

**PFİZER PFE İLAÇLARI ANONİM  
ŞİRKETİ**

**Kişisel Verilerin İşlenmesi ve Korunması**

**Politikası**

**Ocak 2019**

## İçindekiler Tablosu

<b>GİRİŞ</b> .....	<b>3</b>
1. GENEL AÇIKLAMA.....	3
2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR .....	4
3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR .....	9
4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SURELERİ .....	13
5. PFİZER TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN SAHİPLERİNE İLİŞKİN KATEGORİZASYON.....	19
6. PFİZER TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI .....	22
7. PFİZER MERKEZ BİNASI, DEPOLARI, OFİSLERİ İLE BU BİNALAR İÇERİSİNDE YAPILAN KİŞİSEL VERİ İŞLEME FAALİYETLERİ İLE İNTERNET SİTESİ VE PFİZER UYGULAMALARI ZİYARETÇİLERİ İLE PFİZER İÇERİSİNDE KULLANILAN UYGULAMALAR.....	23
8. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI 26	
9. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI İLE BU HAKLARIN KULLANILMASI VE PFİZER TARAFINDAN DEĞERLENDİRİLMESİ .....	27
10. PFİZER'İN KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ KONUSUNDA DİĞER İÇ POLİTİKALARI .....	31
11. PFİZER KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI YÖNETİMİ	31
<b>EK 1- KISALTMALAR VE TANIMLAR</b> .....	<b>33</b>

# GİRİŞ

## 1. GENEL AÇIKLAMA

Pfizer PFE İlaçları Anonim Şirketi (“**Pfizer**”) olarak yalnızca Türkiye’de değil, global bir şirket olarak dünya çapında kişisel verilerin korunması konusunda gerekli özeni göstermekte ve bunu bir şirket politikası haline getirerek tüm gerçek ve tüzel kişiler için uygulamaktayız. Bu kapsamda, işbu Kişisel Verilerin İşlenmesi ve Korunması Politikası (“**Politika**”) ile İş birliği İçinde Olduğumuz Kurumların Yetkililerinin ve Çalışanlarının, Tedarikçi Yetkililerinin ve Çalışanlarının, İş Ortakları Yetkililerinin ve Çalışanlarının, Sağlık Mesleği Mensuplarının, Hastaların, Ziyaretçilerimizin, Web Sitesi ve Aplikasyon Kullanıcılarımızın, Çalışan Adaylarımızın ve diğer Üçüncü Kişilerin kişisel verilerinin korunmasını amaçlamaktayız.

İşbu Politika, Pfizer tarafından otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilen, kişisel verileri işlenen gerçek kişilere yönelik olmakla birlikte, Pfizer çalışanlarının kişisel verilerinin korunmasına ilişkin hususlar “Pfizer PFE İlaçları Anonim Şirketi Çalışanları Kişisel Verilerin Korunması ve İşlenmesi Politikası” içerisinde ayrıca düzenlenmektedir.

Pfizer olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“**Kanun**”) uyarınca işlenen kişisel verilerin korunması için gereken idari ve teknik tedbirleri almaktayız.

Kişisel verilerin işlenmesinde **(i)** Kişisel verileri hukuka ve dürüstlük kurallarına uygun işleme, **(ii)** kişisel verileri doğru ve gerektiğinde güncel tutma, **(iii)** Kişisel verileri belirli, açık ve meşru amaçlar için işleme, **(iv)** Kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü işleme, **(v)** Kişisel verileri ilgili mevzuatta öngörülen veya işledikleri amaç için gerekli olan süre kadar muhafaza etme, **(vi)** Kişisel veri sahiplerini aydınlatma ve bilgilendirme, **(vii)** Kişisel veri sahiplerinin haklarını kullanması için gerekli teknik ve idari alt yapıyı oluşturma, **(viii)** Kişisel verilerin muhafazasında gerekli teknik ve idari tedbirleri alma, **(ix)** Kişisel verilerin işleme amacının gereklilikleri doğrultusunda üçüncü kişilere aktarılmasında ilgili mevzuata ve Kurul’un düzenlemelerine uygun davranma, **(x)** Özel nitelikli kişisel verilerin işlenmesine ve korunmasına gerekli hassasiyeti gösterme ilkelerini benimsemekteyiz.

İşbu Politika’da söz konusu temel ilkelere ilişkin detaylı açıklamalarda bulunmaktayız.

### 1.1. Politika’nın Amacı ve Kapsamı

Bu Politika’nın amacı, Pfizer’in hukuka uygun olarak kişisel verileri işlerken uyguladığı ve benimsediği yöntemler ile işlenen verilerin korunması için almış olduğu güvenlik önlem ve tedbirleri konusunda açıklamalarda bulunmak ve bu kapsamda kişisel verileri Pfizer tarafından işlenen kişileri bilgilendirmektir.

Bu kapsamda, işbu Politika, İşbirliği İçinde Olduğumuz Kurumların Yetkililerinin ve Çalışanlarının, Tedarikçi Yetkililerinin ve Çalışanlarının, İş Ortakları Yetkililerinin ve Çalışanlarının, Sağlık Mesleği Mensuplarının, Hastaların, Ziyaretçilerimizin, Web Sitesi ve Aplikasyon Kullanıcılarımızın, Çalışan Adaylarımızın ve diğer Üçüncü Kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla Pfizer tarafından toplanan kişisel verilerinin işlenmesi, saklanması, imha edilmesi, anonimleştirilmesi ve korunmasına ilişkin kamuyu bilgilendirmek amacıyla hazırlanmıştır.

## **1.2. Politika'nın ve İlgili Mevzuatın Uygulanması**

Kişisel verilerin işlenmesi ve korunması konusunda yürürlükte bulunan ilgili kanuni düzenlemeler öncelikli uygulama alanı bulacaktır. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, Pfizer yürürlükteki mevzuatı uygulayacağını kabul etmektedir.

## **1.3. Politika'nın Yürürlüğü**

İşbu Politika, 3 Ocak 2019 tarihinde yürürlüğe girmiş olup, kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

## **2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUSUSLAR**

### **2.1. Kişisel Verilerin Güvenliğinin Sağlanması**

Pfizer, Kanun'un 12. maddesi kapsamında, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilerin muhafazasını sağlamak ve kişisel verilere yetkisiz kişilerce erişiminin engellenmesi amacıyla gerekli olan önlem ve tedbirleri almakta olup, gerekli denetimleri yapmak ve yaptırmaktadır.

Bu kapsamda, Kurul tarafından yayımlanan Kişisel Veri Rehberi'nde (Teknik ve İdari Tedbirler); (i) Yetki Matrisini, (ii) Yetki Kontrolünü, (iii) Erişim Loglarını, (iv) Kullanıcı Hesap Yönetimini, (v) Ağ Güvenliğini, (vi) Uygulama Güvenliğini, (vii) Şifrelemeyi, (viii) Sızma Testini, (ix) Saldırı Tespit ve Önleme Sistemlerini, (x) Log Kayıtlarını, (xi) Veri Maskeleyi, (xii) Veri Kaybı Önleme Yazılımlarını, (xiii) Yedeklemeyi, (xiv) Güvenlik Duvarlarını, (xv) Güncel Anti Virüs Sistemlerini, (xvi) Silme, Yok Etme ve Anonim Hale Getirmeyi, (xvii) Anahtar Yönetimini veri sorumluları tarafından alınabilecek teknik tedbirler olarak açıklamıştır. Aynı şekilde, söz konusu Kişisel Veri Rehberi'nde (Teknik ve İdari Tedbirler) (i) Kişisel Veri Envanteri Hazırlanmasını, (ii) Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha, vb.) hazırlanmasını ve uygulanmasını, (iii) Sözleşmelerin (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu- Veri İşleyen Arasında) Akdedilmesini, (iv) Gizlilik Taahhütnameleri imzalanmasını, (v) Kurum İçi Rastgele veya Periyodik Denetimler

Yapılmasını, (vi) Risk Analizi Yapılmasını, (vii) İş Sözleşmesine ve Disiplin Yönetmeliği'ne Kanun'a Uygun Hükümler İlave Edilmesini, (viii) Kurumsal İletişim Prensiplerinin Kanun'a Uygun Hale Getirilmesini (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi, vb.), (ix) Eğitim ve Farkındalık Faaliyetlerinin Yürütülmesini (Bilgi Güvenliği ve Kanun çerçevesinde) ve (x) Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim Sürecinin Oluşturulmasını alınabilecek idari tedbirler olarak açıklamıştır.

Pfizer, yukarıda açıklanan ve Kurul tarafından yayımlanan Kişisel Veri Rehberi'nde (Teknik ve İdari Tedbirler) ışığında aşağıda sıralanan idari ve teknik önlemleri almıştır:

- Mevcut risk ve tehditler belirlenmekte,
- Pfizer çalışanlarının eğitilmesi ve farkındalık çalışmaları yapılmakta,
- Kişisel veri güvenliği politikaları ve prosedürleri belirlenmekte,
- Pfizer tarafından işlenen kişisel veriler mümkün olduğunca azaltılmakta,
- Veri İşleyenler ile Pfizer arasında Kanun kapsamında Sözleşme akdedilmekte,
- Siber güvenliğin sağlanması için idari ve teknik tedbirler alınmakta (örneğin, kullanılmayan yazılım ve servislerin silinmesi, güvenlik duvarlarının oluşturulması, yama yönetimi ve yazılım güncellemeleri, erişim sınırlamaları, erişim yetki ve kontrol matrisinin oluşturulması, anti virüs ürünlerinin kullanımı, SSL bağlantılar kurulması, vb.)
- Kişisel veri güvenliği takip edilmekte (örneğin log kayıtları tutulmakta, güvenlik sorunlarının bildirilmesi için resmi bir raporlama prosedürü oluşturulmakta, zafiyet taramaları ve sızma testleri yapılmaktadır),
- Kişisel veriler bulut ortamında şifrelenerek saklanmakta ve şifreleme anahtarı kullanılmakta, ve
- Veri yedekleme stratejileri geliştirilmektedir.

