" hükümlerine göre yapılır.

Bir veri, 6698 sayılı kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması ve verilerin daha uzun süre saklanmasını gerektiren bir neden bulunmaması halinde kişisel veriler res'en veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

Bir kişi kendisi hakkında tutulan bilgilerin doğruluğuna itiraz ediyorsa, yeni bilgilerin doğruluğunu sorgulamak için hiçbir neden olmadığı varsayılarak söz konusu bilgiler değiştirilmeli veya silinmelidir.

Farmakovijilans kaynak dokümanı veri sahibi tarafından istenilse bile imha edilmemelidir (veri sahibinin kimliğinin saptanmasına neden olabilecek herhangi bir kişisel veri hariç). Bu dokümanlar muhafaza edilmeli ve değiştirilmemelidir.

Kişisel verilerin imha süreçleri, Veri Sorumluları Sicili'ne kayıt olmakla yükümlü veri sorumluları tarafından hazırlanan Kişisel Veri Saklama ve İmha Politikası'na uygun olarak yürütülür.

İlaçların Güvenliliği Hakkında Yönetmelik'in 28 inci maddesi uyarınca, ilaçlarla ilgili farmakovijilans verileri ve belgeleri, ilgili ilacın ruhsatı geçerliliğini koruduğu sürece ve ruhsat geçerliliği sona erdikten sonra en az 10 yıl geçmedikçe imha edilemez.

4.4.Kişisel verilerin işlenmesine itiraz

Veri sahibi, verilerin işlenmesinin önemli bir zarar veya sıkıntıya neden olması veya böyle bir ihtimalin olması durumunda, kişisel verilerinin işlenmesine itiraz etme hakkına sahiptir. İşleme süreci farmakovijilans için bir yasal yükümlülüğü yerine getirmek üzere gerçekleştiriliyorsa, şirket böyle bir talebi cevaplarken neden talebin yerine getirilemediğini açıklar.

Şirketler, veri sahibi başvurularına, talebi aldıktan sonra 30 gün içerisinde cevap vermelidir. Cevapta şirketin o kişiye ilişkin kişisel verilerin neden bir bölümünü veya hepsini işlemeye devam edeceği veya talebin ne şekilde yerine getirileceği açıklanmalıdır.

Örneğin; *Yasalar gereği, şirketler ilaçlarının güvenliliğini denetlemek için kendi ilacına karşı gelişen bir advers olayı veya potansiyel bir advers reaksiyonu yaşamış olan kişilerle bağlantılı bazı minimum bilgileri toplamak zorundadır.*

BÖLÜM V
Kişisel verilerin saklanması ve düzeltilmesi

5.1.Kişisel verilerin saklanması

6698 Sayılı Kanun, şirketlerin belirli bir veri işleme faaliyeti için gerekenden fazla kişisel veri tutmamasını ve verilerin işleme amacına bağlı olarak gereğinden uzun süre tutulmamasını gerektirir. Ayrıca kişisel veriler, toplama ve/veya kullanma amaçları ile alâkalı ve yeterli düzeyde olmalı ancak olması gerekenden daha fazla bilgiyi de içermemelidir. Bu nedenle; güvenlilik ile ilgili veri tabanlarına girilen veriler yalnızca farmakovijilans amacıyla işlenmeli ve veri sahibi kişiye VKAM ile açıklanmış nedenler dışında işlenmemelidir.

5.2.Kişisel verilerin düzeltilmesi

Şirketler, güvenlilik raporlama faaliyetlerini uygun şekilde yerine getirmek üzere 'veri minimizasyonu' yapmalı, yani minimum miktarda kişisel veriyi belirlemelidir. Bir şirket, bu işlemlerin gerçekleştirilmesinin farmakovijilans yükümlülüklerini riske atması durumunda, anonimleştirme işlemi yapmamalı veya kişisel verileri düzeltmemelidir.

5.3.Hastalara ilişkin kişisel veriler

Şirketler, kişisel veri unsurlarının düzeltilip düzeltilmeyeceğini belirlerken, verilerin güvenlilik veri tabanında tutulması için geçerli bir neden (mükerrer işlemlerin saptanması ve takip faaliyetlerinin gerçekleştirilmesi gibi) olup olmadığını dikkate almalıdır.

Etkin bir farmakovijilans değerlendirmesi için saklanması tavsiye edilen unsurlar: Hastanın adı ve soyadının baş harfleri veya olgu referans numarası, cinsiyet, doğum tarihi, başlangıçtaki yaş/yaş grubu ve advers olay: semptomlar, sonuç, süre, şüpheli ilaç, tıbbî geçmiş, birlikte kullanılan ilaçlar.

Etkin bir farmakovijilans için genelde şart olmayan ve redaksiyon yapılması tavsiye edilen unsurlar: Hastanın adı, iletişim bilgileri (adres, telefon, e-posta adresi) ve dosya numarası. Şirketler, kaynak verilerden farmakovijilans için gerekli olmayan unsurların çıkarılmasını (örn; kağıt doküman üzerinde siyah keçeli kalem ile, kayıtlardaki taranmış dokümanlarda ise Adobe Acrobat'ın redaksiyon aracı ile) ve isim ile adres bilgilerinin veri tabanına girilmemesini düşünmelidir. Hastanın aynı zamanda bildirimde bulunan kişi olması veya takip bilgilerinin elde edilebilmesi için tek kaynak olması durumunda, bu bilgilerin saklanması kabul edilebilir.

5.4.Sağlık mesleği mensuplarının kişisel verileri

Takip faaliyetleri tamamlansa bile, advers olayların yeniden değerlendirilmesi gerekebileceğinden, SMM'lerin isim ve iletişim bilgileri gibi verilerinin saklanması tavsiye edilir.

5.5. Güvenlilik verilerinin iş ortakları ve tedarikçilerle paylaşılması

Bir advers olay bildirimi başka bir şirkete iletildiğinde, yalnızca alıcının makul bir şekilde ihtiyaç duyduğu ve farmakovijilansın amaçlarıyla tutarlı olan bilgiler aktarılmalıdır. Bölüm 2.1'de belirtildiği gibi, VKAM alıcılara ilişkin ayrıntıları sunmalıdır.

5.6. Saklama süresi

İlaçların Güvenliliği Hakkında Yönetmelik'in 28 inci maddesinde ilaçlarla ilgili farmakovijilans verileri ve belgeleri, ilacın ruhsatı geçerliliğini koruduğu sürece ve ruhsat geçerliliği sona erdikten sonra en az 10 yıl süreyle saklanması gerektiği belirtilmektedir.

Farmakovijilans dışındaki bölümler tarafından alınan ve veri tabanlarında tutulan kişisel verileri içeren kaynak güvenlilik belgeleri farmakovijilans departmanıyla aynı şekilde yönetilmelidir.

Şirketler, iş ortakları ve tedarikçilerle yapılan sözleşmelerde farmakovijilans belgelerinin saklanmasına yönelik koşulları belirtmeli ve farmakovijilans belgelerinin diğer taraf bilgilendirilmeden imha edilmemesi gerektiğini açıklamalıdır.

BÖLÜM VI
Bildirim

6.1. Bildirim

Kişisel verileri işleyen gerçek ve tüzel kişiler, kendisine muafiyet tanınanlar hariç olmak üzere, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Söz konusu muafiyetin kapsamına Kişisel Verileri Koruma Kurulu tarafından karar verilir.

Farmakovijilans için gerçekleştirilen işlemler de dâhil olmak üzere, şirket olarak bütün veri işleme faaliyetlerini kapsayan bir bildirim yeterlidir. Bu kayıt, 6698 Sayılı Kanunun 16 ncı maddesinin 3 üncü fıkrasında belirtilen hususlara uygun olarak yapılmalıdır.

Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

- Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkında açıklamalar,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,

- Kişisel veri güvenliğine ilişkin alınan tedbirler,
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

Şirketler, farmakovijilans ile ilgili verilerin işlenmesi süreçlerinde kişisel verilerin işlenme amacına aşağıdaki gibi kısa bir açıklama yapabilirler:

İlaçların advers reaksiyonları hakkında sağlık mesleği mensuplarından ve hastalardan bilgi toplanması, bunların izlenmesi ve değerlendirilmesi.