### **2.1.1. Kişisel Verilerin Hukuka Uygun İşlenmesini Sağlamak İçin Alınan Teknik Ve İdari Tedbirler**

Pfizer, kişisel verilerin hukuka uygun işlenmesini sağlamak amacıyla gerekli olan ve aşağıda sayılan teknik ve idari tedbirleri teknolojik ve maddi imkanlar doğrultusunda almaktadır. Bu kapsamda;

- Pfizer bünyesinde gerçekleştirilen kişisel veri işleme faaliyetleri kurulan teknik sistemlerle denetlenmekte,
- Alınan teknik önlemler ihtiyaç halinde ilgisine raporlanmakta,
- Teknik konularda bilgili personel istihdam edilmekte,
- Pfizer ile Pfizer Çalışanları arasındaki hukuki ilişkiyi yöneten sözleşme ve belgelere, Kanunla getirilen istisnalar dışında, kişisel verileri işleme, ifşa etmeme ve

kullanmama yükümlülüğü getiren kayıtlar konulmakta ve bu konuda Pfizer Çalışanlarının farkındalığı arttırılmakta,

- Pfizer Çalışanları, periyodik olarak kişisel verilerin korunması hukuku ve kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilgilendirilmekte ve eğitilmekte,
- Düzenli olarak iş süreçleri analiz edilerek veri envanteri çıkarılmakta ve iş birimlerinin yürütmekte olduğu kişisel veri işleme faaliyetleri; bu faaliyetlerin Kanun'a uygunluğunun sağlanması için yerine getirilecek olan gereklilikler her bir süreç özelinde belirlenmekte,
- Hukuksal uyum gerekliliklerinin sağlanması, şirket içerisinde farkındalık yaratılması, uygulamaların sürekliliğinin sağlanması ve düzenli denetimler yapılması için politikalar hayata geçirilmekte ve periyodik olarak Pfizer'in kurumsal sistemlerine erişim hakkı olan kişilere (bunlarla sınırlı kalmaksızın gerekli görülmesi halinde diğer gerçek kişilere) eğitimler verilmekte, ve
- Pfizer ile İş birliği İçinde Olduğumuz Kurumlar, Tedarikçiler, İş Ortakları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız ve diğer Üçüncü Kişiler arasındaki hukuki ilişkiyi yöneten sözleşmeler ve belgelere, kanunla getirilen istisnalar dışında, karşılıklı olarak kişisel verileri işlememe, ifşa etmeme ve kullanmama yükümlülüğü getiren kayıtlar konulmakta ve bu konuda çalışanların farkındalığı sağlanmaktadır.

## **2.1.2. Kişisel Verilerin Hukuka Aykırı Erişimini Engellemek için Alınan Teknik ve İdari Tedbirler**

Pfizer, kişisel verilerin tedbirsizlik sebebiyle veya yetkisiz olarak açıklanmasını, erişimini, aktarılmasını veya başka şekillerdeki tüm hukuka aykırı erişimi önlemek için gerekli olan ve aşağıda sayılan teknik ve idari tedbirleri teknolojik ve maddi imkanları doğrultusunda almaktadır. Buna göre;

- Teknolojideki gelişmelere uygun teknik önlemler alınmakta ve söz konusu önlemler gerektiğinde güncellenmekte ve yenilenmekte,
- Süreç bazında belirlenen hukuksal uyum gerekliliklerine uygun olarak erişim ve yetkilendirmelere ilişkin teknik çözümler devreye alınmakta,
- Erişim yetkileri sınırlandırılmakta, yetkiler düzenli olarak gözden geçirilmekte,
- Alınan teknik önlemler ihtiyaç halinde ilgili kişiye raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmekte,
- Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmakta,
- Teknik konularda bilgili personel istihdam edilmekte,

- Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmakta,
- Pfizer çalışanları, kişisel verilere hukuka aykırı erişimleri engellemek için alınacak teknik tedbirler konusunda eğitilmekte,
- Süreç bazında kişisel veri işlenmesi hukuksal uyum gerekliliklerine uygun olarak şirket içinde kişisel verilere erişim ve yetkilendirme süreçleri tasarlanmakta ve uygulanmakta,
- Pfizer çalışanları, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamayacağı ve işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmasından sonra da devam edeceği konusunda bilgilendirilmekte ve bu doğrultuda kendilerinden gerekli taahhütler alınmakta,
- Pfizer tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.

### **2.1.3. Kişisel Verilerin Güvenli Ortamlarda Saklanması**

Pfizer, kişisel verilerin güvenli ortamlarda saklanması ve hukuka aykırı amaçlarla yok edilmesini, kaybolmasını veya değiştirilmesini önlemek için gerekli olan ve aşağıda sayılan teknik ve idari tedbirleri teknolojik ve maddi imkanları doğrultusunda almaktadır. Buna göre;

- Kişisel verilerin güvenli ortamlarda saklanması için teknolojik gelişmelere uygun sistemler kullanılmakta,
- Teknik konularda uzman personel istihdam edilmekte,
- Saklanma alanlarına yönelik teknik güvenlik sistemleri kurulmakta, alınan teknik önlemler ihtiyaç halinde ilgili kişiye raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmekte,
- Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için hukuka uygun bir biçimde yedekleme programları kullanılmakta,
- Kişisel verilerin bulunduğu veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri ilgililere anlık olarak iletilmekte,
- Pfizer çalışanları, kişisel verilerin güvenli bir biçimde saklanmasını sağlamak konusunda eğitilmekte,
- Pfizer tarafından kişisel verilerin saklanması konusunda teknik gereklilikler sebebiyle dışarıdan bir hizmet alınması durumunda, kişisel verilerin hukuka uygun olarak aktarıldığı ilgili firmalar ile akdedilen sözleşmelere; kişisel verilerin aktarıldığı kişilerin, kişisel verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlanacağına ilişkin hükümlere yer verilmektedir.

#### **2.1.4. Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi**

Pfizer, Kanun'un 12. maddesine uygun olarak, kendi bünyesinde gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları Pfizer'in iç işleyişi kapsamında konu ile ilgili birimine raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

#### **2.1.5. Kişisel Verilerin Yetkisiz Bir Şekilde İfşası Durumunda Alınacak Tedbirler**

Pfizer, Kanun'un 12. maddesine uygun olarak işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede ilgili kişisel veri sahibine, Pfizer Veri Koruma Kurulu'na ve Kurul'a bildirilmesini sağlamaktadır.

#### **2.2. Özel Nitelikli Kişisel Verilerin Korunması**

Kanun bazı kişisel verilerin özel nitelikli olması sebebiyle bu tip verilerin işlenmesi ve korunmasına ilişkin ayrıca birtakım düzenlemeler getirmiştir. Kanun uyarınca, ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli kişisel verilerdir.

İlaç sektöründe faaliyet gösteren global bir şirket olarak, yaptığımız işin mahiyeti gereği özel nitelikli kişisel verilerin hukuka uygun işlenmesinde ve korunmasına ayrıca önem ve özen göstermekteyiz. Bu kapsamda, Pfizer tarafından, kişisel verilerin korunması için teknik ve idari tedbirler alınmakta, periyodik olarak da gerekli denetimler yapılmaktadır.

#### **2.3. Pfizer Çalışanlarının, Şirket Yetkililerimizin, İş Birliği İçinde Olduğumuz Kurumların Yetkililerinin ve Çalışanlarının, Tedarikçi Yetkililerinin ve Çalışanlarının, İş Ortakları Yetkililerinin ve Çalışanlarının, Sağlık Mesleği Mensuplarının ve Diğer Üçüncü Kişilerin Kişisel Verilerin Korunması Ve İşlenmesi Konusunda Farkındalıklarının Arttırılması ve Denetimi**

Pfizer olarak, kişisel verilerin hukuka aykırı olarak işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemeye ve verilerin muhafazasını sağlamaya yönelik farkındalığın artırılması için Pfizer'in emir ve talimatları ile Kanun kapsamında veri işleyen sıfatına haiz kişilere eğitimler düzenlemekte olup, ihtiyaç duyulması halinde kişisel verilerin korunması konusunda bu konuda uzman kişilerle çalışmaktayız. Söz konusu eğitimler periyodik olarak tekrarlanmakta olup, mevzuatın güncellenmesine paralel olarak eğitimlerimizi güncellemekte ve yenilemekteyiz.



### 3. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN HUSUSLAR

#### 3.1. Kişisel Verilerin İşlenmesi

Pfizer, Anayasa'nın 20. maddesi olan Özel Hayatın Gizliliği ve Kanun'un 4. maddesine ve 6. maddesine uygun olarak, kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmaktadır. Pfizer kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği ve/veya sektörel bazda da kabul görmüş süre kadar ve aşağıdaki ilkeler ışığında kişisel verileri muhafaza etmektedir.

- i. Hukuka ve Dürüstlük Kuralına Uygun İşlemek:** Pfizer; kişisel verilerin iş lenmesinde hukuksal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kurallarına uygun hareket etmektedir. Bu kapsamda Pfizer, kişisel verileri, "kişisel verileri işleme amacının" gerektirdiği dışında işlememekte ve kullanmamaktadır.
- ii. Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama: Pfizer;** işlediği kişisel verilerin doğru ve güncel olmasını sağlamak ve bu doğrultuda işbu Politika'da açıklandığı üzere gerekli tedbirleri almaktadır.
- iii. Belirli, Açık ve Meşru Amaçlarla İşleme:** Pfizer, meşru ve hukuka uygun olan kişisel veri işleme amacını açık ve kesin olarak belirlemektedir. Pfizer, yürütmekte olduğu ticari faaliyet ile bağlantılı ve bunlar için gerekli olan kadar kişisel veri işlemektedir. Pfizer tarafından kişisel verilerin hangi amaçla işleneceği henüz kişisel veri işleme faaliyeti başlamadan ortaya konulmaktadır.
- iv. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma:** Pfizer, kişisel verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işlemekte ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınmaktadır.
- v. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Etme:** Pfizer, kişisel verileri ancak ilgili mevzuatta belirtildiği veya sektörel bazda kabul görmüş süre kadar veya işlendikleri amaç için gerekli olan süre kadar ve/veya silme politikalarında belirlediği süreler içerisinde muhafaza etmektedir. Bu kapsamda, Pfizer öncelikle ilgili mevzuatta kişisel verilerin saklanması için bir süre öngörülüp öngörülmediğini tespit etmekte, bir süre belirlenmişse bu süreye uygun davranmakta, bir süre belirlenmemişse kişisel verileri iş lendikleri amaç için gerekli olan ve/veya sektörel bazda kabul görmüş süre kadar ve/veya Pfizer tarafından belirlenen süreler kadar saklamaktadır. Sürenin bitimi veya işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler Pfizer tarafından silinmekte, yok edilmekte veya anonim hale getirilmektedir. Gelecekte kullanma ihtimali ile Pfizer tarafından kişisel veriler ancak meşru menfaat hallerinin varlığı halinde saklanmaktadır.

Kişisel verilerin korunması Anayasal bir haktır. Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Anayasa'nın 20. maddesinin üçüncü fıkrası gereğince, kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilecektir. Pfizer, hem Anayasa'nın 20. maddesinin üçüncü fıkrası hem de Kanun'un 5. maddesi uyarınca, ilgili Kanun maddesinde sayılan şartlardan bir veya birkaçına dayalı olarak işlemekte olup, kişisel verileri, ancak Kanunda öngörülen hallerde veya kişinin açık rızasıyla işlemektedir. Ayrıca Pfizer, Kanun'un 8. ve 9. maddelerine uygun olarak, kişisel verileri Kanun'da öngörülen ve Kurul tarafından yayınlanan düzenlemelere uygun olarak aktarmaktadır.

Pfizer, Kanun'un 10.maddesine uygun olarak, kişisel veri sahiplerini, işlenen kişisel verilerine ilişkin aydınlatmak ve kişisel veri sahiplerinin bilgi talep etmeleri durumunda gerekli bilgilendirmeyi yapmaktadır. Bu kapsamda Pfizer, varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılacağı, kişisel veri toplamının yöntemi ve hukuki sebebi ile kişisel veri sahibinin sahip olduğu hakları konusunda aydınlatma yapmaktadır.

Anayasa'nın 20. maddesinde herkesin, kendisiyle ilgili kişisel veriler hakkında bilgilendirilme hakkına sahip olduğu ortaya konulmuştur. Bu doğrultuda Kanun'un 11. maddesinde kişisel veri sahibinin hakları arasında "bilgi talep etme" de sayılmıştır. Pfizer, bu kapsamda, Anayasa'nın 20. ve Kanun'un 11. maddelerine uygun olarak Kişisel Veri Sahibi'nin bilgi talep etmesi durumunda gerekli bilgilendirmeyi yapmaktadır.

### **3.2. Özel Nitelikli Kişisel Verilerin İşlenmesi**

İlaç sektöründe faaliyet gösteren global bir şirket olarak, yaptığımız işin mahiyeti gereği özel nitelikli kişisel verilerin hukuka uygun işlenmesinde Anayasa'da ve Kanunu'nda öngörülen düzenlemelere hassasiyet gösterilmekte ve uygun davranılmaktadır.

Kanun'un 6. maddesinde, hukuka aykırı olarak işlendiğinde kişilerin mağduriyetine veya ayrımcılığa sebep olma riski taşıyan bir takım kişisel veri "özel nitelikli" olarak belirlenmiştir. Bu veriler; ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, ~~kl~~ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Özel nitelikli kişisel veriler, Pfizer tarafından Kanun'a uygun Kurul tarafından yayımlanan Kişisel Veri Güvenliği Rehberi (İdari ve Teknik) ile 3.01.2018 karar tarihli 2018/10 sayılı Kurul kararı uyarınca 13.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler"de belirlenen önlemlerin alınması kaydıyla aşağıdaki durumlarda işlenmektedir:

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
  - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,
  - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 işlenmektedir.

### **3.3. Kişisel Verilerin Aktarılması**

Pfizer hukuka uygun olan kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemlerini alarak kişisel veri sahibinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere aktarabilmektedir. Pfizer, bu doğrultuda Kanun'un 8. maddesinde öngörülen düzenlemelere uygun hareket etmektedir.

Pfizer meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda aşağıda sayılan ve Kanun'un 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak kişisel verileri üçüncü kişilere aktarabilmektedir:

- Kişisel veri sahibinin açık rızası var ise,
- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa;
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,
- Pfizer'in hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Kişisel veriler, kişisel veri sahibi tarafından alenileştirilmiş ise,
- Kişisel veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Pfizer'in meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

#### **3.3.1. Özel Nitelikli Kişisel Verilerin Aktarılması**

Pfizer gerekli özeni göstererek, gerekli güvenlik tedbirlerini alarak ve Kurul tarafından yayınlanan yeterli önlemleri alarak; meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin özel nitelikli kişisel verilerini aşağıdaki durumlarda üçüncü kişilere aktarabilmektedir.

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
  - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir), kanunlarda öngörülen hallerde,
  - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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.

### 3.4. Kişisel Verilerin Yurtdışına Aktarılması

Pfizer hukuka uygun kişisel veri işleme amaçları doğrultusunda gerekli güvenlik önlemleri alarak kişisel veri sahibinin kişisel verilerini ve özel nitelikli kişisel verilerini üçüncü kişilere aktarabilmektedir.

Pfizer; Kurul tarafından yeterli korumaya sahip olduğu ilan edilen<sup>1</sup> yabancı ülkelere (“Yeterli Korumaya Sahip Yabancı Ülke”) veya yeterli korumanın bulunmaması durumunda, Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ettiği ve Kurul izninin bulunduğu yabancı ülkelere (“Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülke”) kişisel veriler aktarılabilir. Pfizer bu doğrultuda Kanun’un 9. maddesinde öngörülen düzenlemelere uygun hareket etmektedir.

Pfizer meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin açık rızası var ise veya kişisel veri sahibinin açık rızası yok ise aşağıdaki hallerden birinin varlığı durumunda kişisel verileri Yeterli Korumaya Sahip veya Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülkelere aktarabilmektedir:

- Kişisel veri sahibinin açık rızası var ise,
- Kanunlarda kişisel verinin aktarılacağına ilişkin açık bir düzenleme var ise,
- Kişisel veri sahibinin veya başkasının hayatı veya beden bütünlüğünün korunması için zorunlu ise ve kişisel veri sahibi fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda ise veya rızasına hukuki geçerlilik tanınmıyorsa,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla sözleşmenin taraflarına ait kişisel verinin aktarılması gerekli ise,

---

<sup>1</sup> Kişisel Verileri Koruma Kurulu tarafından “Yeterli Korumaya Sahip Yabancı Ülke” listesi halihazırda ilan edilmemiştir.

- Pfizer'in hukuki yükümlülüğünü yerine getirmesi için kişisel veri aktarımı zorunlu ise,
- Kişisel veriler, kişisel veri sahibi tarafından alenileştirilmiş ise,
- Kişisel veri aktarımı bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Kişisel veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Pfizer'in meşru menfaatleri için kişisel veri aktarımı zorunlu ise.

#### 3.4.1. Özel Nitelikli Kişisel Verilerin Yurtdışına Aktarılması

Pfizer meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda kişisel veri sahibinin açık rızası var ise veya kişisel veri sahibinin açık rızası yok ise aşağıdaki hallerden birinin varlığı durumunda özel nitelikli kişisel verileri Yeterli Korumaya Sahip veya Yeterli Korumayı Taahhüt Eden Veri Sorumlusunun Bulunduğu Yabancı Ülkelere aktarabilmektedir:

- Kişisel veri sahibinin açık rızası var ise veya
- Kişisel veri sahibinin açık rızası yok ise;
  - Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel verileri (ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir), kanunlarda öngörülen hallerde,
  - Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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.