BÖLÜM VII
Yaptırımlar

7.1. Yaptırımlar

KVKK, 6698 sayılı Kanuna uygun veri işlenmesini sağlamaya yönelik işlemler gerçekleştirebilir, ihlallere ilişkin olarak resen veya şikâyet üzerine denetimler gerçekleştirebilir. KVKK ayrıca veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında idari para cezası uygulama yetkisine sahiptir. Hukuka aykırı veri işleme faaliyetleri ayrıca 5237 sayılı Türk Ceza Kanunu'nun 135 vd. maddeleri kapsamında hapis cezası yaptırımı ile cezalandırılabilmektedir.

Seçilmiş Mevzuat:

Kanun:

- 26/09/2004 tarihli ve 5237 sayılı "Türk Ceza Kanunu"
- 24/03/2016 tarihli ve 6698 sayılı "Kişisel Verilerin Korunması Kanunu"

Yönetmelik:

- 15/04/2014 tarih ve 28973 sayılı Resmi Gazete'de yayımlanmış olan "İlaçların Güvenliliği Hakkında Yönetmelik"
- 28/10/2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanmış olan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"
- 16/11/2017 tarih ve 30242 sayılı Resmi Gazete'de yayımlanmış olan "Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik"
- 30/12/2017 tarih ve 30286 sayılı Resmi Gazete'de yayımlanmış olan "Veri Sorumluları Sicili Hakkında Yönetmelik"
- 28/04/2019 tarih ve 30758 sayılı Resmi Gazete'de yayımlanmış olan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik"
- 28/04/2019 tarih ve 30758 sayılı Resmi Gazete'de yayımlanmış olan "Veri Sorumluları Sicili Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik"
- 21/06/2019 tarih ve 30808 sayılı Resmi Gazete'de yayımlanmış olan "Kişisel Sağlık Verileri Hakkında Yönetmelik"

Tebliğ:

- 10/03/2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanmış olan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"
- 10/03/2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanmış olan "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"

Karar:

- Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararı
- Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24/01/2019 tarih ve 2019/10 sayılı Kararına İlişkin Duyuru
- Veri Sorumlusuna Başvuru ve Kurula Şikayet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı
- "Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları" ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/87 Sayılı Kararı

Kılavuz ve Rehber:

- 12/06/2014 tarihinde yayımlanan "İyi Farmakovijilans Uygulamaları (İFU) Kılavuzu Modül I–Advers İlaç Reaksiyonlarının Yönetimi ve Bildirimi"
- Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi

- Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi
- Kişisel Veri İşleme Envanteri Hazırlama Rehberi

Ek: Veri Koruma Aydınlatma Metinleri Örnekleri

Aşağıdaki taslak "veri koruma aydınlatma metni (VKAM)" örnek amaçlı olup, özel durumların ortaya çıkabileceği göz önüne alındığında bunlarla ilgili hukuki görüş alındıktan sonra gerekli değişiklikler yapılmalıdır.

İnternet sitesi

VERİ KORUMA AYDINLATMA METNİ

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gereğince <<FİRMA ADI>> olarak Veri Sorumlusu sıfatıyla Kanunun "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10 uncu maddesi uyarınca farmakovijilansla ilgili faaliyetlerimize yönelik kişisel verilerinizin toplanması ve işlenmesi ile ilgili hususlarda sizleri bilgilendirmek isteriz.

Kişisel verilerinizin işbu Aydınlatma Metni kapsamında işlenmesine ilişkin detaylı bilgilere [şirket web-sayfası adresi] adresinde yer alan <<FİRMA ADI>> Kişisel Verilerin Korunması ve İşlenmesi Politikası'ndan ulaşabilirsiniz.

1. Kişisel Verilerin İşlenme Amacı

İlaç şirketlerinin ilaç kullanımı sırasında ortaya çıkabilen advers reaksiyonların (yan etkilerin) ve ilaçlara bağlı diğer muhtemel sorunların saptanması, değerlendirilmesi, tanımlanması ve önlenmesi ile ilgili faaliyetleri yürütmesi zorunludur. Farmakovijilans adı verilen bu faaliyetler sonucu ilaç güvenliliğinin izlenmesi ve gerektiğinde ulusal ya da uluslararası düzeyde birtakım tedbirlerin alınarak halk sağlığının korunması mümkün hale gelir.

Advers ilaç reaksiyonları ve diğer farmakovijilans faaliyetleri ile ilgili olarak şirketimize ulaşan tüm kişisel veriler sadece farmakovijilans faaliyetleri için kullanılmaktadır. Kişisel verileriniz; KVKK, ilgili yönetmelikler ile uyumlu olacak şekilde toplanmakta ve işlenmektedir. Farmakovijilans faaliyetleri sırasında raportörün adını, iletişim bilgilerini ve mesleğini/bağlı olduğu kuruluş bilgilerini toplamaktayız. Farmakovijilans amacıyla advers olayların işlenmesi sırasında gerek duyarsak advers olayı deneyimleyen kişinin tıbbi öyküsü ve sağlığı ile ilişkili ilave kişisel veri toplamamız da gerekebilir.

2. Kişisel Verilerin Aktarılabileceği Taraflar ve Aktarım Amacı

Vereceğiniz bilgiler ilaç güvenliliğinin izlenmesine yönelik mevzuatta öngörülen hukuki yükümlülüklerin yerine getirilmesi amacıyla kullanılacak ve Türkiye İlaç ve Tıbbi Cihaz Kurumu ile paylaşılabilecektir. Bu verileriniz İlaç İzleme ve İşbirliği Programı kapsamında Dünya Sağlık Örgütü'nün veri tabanına da anonim hale getirilerek girilebilmektedir.

Şirketimiz; bize sağladığınız bilgiyi gerektiğinde global farmakovijilans veri tabanında işlenmesi ve farmakovijilans mevzuatı gerekliliklerinin yerine getirilmesi için ana grup şirketimiz, bağlı kuruluşlarımız, iş ortaklarımız ve servis sağlayıcılarımız (tedarikçi, hukuken yetkili kurum ve kuruluşlar ile hukuken yetkili özel hukuk tüzel kişileriyle) ile paylaşabilir.

Şirketimizin bazı farmakovijilans verilerini veri koruma düzeyleri farklılık gösteren ülkeler de dâhil olmak üzere Avrupa'daki ve dünyadaki diğer sağlık otoritelerine de bildirmesi gerekmektedir. Ancak bu raporlar olay hakkında ayrıntılı bilgi içermekle birlikte kişisel veriyi kısıtlı miktarda içermektedir:

- Hastalar: Yaş veya doğum tarihi/yılı, cinsiyeti, hasta adının baş harflerini de içeren bilgi (Hasta adı açık olarak bildirilmemektedir).
- Raportör: Kurumun raporlayan kişiyi takip etmesi için sağlanan isim, meslek, ad ve soy adının ilk harfleri, adres, e-posta, telefon numarası gibi bilgiler.

3. Kişisel Verilerin Toplama Yöntemi ve Hukuki Sebebi

Kişisel verileriniz, kağıt ortamda veya elektronik ortamda toplanmaktadır. Farmakovijilansa ilişkin verileriniz, 6698 sayılı Kanun'un 6 ncı maddesinin üçüncü fıkrasında yer alan kamu sağlığının korunması ile koruyucu hekimlik amaçlarıyla ve bu maddeye dayanılarak işlenmekte; kişisel verileriniz ise 6698 sayılı Kanun'un 5 nci maddesinin ikinci fıkrasının (ç) bendinde yer alan "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" kapsamında işlenmektedir.

4. Saklama

Farmakovijilans ile ilgili bilginin (advers olay raporları) halk sağlığı açısından önem arz etmesi sebebiyle ilacın pazarlandığı son ülkede piyasadan çekilmesinden sonra minimum 10 yıl daha raporların saklanması gerekmektedir.

5. Veri Sahiplerinin Hakları

6698 sayılı Kanun'un 11. maddesi uyarınca kişisel veri sahibi olarak aşağıdaki haklara sahipsiniz:

- Kişisel verilerinizin işlenip işlenmediğini öğrenme,
- Kişisel verileriniz işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerinizin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Yurt içinde veya yurt dışında kişisel verilerinizin aktarıldığı üçüncü kişileri bilme,
- Kişisel verilerinizin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- 6698 sayılı Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerinizin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerinizin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerinizin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Ancak, farmakovijilans mevzuatı yükümlülükleri gereğince şirketimiz farmakovijilans için işlem görmüş veriyi silemeyebilir ya da işlenmesini kısıtlamayabilir.