## 4. ŞİRKETİMİZ TARAFINDAN İŞLENEN KİŞİSEL VERİLERİN KATEGORİZASYONU, İŞLENME AMAÇLARI VE SAKLANMA SÜRELERİ

### 4.1. Kişisel Verilerin Kategorizasyonu

Pfizer nezdinde; Pfizer'in meşru ve hukuka uygun kişisel veri işleme amaçları doğrultusunda, Kanun'un 5. maddesinde belirtilen kişisel veri işleme şartlarından bir veya birkaçına dayalı ve sınırlı olarak, başta kişisel verilerin işlenmesine ilişkin 4. maddede belirtilen ilkeler olmak üzere Kanun'da belirtilen genel ilkelere ve Kanun'da düzenlenen bütün yükümlülöklere uyularak ve işbu Politika kapsamındaki sùjelerle (İşbirliğı İçinde Olduğumuz Kurumların Yetkilileri ve Çalıřanları, Tedarikçi Yetkilileri ve Çalıřanları, İş Ortakları Yetkilileri ve Çalıřanları, Sağlık Mesleğı Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalıřan Adayları ve diğeri üçüncü Kişilerin) sınırlı olarak aşağıda belirtilen kategorilerdeki kişisel veriler, Kanun'un 10. maddesi uyarınca ilgili kişiler bilgilendirilmek suretiyle

işlenmektedir. Bu kategorilerde işlenen kişisel verilerin işbu Politika kapsamında düzenlenen hangi veri sahipleriyle ilişkili olduğu da işbu Politika'nın 5. Maddesinde belirtilmektedir.

<b>Kişisel Veri veya Özel Nitelikli Kişisel Veri</b>	<b>Açıklama</b>
<b>Kimlik Bilgisi</b>	Ad-soyad, T.C. kimlik numarası, uyruk bilgisi, anne adı-soyadı, baba adı-soyadı, doğum yeri, doğum tarihi, cinsiyet gibi bilgileri içeren ehliyet, nüfus cüzdanı ve pasaport gibi belgeler ile bu bilgilerin yer aldığı diğer dokümanlar, vergi numarası, SGK numarası, imza bilgisi, taşıt plakası, vb.
<b>İletişim Bilgisi</b>	Telefon numarası, adres, elektronik posta (e-mail) adresi, faks numarası, IP adresi, vb.
<b>Özel Nitelikli Kişisel Veri</b>	Reçete bilgisi, doktor raporu, tahlil ve radyoloji sonuçları, sağlık raporu, kan grubu, genetik verisi, vb. gib her türlü sağlık verisi ile din, üye olunan dernek verisi, vb.
<b>Fiziksel Mekân Güvenlik Bilgisi</b>	Pfizer'e ait veya kiracısı olduğu (Pfizer Merkez Binası ve/veya Pfizer Ofisleri) fiziksel mekânın içerisinde kalış sırasında alınan kayıtlar ve belgelere ilişkin kişisel veriler ( kamera kayıtları, güvenlik noktasında alınan kayıtlar, vb.)
<b>Finansal Bilgi</b>	Tedarikçiler, İş Ortakları, SMM'ler ve diğer 3. Kişilerle veya diğer kişisel veri sahipleri ile kurmuş olduğu hukuki ilişkinin tipine göre yaratılan her türlü finansal sonucu gösteren bilgi, belge ve kayıtlara ilişkin işlenen kişisel veriler ile

	banka hesap numarası IBAN numarası kredi kartı bilgisi, finansal profil, malvarlığı verisi, gelir bilgisi verileri vb.
<b>Görsel/İşitsel Bilgi</b>	Her türlü fotoğraf ve kamera kayıtları, ses kayıtları
<b>Özlük Bilgileri</b>	Pfizer ile çalışma ilişkisi olan veya olacak olan (Çalışan Adayları da dahil) gerçek kişilerin özlük haklarının oluşmasına temel olacak bilgiler (özgeçmiş, sağlık raporu, banka hesap, SGK dökümü, vesikalık fotoğraf, ikametgâh sureti, nüfus cüzdanı sureti, vb.)
<b>Talep/Şikâyet Yönetimi Bilgisi</b>	Ürün Güvenliği, Kalite, Medikal Enformasyon, vb. işlemlerin icrası esnasında alınan her türlü kişisel veri ile Pfizer'e yöneltilmiş olan her türlü talep veya şikâyetin alınması ve değerlendirilmesine ilişkin veriler.
<b>İşlem Güvenliği Bilgisi</b>	Pfizer'in ticari faaliyetlerini yürütürken gerek veri sahibinin gerekse de şirket'in teknik, idari, hukuki ve ticari güvenliğinin sağlanması için işlenen kişisel veriler.
<b>Risk Yönetim Bilgisi</b>	Ticari, teknik ve idari risklerin yönetilmesi için bu alanlarda genel kabul görmüş hukuki, ticari teamül ve dürüstlük kuralına uygun olarak kullanılan yöntemler vasıtasıyla işlenen kişisel veriler.
<b>Hukuki İşlem Uyum Bilgisi</b>	Pfizer'in hukuki alacak ve haklarının tespiti, tespiti, takibi ve borçlarının ifası ile kanuni yükümlülüklerin ve Pfizer politikalarına uyum kapsamında işlenen

	kişisel veriler.
<b>Denetim ve Teftiş Bilgisi</b>	Pfizer'in kanuni yükümlülükleri ve şirket politikalarına uyumu kapsamında işlenen kişisel veriler
<b>İtibar Yönetimi Bilgisi</b>	Kişiyle ilişkilendirilen ve Pfizer'in ticari itibarını korumak maksatlı toplanan kişisel veriler.

#### 4.2. Kişisel Verilerin İşlenme Amaçları

Pfizer, Kanun'un 5. maddesinin 2. fıkrasında ve 6. maddenin 3. fıkrasında belirtilen kişisel veri işleme şartları içerisindeki amaçlarla ve koşullarla sınırlı olarak kişisel verileri işlemektedir. Bu amaçlar ve koşullar;

- Kişisel verilerinizin işlenmesine ilişkin Pfizer'in ilgili faaliyette bulunmasının Kanunlarda açıkça öngörülmesi,
- Kişisel verilerinizin Pfizer tarafından işlenmesinin bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili ve gerekli olması,
- Kişisel verilerinizin işlenmesinin Pfizer'in hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- Kişisel verilerinizin sizler tarafından ahenileştirilmiş olması şartıyla; sizin ahenileştirme amacıyla sınırlı bir şekilde Pfizer tarafından işlenmesi,
- Kişisel verilerinizin Pfizer tarafından işlenmesinin Pfizer'in veya sizlerin veya üçüncü kişilerin haklarının tesisi, kullanılması veya korunması için zorunlu olması,
- Sizlerin temel hak ve özgürlüklerinize zarar vermemek kaydıyla Pfizer'in meşru menfaatleri için kişisel veri işleme faaliyetinde bulunulmasının zorunlu olması,
- Pfizer tarafından kişisel veri işleme faaliyetinde bulunulmasının kişisel veri sahibinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması ve bu durumda da kişisel veri sahibinin fiili veya hukuki geçersizlik nedeniyle rızasını açıklayamayacak durumda bulunması,
- Kişisel veri sahibinin sağlığı ve cinsel hayatı dışındaki özel nitelikli kişisel veriler açısından kanunlarda öngörülmüş olması,
- Kişisel veri sahibinin sağlığına ve cinsel hayatına ilişkin özel nitelikli kişisel verileri açısından ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi 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 islenmesidir.

Bu kapsamda Pfizer, kişisel verilerinizi aşağıdaki amaçlarla işlemektedir:

- Şirket iç operasyonlarının, iş faaliyetlerinin yürütülmesi ve şirket operasyonlarının güvenliğinin temin edilmesi, iş faaliyetlerinin etkinlik, verimlilik, yerindelik analizlerinin gerçekleştirilmesi için gerekli faaliyetlerinin yürütülmesi,
- Personel işe alım süreçlerinin yürütülmesi,
- Strateji planlama faaliyetlerinin ve İş Ortakları veya Tedarikçilerle olan ilişkilerin yönetimi ve icrası,
- Pazarlama ve satış faaliyetlerinin yürütülmesi, şirket'in sunduğu ürün ve/veya hizmetlere bağlılık oluşturulması ve/veya artırılması süreçlerinin yürütülmesi, ürün ve hizmetlerin satış ve pazarlaması için pazar araştırması faaliyetlerinin yürütülmesi,
- Üretim ve/veya operasyon süreçlerinin yürütülmesi,
- Ürün Güvenliği'nin, Medikal Enformasyonun ve Yan Etki Bildirimlerinin yönetimi ve icrası,
- İş sürekliliğinin sağlanması ve kurumsal yönetim faaliyetler için gereken süreçlerin işletilmesi,
- Kongre faaliyetlerinin planlanması, yürütülmesi ve icrası,
- Klinik Araştırma faaliyetlerinin yürütülmesi ve icrası,
- Hastalar, İş birliği İçinde Olduğumuz Kurumlar ve SMM'ler ile olan ilişkilerin yönetimi ve icrası,
- Pfizer ruhsatlandırma işlemlerinin yönetimi ve icrası,
- Pfizer kalite yönetimi ve icrası,
- Kurumsal sürdürülebilirlik faaliyetlerinin planlanması ve icrası,
- Etkinlik yönetimi,
- Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi,
- Satın alma faaliyetlerinin planlanması, değerlendirilmesi ve takibi,
- Pfizer hukuk işlerinin icrası/takibi,
- Hukuksal, teknik ve idari sonucu olan faaliyetlerin yürütülmesi ve yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi, hukuksal taleplere ilişkin faaliyetler ile hukuki işlerin yürütülmesi,
- Verilerin doğru ve güncel tutulması,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Kurumsal yönetim faaliyetlerinin icrası,
- Talep ve şikâyet yönetimi,
- Mevzuata uyum,

- Yetkili kuruluřlara mevzuattan kaynaklı bilgi verilmesi,
- Ziyaretçi kayıtlarının oluřturulması ve takibi,
- Őirket yerleřkeleri ve/veya tesislerinin g¼venlięinin teminin edilmesi,
- Lojistik faaliyetlerin planlanması ve icrası,
- Bilgi g¼venlięi s¼reçleri ile bilgi teknoloji alt yapısına iliřkin faaliyetlerin y¼r¼t¼lmesi,
- Acil durum y¼netimi s¼reçlerinin planlanması ve icrası, iř saęlıęı ve/veya g¼venlięi s¼reçlerinin y¼r¼t¼lmesi,
- Grup Őirketlerine iliřkin faaliyetlerin y¼r¼t¼lmesi, çalıřanların bilgiye eriřimlerinin saęlanması,
- Sosyal medya hesaplarının ve web sitelerinin y¼netilmesi.

İřbu Politika kapsamında kiřisel verileri iř lenen kiřilerin kiřisel verileri yazılı veya elektronik ortamda elektronik posta (e-posta), kısa mesaj (sms), Pfizer Web Siteleri ve Aplikasyonları ve dięer mobil uygulamalar, çevrimiçi veya fiziki bařvuru formu, iletiřim formu, vb. formlar, santral ve telesekreter hizmetleri, Őikâyet y¼netim sistemleri, sosyal medya mecraları, ses kaydı, video kaydı, vb. y¼ntemlerle önceden belirlenen ve iřbu Politika'da açıklanan amaçlar kapsamında toplanmaktadır.

Bahsi geçen amaçlarla gerçeleřtirilen iřleme faaliyetinin, Kanun kapsamında öngör¼len Őartlardan herhangi birini karřılamıyor olması halinde, ilgili iřleme s¼recine iliřkin olarak Pfizer tarafından açık rızanız temin edilmektedir.

Bunun yanı sıra Pfizer'in en çok kiřisel veri topladıęı veri sahibi kategorisi olan Çalıřan Aday'larının iře alım s¼recinde Pfizer tarafından toplanan kiřisel verileri ile iř in nitelięine göre toplanan özel nitelikli kiřisel veriler ařaęıda açıklanan amaçlar kapsamında iřlemektedir:

- Çalıřan Adayının nitelięini, tecr¼besini ve ilgisini açık pozisyona uygunluęunu deęerlendirmek,
- Üç¼nc¼ kiřiler ile iletiřime geçerek Çalıřan Adayı hakkında arařtırma yapmak,
- Bařvuru ve iře alım s¼reci hakkında Çalıřan Adayı ile iletiřime geçmek,
- Sonradan pozisyon açılması durumunda Çalıřan Adayı ile iletiřime geçmek,
- İlgili mevzuatın gereklerini ve/veya yetkili kurum ve kuruluřların taleplerini karřılamak,

Bu kapsamda, Çalıřan Adaylarının (i) yazılı veya elektronik ortamda yayımlanan dijital bařvuru formu, (ii) Pfizer'e e-posta, kargo, referans vb. yollarla ulařtırdıkları özgeçmiřler ve (iii) istihdam ve/veya danıřmanlık Őirketleri, çevrimiçi iře alım platformları aracılıęı, (iv) video konferans veya yüz y¼ze yapılan m¼lakatlar sırasında, (v) tecr¼besi olan uzman kiřiler tarafından yapılan ve sonuçları incelenen yetenek ve kiřilik özelliklerini tespit eden iře alım

testleri aracılığı ile, (vi) işe alım sürecinde, (vii) işe alım sonrası önceden belirlenen bir amaç kapsamında toplanmaktadır.

Çalışan Adayları diledikleri takdirde Veri Sahibi olmalarından kaynaklanan ve Kanun'dan doğan hakları ile ilgili taleplerini işbu Politika'nın 9. maddesinde açıklanan yöntem ile iletebilirler.

#### **4.3. Kişisel Verilerin Saklanma Süreleri**

Pfizer, ilgili kanunlarda ve mevzuatlarda öngörülmesi durumunda kişisel verileri bu mevzuatlarda belirtilen süre boyunca saklamaktadır.

Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin mevzuatta bir süre düzenlenmemişse, kişisel veriler Pfizer'in o veriyi işlerken yürütülen faaliyet ile bağlı olarak Pfizer'in uygulamaları ve ticari yaşamının teamülleri uyarınca işlenmesini gerektiren süre kadar işlenmekte daha sonra silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Kişisel verilerin işlenme amacı sona ermiş, ilgili mevzuat ve Pfizer'in belirlediği saklama sürelerinin de sonuna gelmişse; kişisel veriler yalnızca olası hukuki uyumsuzluklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zaman aşımı süreleri ile zaman aşımı sürelerinin geçmesine rağmen daha önce aynı konularda Pfizer'e yöneltilen taleplerdeki örnekler esas alınarak saklama süreleri belirlenmektedir. Bu durumda saklanan kişisel verilere herhangi bir başka amaçla erişilmemekte ve ancak ilgili hukuki uyumsuzlukta kullanılması gerektiği zaman ilgili kişisel verilere erişim sağlanmaktadır. Burada da bahsi geçen süre sona erdikten sonra kişisel veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

#### **5. PFİZER TARAFI NDAN İŞLENEN KİŞİSEL VERİLERİN SAHIPLERİ NE İLİŞKİN KATEGORİZASYON**

Pfizer tarafından, aşağıda sıralanan kişisel veri sahibi kategorilerinin kişisel verileri işlenmekle birlikte, işbu Politika'nın uygulama kapsamı İş Birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişileri ile sınırlıdır.

Pfizer tarafından kişisel verileri işlenen kişiler in kategorileri yukarıda belirtilen kapsamda olmakla birlikte, bu kategorilerin dışında yer alan kişiler de Kanun kapsamında Pfizer'e taleplerini yöneltebilecek olup; bu kişilerin talepleri de bu Politika kapsamında değerlendirmeye alınacaktır.

Aşağıdaki tabloda İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişileri olarak tanımladığımız kişisel veri sahibi kategorileri ile bu kategoriler içerisindeki kişilerin hangi tip kişisel verilerinin işlendiği detaylandırılmaktadır.

<b>Kişisel Veri Kategorizasyonu</b>	<b>Kişisel Veri Sahibi Kategorizasyonu</b>
<b>Kimlik Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişileri
<b>İletişim Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişileri
<b>Özel Nitelikli Kişisel veri</b>	Hastalar, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>Aile Bireyleri ve Yakın Bilgisi</b>	Hastalar, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>Fiziksel Mekân Güvenlik Bilgisi</b>	Ziyaretçilerimiz
<b>Finansal Bilgi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları

	Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları ve diğer Üçüncü Kişileri
<b>Görsel/İşitsel Bilgi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Çalışan Adayları ve diğer Üçüncü Kişileri
<b>Özlük Bilgileri</b>	Pfizer Çalışanları, Eski Pfizer Çalışanları, diğer Üçüncü Kişiler
<b>Talep/Şikâyet Yönetimi Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>İşlem Güvenliği Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>Risk Yönetim Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler

<b>Hukuki İşlem Uyum Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>Denetim ve Teftiş Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler
<b>İtibar Yönetimi Bilgisi</b>	İş birliği İçinde Olduğumuz Kurumların Yetkilileri ve Çalışanları, Tedarikçi Yetkilileri ve Çalışanları, İş Ortakları Yetkilileri ve Çalışanları, Sağlık Mesleği Mensupları, Hastalar, Ziyaretçilerimiz, Web Sitesi ve Aplikasyon Kullanıcılarımız, Çalışan Adayları ve diğer Üçüncü Kişiler

## **6. PFİZER TARAFINDAN KİŞİSEL VERİLERİN AKTARILDIĞI ÜÇÜNCÜ KİŞİLER VE AKTARILMA AMAÇLARI**

Pfizer Kanun'un 8. ve 9. maddelerine uygun olarak Politika ile yönetilen veri sahiplerinin kişisel verilerini aşağıda sıralanan kişi kategorilerine aktarılabilir:

- i.** Pfizer İş Ortaklarına (doktorlar, eczacılar, hastalar da dahil olmak üzere),
- ii.** Pfizer Tedarikçilerine,
- iii.** Pfizer global şirketlerine ve iştiraklerine (Pfizer Inc. başta olmak üzere Pfizer PFE İlaçları A.Ş. vb.),
- iv.** Pfizer şirket yetkililerine,

- v. Hukuken Yetkili kamu kurum ve kuruluşlarına (Örneğin Sağlık Bakanlığı, Gümrük Müdürlüğü, Mahkemeler, vb.)
- vi. Hukuken yetkili özel hukuk kişilerine,
- vii. Yetkili Pfizer çalışanlarına.

Aktarımda bulunulan yukarıda belirtilen kişilerin kapsamı ve veri aktarım amaçları aşağıda belirtilmektedir.

Pfizer, Kanun'un 10. maddesine uygun olarak kişisel verilerin aktarıldığı kişi gruplarını kişisel veri sahibine bildirmektedir.

## **7. PFİZER MERKEZ BİNASI, DEPOLARI, OFİSLERİ İLE BU BİNALAR İÇERİSİNDE YAPILAN KİŞİSEL VERİ İŞLEME FAALİYETLERİ İLE İNTERNET SİTESİ VE PFİZER UYGULAMALARI ZİYARETÇİLERİ İLE PFİZER İÇERİSİNDE KULLANILAN UYGULAMALAR**

### **7.1 Pfizer Merkez Binası, Depoları, Ofislerinde Yapılan Kişisel Veri İşleme Faaliyetleri**

Pfizer tarafından güvenliğin sağlanması amacıyla, Pfizer Merkez Binasında, depolarında ve ofislerinde ("Binalar") güvenlik kamerasıyla izleme faaliyeti ile misafir giriş-çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunmaktadır.