Kişisel veri sahipleri olarak aşağıda belirtilen haklarınıza ilişkin taleplerinizi [şirket web-sayfası adresi] adresinde yer alan <<FİRMA ADI>> Kişisel Verilerin Korunması ve İşlenmesi Politikası'nda belirtilen yöntemlerle Şirket'e iletmeniz durumunda talepleriniz Şirketimiz tarafından mümkün olan en kısa sürede ve her hâlükârda 30 (otuz) gün içerisinde değerlendirilerek sonuçlandırılacaktır.

Veri sorumlusunun adı ve iletişim bilgileri:
Şirketin adı, adresi
e-posta: …….

Telefon

Advers olayları almak üzere tasarlanmış bir departman bir çağrıyı cevapladığında aşağıdakiler geçerlidir.

Kişiye bir advers olay bildiriminde bulunduğunu söyleyin ve herhangi bir kişisel veriyi işlemeden önce aşağıdaki gibi bir veri VKAM sunun:

Bu telefon konuşmasında bizimle paylaşacağınız tüm bilgiler ve kişisel veriler, [ŞİRKETİN STANDART UYGULAMA PROSEDÜRÜ veya POLİTİKASI] ve yerel düzenlemeler uyarınca korunacak ve gizli tutulacaktır. Vereceğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır [ve talebinizi uygun bir şekilde ele almamızı sağlayacaktır] ve sağlık otoriteleri ile paylaşılabilecektir. Sizinle ilgili tuttuğumuz verilerinize erişim hakkına sahipsiniz. Daha detaylı bilgiye internet sitemizde yer alan "Farmakovijilans Kapsamında Kişisel Verilerin Korunması Aydınlatma Metni"nden ulaşabilirsiniz.

Kişisel verilerin paylaşıldığı diğer tarafların, kategorik olarak VKAM'ın içerisinde belirtilmesi gerekir.

Telefonun yanlışlıkla diğer departmanlar tarafından cevaplanması durumunda, telefonu cevaplayan kişi telefon eden kişiye bir advers olay bildiriminde bulunduğunu söylemeli, konuşmaları gereken kişinin kendileri olmadığını, ancak kendisinden bazı ayrıntılar alarak doğru kişinin kendisini aramasını sağlayacağını veya çağrıyı aktaracağını belirtmelidir. Herhangi bir kişisel verinin işlenmesi durumunda bir VKAM verilmelidir; bunun yalnızca bir kere verilmesi gerekir.

Daha küçük şirketler veya bağlı ofislerde, çağrılar doğrudan ilgili departman/kişi tarafından cevaplanmayabilir. Telefonu cevaplayan kişi, aramayı yapan kişiye bir olay bildiriminde bulunduğunu söylemeli, konuşmaları gereken kişinin kendileri olmadığını, ancak doğru kişinin kendilerini aramaları için not alacaklarını belirtmelidir.

Özellikle çalışma saatlerinin dışındaki aramalara cevap veren otomatik sesli mesajlarda VKAM verilmeli ve aramayı yapandan bir mesaj bırakarak aşağıdaki beyanı teyit etmesi istenmelidir:

Sesli mesajınızda bırakacağınız tüm bilgiler ve kişisel veriler [ŞİRKET STANDART OPERASYON PROSEDÜRÜ veya POLİTİKASI] ve yerel düzenlemeler uyarınca korunacak ve gizli tutulacaktır. Vereceğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır [ve talebinizi uygun bir şekilde ele almamızı sağlayacaktır] ve sağlık otoriteleri ile paylaşılabilecektir. Sizinle ilgili tuttuğumuz kişisel verilerinize erişim hakkına sahipsiniz.