Güvenlik kameraları kullanılması ve misafir giriş-çıkışlarının kayıt altına alınması yoluyla Pfizer tarafından kişisel veri işleme faaliyeti yürütülmektedir.

Pfizer, Binaların girişlerinde ve içerisinde kamera izleme faaliyeti yürütmekte olup, Şirketin ve diğer kişilerin (Pfizer çalışanları, ziyaretçiler vb.) güvenliğini sağlamaya ilişkin menfaatlerini korumayı amaçlamaktadır. Bu kapsamda, Pfizer, Kanun'a ve diğer ilgili mevzuata uygun hareket etmektedir. Şöyle ki, kamera ile izleme faaliyeti, Özel Güvenlik Hizmetlerine Dair Kanun ve ilgili mevzuata uygun olup, Pfizer tarafından güvenlik amacıyla kamera ile izleme faaliyeti yürütülmesinde Kanun'da yer alan düzenlemelere uygun hareket edilmektedir. Buna göre; Kanun'un 10. maddesi çerçevesinde, kişisel veri sahibi aydınlatılmaktadır. Aydınlatma yükümlülüğünün bir parçası olarak, Pfizer hem Bina girişlerine aydınlatma metni asmakta hem de internet sitesinde işbu Politika'yı yayımlamaktadır. Ayrıca, izlemenin yapıldığı alanlara da buna ilişkin uyarı tabelaları asılmaktadır.

Pfizer, Kanun'un 4. maddesi uyarınca, kişisel verileri işlendikleri amaçlarla bağlantılı, sınırlı ve ölçülü bir biçimde işlemekte olup, video kamera ile izleme faaliyetini de amacı kapsamında sürdürmektedir. Bu doğrultuda, Pfizer güvenlik kameralarının izleme alanlarını, sayısını ve

video kayıtlarının saklanma sürelerini güvenlik amacını aşmadan sınırlı olarak belirlemektedir. Ayrıca belirtmek gerekir ki, kişinin mahremiyetine müdahale edilmeyecek şekilde video kayıt faaliyeti sürdürülmektedir.

Pfizer tarafından video kayıt yoluyla yürütülen izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için de gerekli teknik ve idari tedbirler Pfizer tarafından alınmaktadır. Bu kapsamda, ilgili video kayıtlarına sınırlı sayıda Pfizer çalışanını erişimi bulunmaktadır.

Ayrıca, Pfizer tarafından; güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla, Pfizer Binalarında misafir giriş-çıkışlarının takibine yönelik kişisel veri işleme faaliyetinde bulunmaktadır. Şöyle ki, Ziyaretçi olarak Pfizer Binalarına gelen kişilerin isim, soyadları ve T.C. Kimlik Numaraları işlenmekte olup, kişisel veri sahibi olan ziyaretçiler bu kapsamda girişlere asılmış aydınlatma metinleri ile bilgilendirilmektedirler. Ziyaretçi giriş-çıkış takibi yapılması amacıyla elde edilen veriler yalnızca bu amaçla işlenmekte ve ilgili kişisel veriler fiziki ortamda veri kayıt sistemine kaydedilmektedir.

## **7.2 İnternet Sitesi ve Pfizer Mobil Uygulamaları Ziyaretçileri**

Pfizer sahibi olduğu internet sitelerinde ve mobil uygulamalarında (aplikasyonlar); bu siteleri ve uygulamaları ziyaret eden kişilerin ziyaretlerini, ziyaret amaçlarıyla uygun olarak gerçekleştirmeleri ve kendilerine özelleştirilmiş içerikler gösterebilmek, çevrimiçi reklamcılık faaliyetlerinde bulunabilmek amacıyla (Kurabiyeler (cookie), vb.) site ve/veya uygulama içerisindeki internet hareketleri teknik yöntemlerle kaydedilmektedir. Pfizer internet sitesi ve uygulamaları içerisinde yürütmekte olduğu bu faaliyetlerine ve kişisel verilerin korunması ve işlenmesine ilişkin detaylı açıklamaları ilgili internet sitelerinin ve uygulamalarının "Gizlilik Politikası" başlıklı metinleri içerisinde açıklamaktadır.

Pfizer faaliyetlerini yürütebilmek amacıyla çeşitli sistemler kullanmaktadır. Bu sistemlere Pfizer çalışanları tarafından aşağıda sayılan amaçlar kapsamında yürütmekte oldukları işin amacına ve görev tanımlarına uygun olarak kişisel veri işleyebilmektedirler:

- Şirket iç operasyonlarının, iş faaliyetlerinin yürütülmesi ve şirket operasyonlarının güvenliğinin temin edilmesi, iş faaliyetlerinin etkinlik, verimlilik, yerindelik analizlerinin gerçekleştirilmesi için gerekli faaliyetlerinin yürütülmesi,
- Personel işe alım süreçlerinin yürütülmesi,
- Strateji planlama faaliyetlerinin ve İş Ortakları veya Tedarikçilerle olan ilişkilerin yönetimi ve icrası,



- Pazarlama ve satış faaliyetlerinin yürütülmesi, şirket'in sunduğu ürün ve/veya hizmetlere bağlılık oluşturulması ve/veya artırılması süreçlerinin yürütülmesi, ürün ve hizmetlerin satış ve pazarlaması için pazar araştırması faaliyetlerinin yürütülmesi,
- Üretim ve/veya operasyon süreçlerinin yürütülmesi,
- Ürün Güvenliği'nin, Medikal Enformasyonun ve Yan Etki Bildirimlerinin yönetimi ve icrası,
- İş sürekliliğinin sağlanması ve kurumsal yönetim faaliyetler için gereken süreçlerin işletilmesi,
- Kongre faaliyetlerinin planlanması, yürütülmesi ve icrası,
- Klinik Araştırma faaliyetlerinin yürütülmesi ve icrası,
- Hastalar, İş birliği İçinde Olduğumuz Kurumlar ve SMM'ler ile olan ilişkilerin yönetimi ve icrası,
- Pfizer ruhsatlandırma işlemlerinin yönetimi ve icrası,
- Pfizer kalite yönetimi ve icrası,
- Kurumsal sürdürülebilirlik faaliyetlerinin planlanması ve icrası,
- Etkinlik yönetimi,
- Finansal raporlama ve risk yönetimi işlemlerinin icrası/takibi,
- Satın alma faaliyetlerinin planlanması, değerlendirilmesi ve takibi,
- Pfizer hukuk işlerinin icrası/takibi,
- Hukuksal, teknik ve idari sonucu olan faaliyetlerin yürütülmesi ve yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi, hukuksal taleplere ilişkin faaliyetler ile hukuki işlerin yürütülmesi,
- Verilerin doğru ve güncel tutulması,
- Kurumsal iletişim faaliyetlerinin planlanması ve icrası,
- Kurumsal yönetim faaliyetlerinin icrası,
- Talep ve şikâyet yönetimi,
- Mevzuata uyum,
- Yetkili kuruluşlara mevzuattan kaynaklı bilgi verilmesi,
- Ziyaretçi kayıtlarının oluşturulması ve takibi,
- Şirket yerleşkeleri ve/veya tesislerinin güvenliğinin teminin edilmesi,
- Lojistik faaliyetlerin planlanması ve icrası,
- Bilgi güvenliği süreçleri ile bilgi teknoloji alt yapısına ilişkin faaliyetlerin yürütülmesi,
- Acil durum yönetimi süreçlerinin planlanması ve icrası, iş sağlığı ve/veya güvenliği süreçlerinin yürütülmesi,
- Grup şirketlerine ilişkin faaliyetlerin yürütülmesi, çalışanların bilgiye erişimlerinin sağlanması,
- Sosyal medya hesaplarının ve web sitelerinin yönetilmesi.

## 8. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ ŞARTLARI

Türk Ceza Kanunu'nun 138. maddesinde ve Kanun'un 7. Maddesi uyarınca ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Pfizer'in kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir. Bu kapsamda Pfizer aşağıdaki yöntemler ve teknikler ile kişisel verileri silmekte, yok etmekte veya anonim hale getirmektedir.

### 8.1. Kişisel Verilerin Silinmesi ve Yok Edilmesi

- i. **Fiziksel Olarak Yok Etme:** Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Örneğin, çıktısı alınmış bir özgeçmişin yırtmak veya imha makinesinden geçirmek suretiyle imha edilmesi fiziksel olarak yok etmektir.
- ii. **Yazılımdan Güvenli Olarak Silme:** Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır. Dijital olarak silinmesi/yok edilmesi teknik olarak mümkün olmayan durumlarda Pfizer bu verileri kanunun öngördüğü şekilde erişim yetkilerini kısıtlayarak kullanımını önlemektedir. Ayrıca, Pfizer bazı durumlarda kendisi adına kişisel verileri silmesi için dışarıdan da hizmet alarak bu verileri yazılımdan sildirtebilir.

### 8.2. Kişisel Verileri Anonim Hale Getirme

Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Pfizer, Kanun'un 28. maddesine uygun olarak hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir. Buna göre, anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla Pfizer tarafından işlenebilmektedir. Bu tür işlemler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır. Pfizer tarafından en çok kullanılan anonimleştirme teknikleri aşağıda sıralanmaktadır.

- i. **Maskleme:** Veri maskleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örneğin, kişisel veri sahibinin tanınmasını sağlayan, T.C. Kimlik Numarasının çıkartılması veya üzerinin görünmeyecek şekilde karalanması yoluyla veri sahibinin kimliğinin tespit

edilememesinin sağlanması ve tanınmasının imkansız hale getirilmesi bir çeşit maskeleyme yöntemidir.

- ii. **Toplulaştırma:** Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin, hastaların doğum tarihlerini göstermeksizin X yaşında Y hastaları eğitime katılmıştır şeklinde veri işlenmesi toplulaştırma yöntemidir.
- iii. **Veri Türetme:** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin, çalışanların doğum tarihleri yerine yaşlarının belirtilmesi veri türetme yöntemidir.
- iv. **Veri Karma:** Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örneğin, video kayıtlarında buzlanma yönteminin uygulanması suretiyle kişinin belirlenememesi

## 9. KİŞİSEL VERİ SAHİPLERİNİN HAKLARI İLE BU HAKLARIN KULLANILMASI VE PFİZER TARAFINDAN DEĞERLENDİRİLMESİ

### 9.1. Veri Sahibinin Hakları

Kanun'un 11. maddesi uyarınca kişisel veri sahibinin hakları aşağıdaki gibidir:

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

#### 9.1.1. Kişisel Veri Sahibinin Haklarını İleri Süremeyeceği Haller

Kişisel veri sahipleri, Kanun'un 28. maddesi gereğince aşağıdaki haller Kanun kapsamı dışında tutulduğundan, kişisel veri sahiplerinin bu konularda işbu Politika'nın 9.1.1. maddesinde sayılan haklarını ileri süremezler. Şöyle ki;

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi,
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

Kanun'un 28.maddesinin 2. fıkrası gereğince; aşağıda sayılan hallerde kişisel veri sahipleri zararın giderilmesini talep etme hakkı hariç işbu Politika'nın 9.1.1. maddesinde sayılan diğer haklarını ileri süremezler:

- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,
- Kişisel veri işleminin kanunun verdiği yetkiye dayanarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

### **9.1.2. Kişisel Veri Sahibinin Haklarını Kullanması**

Kişisel Veri Sahipleri işbu Politika'nın 9.1. maddesinde sayılan haklarına ilişkin taleplerini kimliklerini tespit edecek bilgi ve belgelerle ve aşağıda belirtildiği şekilde [www.pfizer.com.tr](http://www.pfizer.com.tr) adresinde bulunan Başvuru Forumu'nu doldurup imzalayarak noter aracılığı ile Esentepe Mah. Büyükdere Cad. Levent 199, No:199, İç Kapı No: 106, Kat: 26, 34394, Levent, Şişli / İstanbul adresine ücretsiz olarak iletebileceklerdir:

Ayrıca, Kişisel Veri Sahipleri adına üçüncü kişilerin başvuru talebinde bulunabilmesi için veri sahibi tarafından başvuruda bulunacak kişi adına noter kanalıyla düzenlenmiş özel vekâletname bulunmalıdır.

Kişisel Veri Sahipleri başvurularını Türkçe yapmak zorunda olup, sizden aşağıdaki bilgiler talep edilir:

- Ad, soyad ve imza,
- Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu,
- pasaport numarası veya varsa kimlik numarası,
- Tebligata esas yerleşim yeri veya iş yeri adresi,
- Varsa bildirim esas elektronik posta adresi, telefon ve faks numarası,
- Talep konusu,
- Varsa konuya ilişkin ayrıca bilgi ve belgeler.

### **9.1.3. Kişisel Veri Sahibinin Kurul'a Şikâyette Bulunma Hakkı**

Kişisel Veri Sahibi, Kanun'un 14. maddesi uyarınca başvurunun süresi içerisinde reddedilmesi veya verilen cevabın yetersiz bulunması veya Pfizer tarafından cevap verme süresi içerisinde başvuruya cevap verilmemesi durumunda; Pfizer'in cevabını öğrendiği tarihten itibaren otuz (30) ve her hâlde başvuru tarihinden itibaren altmış (60) gün içinde Kurul'a şikâyette bulunabilir.

### **9.2. Pfizer'in Başvurulara Cevap Verme Süreci**

Pfizer'e yalnızca Pfizer'in Kanun kapsamında veri sorumlusu sayıldığı durumlarda başvuru yapılması gerekmektedir. Bu durum, Pfizer'in doğrudan ilgili kişiden kişisel veri topladığı ya da ilgili Pfizer Grup Şirketleri ile Pfizer arasındaki veri paylaşımının Kanun kapsamında veri sorumlusundan veri sorumlusuna veri transferi sayıldığı durumlarda mevcut olabilmektedir. Bunlar dışında, Pfizer Grup Şirketi'nin veri sorumlusu sayıldığı kişisel veri işleme faaliyetleri ile ilgili başvuruların Pfizer'e değil, ilgili Pfizer Grup Şirketi'ne yapılması gerekmektedir.

Kişisel veri sahibinin, işbu Politika'nın 9.1.3. maddesinde açıklanan usule uygun olarak talebini Pfizer'e iletmesi durumunda Pfizer talebin niteliğine göre en geç otuz (30) gün içinde ilgili talebi ücretsiz olarak sonuçlandıracaktır. Ancak, Kurul tarafından bir ücret öngörülmesi halinde, Pfizer tarafından başvuru sahibinden Kurul tarafından belirlenen tarifedeki ücret alınacaktır. 10 Mart 2018 tarihli 30356 sayılı Resmi Gazete'de yayımlanan "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" in 7. maddesi uyarınca Kişisel Veri Sahibinin talebine yazılı olarak cevap verilmesi halinde, ilgili cevap 10 (on) sayfa veya daha fazla ise her sayfa için 1 Türk Lirası ücret alınabilecektir. Başvuruya CD, flash bellek gibi kayıt ortamında cevap verilmesi halinde, Pfizer'in talep edeceği ücret kayıt ortamının maliyetini geçmeyecektir.

Pfizer, başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir, başvurusu ile ilgili soru yöneltebilir. Pfizer aşağıda yer alan hallerde başvuruda bulunan kişinin başvurusunu, gerekçesini açıklayarak reddedebilir:

1. Kişisel verilerin resmi istatistik ile anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,
2. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ~~fab~~özgürlüğü kapsamında işlenmesi,
3. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,
4. Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi,
5. Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
6. Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,
7. Kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması,
8. Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması,
9. Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması,
10. Orantısız çaba gerektiren taleplerde bulunmuş olması,
11. Talep edilen bilginin kamuya açık bir bilgi olması.

## **10. PFİZER'İN KİŞİSEL VERİLERİNİN KORUNMASI VE İŞLENMESİ KONUSUNDA DİĞER İÇ POLİTİKALARI**

Pfizer, işbu Politika ile ortaya koymuş olduğu esasların ilişkili olduğu kişisel verilerin korunması ve işlenmesi konusunda iç kullanıma yönelik alt politikalar oluşturmaktadır.

## **11. PFİZER KİŞİSEL VERİLERİNİN KORUNMASI VE İŞLENMESİ POLİTİKASI YÖNETİMİ**

Pfizer tarafından Kanun düzenlemelerine uygun hareket edilmesi ve Kişisel Verilerin Korunması ve İşlenmesi Politikasının yürürlüğünü sağlamak için yönetim ekibi oluşturulmuştur. Bu kapsamda, Pfizer bünyesinde işbu Politika ve bu Politika'ya bağlı ve ilişkili 10. maddede belirtilen diğer politikaların uygulanmasını ve yönetimini sağlamak amacıyla Şirket Yönetiminin kararı gereğince bir veri sorumlusu temsilcisi, bir irtibat kişisi ve bir bilişim teknoloji uzmanı, bir hukukçu olmak üzere 4 kişiden oluşan Pfizer Veri Koruma Kurulu atamıştır. Pfizer Veri Koruma Kurulu'nun görevleri aşağıdaki gibidir:

- Kişisel verilerin korunması ve işlenmesi ile ilgili temel politikaları ve gerektiğinde değişiklikleri hazırlamak ve yürürlüğe koymak ve Şirket Yönetimi'nin onayına sunmak,
- Kişisel verilerin korunması ve işlenmesine ilişkin politikaların uygulanması ve denetiminin ne şekilde yerine getirileceğine karar vermek ve bu çerçevede şirket içi görevlendirmede bulunulması ve koordinasyonun sağlanması hususlarını Şirket Yönetiminin onayına sunmak,
- Kanun ve ilgili mevzuata uyumun sağlanması için yapılması gereken hususları tespit etmek ve Şirket Yönetiminin onayına sunmak, uygulanmasını gözetmek ve koordinasyonunu sağlamak üzere Şirket Yönetimi'ne iletmek,
- Kişisel verilerin korunması ve işlenmesi konusunda Pfizer içerisinde ve Pfizer'in iş birliği içerisinde olduğu kurumlar nezdinde farkındalığı arttırmak,
- Pfizer'in kişisel veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini Şirket Yönetiminin onayına sunmak,
- Kişisel verilerin korunması ve politikaların uygulanması ve yayılımı konusunda, kişisel veri sahiplerinin kişisel veri işleme faaliyetleri ve kanuni hakları konusunda bilgilendirilmelerinin sağlanması yönünde eğitimler düzenlenmesini sağlamak,
- Kişisel veri sahiplerinin başvurularını karara bağlamak üzere Şirket Yönetimi'ne iletmek,
- Kişisel verilerin korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak Pfizer içinde yapılması gerekenler konusundaki önerilerini Şirket Yönetimi'ne iletmek,

- Kurul ve Kurum ile olan iliřkileri Őirket Yönetimi'nin koordinasyonunda yürütmek,
- Őirket Yönetimi'nin kişisel verilerin korunması konusunda vereceđi diđer görevleri icra etmektir.