e-posta

Gönderen kişiye e-posta aracılığıyla, VKAM içeren bir "Alındı Bildirimi" gönderilmesi gerekir. Şirketler çalışma saatleri dışında, bunun bir otomatik cevap olduğunu belirterek aynı otomatik "Alındı Bildirimi"ni veya VKAM'ını kullanabilirler:

E-postanız tarafımıza ulaşmıştır. E-posta üzerinden bizimle paylaşacağınız tüm bilgiler ve kişisel veriler [ŞİRKET OPERASYON PROSEDÜRÜ veya POLİTİKASI] ve yerel düzenlemeler uyarınca korunacak ve gizli tutulacaktır. Vereceğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır [ve talebinizi uygun bir şekilde ele almamızı sağlayacaktır] ve sağlık otoriteleri ile paylaşılabilecektir. Sizinle ilgili tuttuğumuz kişisel verilerinize erişim hakkına sahipsiniz.

Yüz yüze

Şirketler bir advers olayın ne olduğu ve kendilerine bir advers olay bildirildiğinde ne yapacakları konusunda bilgi sahibi olmaları için tüm çalışanlarını eğitmekle yükümlüdür. Çalışanlar, müşterilerine kişisel verilerinin uygun bir şekilde ele alınacağını garanti etmelidirler:

Bugün bana verdiğiniz tüm bilgiler ve kişisel veriler korunacak ve gizli tutulacaktır. Bana verdiğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır [ve bizim talebinizi uygun bir şekilde ele almamızı sağlayacaktır].

Dijital medya

Advers olayların 'bizimle iletişime geçin' sayfası veya 'Advers olay bildirim linki' üzerinden bildirildiği şirket destekli (kontrollü) dijital faaliyetlerde aşağıdaki gibi bir VKAM olması gereklidir:

Bilgi talebinizle birlikte bizimle paylaştığınız tüm bilgi ve kişisel veriler [ŞİRKET OPERASYON PROSEDÜRÜ veya POLİTİKASI] ve yerel düzenlemeler uyarınca korunacak ve gizli tutulacaktır. Verdiğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır (ve talebinizi uygun bir şekilde ele almamızı sağlayacaktır) ve sağlık otoriteleri ile paylaşılabilecektir. Sizinle ilgili tuttuğumuz kişisel verilerinize erişim hakkına sahipsiniz.

Bu duyuru, web sitesinin ana sayfasında yer alabilir ya da advers olay web sitesi üzerinden iletilmeden önce beliren (pop-up) ileti şeklinde ortaya çıkabilir.

Şirket tarafından desteklenmeyen (kontrol edilmeyen) web siteleri: Şirketler kontrol etmedikleri bir web sitesine VKAM koyamaz. Ancak, şirket tarafından desteklenmeyen bir web sitesinden alınan ve irtibat bilgilerini içeren herhangi bir mesaj e-posta üzerinden iletilmiş gibi ele alınmalıdır.

Şirkete ait olmayan ürünlere ilişkin talepler/bildirimler

Şirketler kendi ürün portföylerinde yer almayan ürünler hakkında bilgi verme yükümlülüğü taşımamaktadır. Çalışanların bu gibi talepleri nasıl ele alacağı şirket kararına bağlıdır. Şirketler, arayanlara ilgili şirketin irtibat bilgilerini sağlama konusunda yardımcı olabilirler.

Farmakovijilans verilerinin takibi
Bildirimde bulunan kişi ile yapılan tüm yazışmalarda bir VKAM gerekecektir. Aşağıdaki duyuru şirkete özel takip talep formlarına veya tamamlanması için bildirimde bulunan kişiye gönderilen advers olay formlarına eklenebilir: ***Bizimle paylaştığınız tüm bilgiler ve kişisel veriler [ŞİRKET STANDART OPERASYON PROSEDÜRÜ ve POLİTİKASI] ve yerel düzenlemeler uyarınca korunacak ve gizli tutulacaktır. Verdiğiniz bilgiler ilaç güvenliliği izlemi amacıyla kullanılacaktır (ve talebinizi uygun bir şekilde ele almamızı sağlayacaktır) ve sağlık otoriteleri ile paylaşılabilecektir. Sizinle ilgili tuttuğumuz kişisel verilerinize erişim hakkına sahipsiniz.***