## EK 1- KISALTMALAR VE TANIMLAR

Kanun: 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete’de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu’nu ifade eder.

Kurul: Kişisel Verileri Koruma Kurulu’nu ifade eder.

Kurum: Kişisel Verileri Koruma Kurumu’nu ifade eder.

Şirket: Pfizer PFE İlaçları Anonim Şirketi’dir.

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi Kanun kapsamında değildir. (Örneğin; ad-soyad, TCKN, e-posta, adres, doğum tarihi, kredi kartı numarası vb.)

Kişisel veri sahibi: Kişisel verisi işlenen gerçek kişidir. (Örneğin; çalışan adayları, doktorlar, Pfizer İş Ortakları, vb.)

Özel nitelikli kişisel veri: Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.

Kişisel verilerin işlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemidir.

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

Anonim hale getirme: Kişisel verinin, kişisel veri niteliğini kaybedecek ve bu durumun geri alınmayacağı şekilde değiştirilmesidir. (Örneğin, maskeleyme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesidir.)

İmha: Kişisel verilerin, silinmesi, yok edilmesi veya anonim hale getirilmesidir.

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir. (Örneğin, Pfizer’in verilerini tutan bulut bilişim firması, vb.)

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu veri kayıt sistemini yöneten kişidir.

İrtibat Kişisi: Türkiye’de yerleşik olan tüzel kişiler ile Türkiye’de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişidir.

Üçüncü Kişi: Kişisel verileri Politika kapsamında işlenen herhangi bir gerçek kişidir. (Örneğin, yan etki bildiriminde bulunan kişiler, vb.).

Başvuru Formu: Kişisel veri sahiplerinin haklarını kullanmak için yapacakları başvuruyu içeren Kanun gereğince kişisel veri sahibi veya temsilcisi tarafından Veri sorumlusuna yapılacak başvurulara ilişkin Pfizer internet sitesinden ulaşılabilen başvuru formudur.

Pfizer Grup Şirketleri: Pfizer İlaçları Limited Şirketi’nin doğrudan ya da dolaylı olarak bağlı olduğu Pfizer PFE İlaçları A.Ş. ve Pfizer Inc. da dahil olmak üzere diğer (iştirak, ortak, vb.) tüm şirketlerdir.

Çalışan Adayı: Pfizer’e herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini Pfizer’in incelemesine açmış olan gerçek kişilerdir.

İş birliği İçinde Olduğumuz Kurum Yetkilileri ve Çalışanları: Pfizer’in her türlü iş ilişkisi içerisinde bulunduğu kurumların (hastaneler, bakanlıklar, danışmanlar, dernekler gibi, ancak bunlarla sınırlı olmaksızın) hissedarları, yetkilileri ve çalışanları olmak üzere gerçek kişilerdir.

Tedarikçi: Pfizer’in ticari faaliyetlerini yürütürken Pfizer’in emir ve talimatlarına uygun olarak sözleşme temelli olarak Pfizer’e hizmet sunan tüzel veya gerçek kişilerdir.

Tedarikçi Yetkilileri ve Çalışanları: Tedarikçilerin hissedarları, yetkilileri ve çalışanları olmak üzere gerçek kişilerdir.

İş Ortakları: Pfizer’in ticari faaliyetlerinin yürütülmesi gibi amaçlarla iş ortaklığı kurduğu taraflardır.

İş Ortakları Yetkilileri ve Çalışanları: İş Ortakları’nın hissedarları, yetkilileri ve çalışanları olmak üzere gerçek kişilerdir.

Sağlık Mesleği Mensupları (“SMM”): Pfizer’in kamu sağlığını korumak ve kamuyu bilgilendirmek amacıyla işbirliği içerisinde olduğu tabip, diş tabibi, eczacı, hemşire, ebe ve optisyen ile 1219 sayılı Kanununun ek 13 üncü maddesinde tanımlanan diğer meslek mensupları gerçek kişilerdir.

Hasta: Saęlık hizmetlerinden faydalanma ihtiyaçı bulunan ve Pfizer ilaęlarını kullanan ve/veya klinik arařtırmalara katılan geręek kiřilerdir. (Örneęin, yan etki bildiriminde bulunan hastalar)

Ziyaretçi: Pfizer'in iř yerlerinde çeřitli amaęlarla fiziksel olarak bulunmuř olan veya internet sitelerini ziyaret eden geręek kiřiler.

Web Sitesi ve Aplikasyon Kullanıcısı: Pfizer'in web sitelerini ve/veya aplikasyonlarını ziyaret eden ve/veya üye olan geręek kiřilerdir.

Pfizer Merkez Binası: Esentepe Mah. Büyükdere Cad. Levent 199, No:199, İç Kapı No: 106, Kat: 26, 34394, Levent, řiřli / İstanbul'da bulunan Pfizer binasıdır.

řirket Yetkilisi: Pfizer yönetim kurulu üyesi ve dięer yetkili geręek kiřiler.

SSL: Güvenli giriş katmanını ifade eder. Sunucu ile istemci arasında alan verinin güvenliğini ve bütünlüğünü mümkün kılan sertifikadır.

Güvenli Elektronik İmza: Münhasıran imza sahibine baęlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluřturma aracı ile oluřturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini saęlayan, imzalanmıř elektronik veride sonradan herhangi bir deęiřiklik yapılp yapılmadıęının tespitini saęlayan elektronik imzadır.

Kayıtlı Elektronik Posta (KEP): Elektronik iletilerin, gönderimi ve teslimatı da dahil olmak üzere kullanımına iliřkin olarak hukuki delil saęlayan, elektronik postanın nitelikli řeklidir.

Mobil İmza: Mobil bir cihaz kullanılarak oluřturulan elektronik imzadır.



**PFİZER PFE İLAÇLARI ANONİM  
ŞİRKETİ**

**Policy on Processing and Protection of Personal Data**

**January 2019**

Table of Contents

**INTRODUCTION 39**

- 1. OVERVIEW ..... 39
- 2. PROTECTION OF PERSONAL DATA.....**Error! Bookmark not defined.**
- 3. PROCESSING OF PERSONAL DATA .....**Error! Bookmark not defined.**
- 4. CATEGORISATION, PROCESSING PURPOSES AND RETENTION PERIOD OF THE PERSONAL DATA PROCESSED BY PFIZER.....**Error! Bookmark not defined.**
- 5. CATEGORISATION OF DATA SUBJECTS WHOSE PERSONAL DATA ARE PROCESSED BY PFIZER.....**Error! Bookmark not defined.**
- 6. THIRD PARTIES TO WHOM PERSONAL DATA ARE TRANSFERED BY PFIZER AND PURPOSES OF TRANSFERRING .....**Error! Bookmark not defined.**
- 7. PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT IN PFIZER HEADQUARTERS AND PREMISES AND APPLICATIONS USED FOR WEBSITE VISITORS AND INSIDE PFIZER.....**Error! Bookmark not defined.**
- 8. CONDITIONS FOR ERASURE, DESCTRUTION AND ANONYMISATION OF THE PERSONAL DATA .....**Error! Bookmark not defined.**
- 9. RIGHTS OF DATA SUBJECTS AND ENFORCEMENT OF THOSE RIGHTS AND EXAMINATION THEREOF BY PFIZER.....**Error! Bookmark not defined.**
- 10. OTHER DOMESTIC POLICIES OF PFIZER ON PROTECTION AND PROCESSING OF PERSONAL DATA .....**Error! Bookmark not defined.**
- 11.MANAGEMENT OF THE POLICY OF PFIZER ON PROTECTION AND PROCESSING OF PERSONAL DATA .....**Error! Bookmark not defined.**

**ANNEX 1- ABBREVIATIONS AND TERMS 68**

## INTRODUCTION

### 1. OVERVIEW

As Pfizer PFE İlaçları Anonim Şirketi (hereinafter referred to briefly as “**Pfizer**”), we protect personal data with due diligence not only in Turkey but also worldwide as a global company, and we adapt this as a corporate policy, implementing it for all natural and legal persons. In accordance with the Law on Protection of Personal Data numbered 6698 (“**Law**”) and other primary and secondary regulations that Pfizer is subject to, we aim to protect the personal data of executives and employees of the institutions, suppliers and business partners; and health care professionals, patients, visitors, website visitors, former Pfizer employees, job candidates and other third parties whom we cooperate with and process data of (“**Data Subjects**”) pursuant to this Policy on Processing and Protection of Personal Data (“**Policy**”).

Despite the fact that this Policy is for the natural persons of whom personal data is processed either manually provided that it is an entry of a data registry system or automatically by Pfizer, protection of personal data of Pfizer employees are regulated separately under the “Policy on Processing and Protection of Personal Data of Pfizer PFE İlaçları Anonim Şirketi Employees”.

As Pfizer, we take the necessary administrative and technical measures to protect personal data processed in accordance with the Personal Data Protection Law No. 6698 (“**Law**”).

In the processing of personal data we adopt the principles of (i) Processing personal data in accordance with the law and the rules of honesty,(ii) keeping personal data accurate and updated when necessary, (iii) related, limited and proportionate processing of personal data, (v) Keeping personal data for the period stipulated in the relevant legislation or necessary for the purpose for which they are processed, (vi) Enlightening and informing data subjects, (vii) Creating the necessary technical and administrative infrastructure for data subjects to exercise their rights, (viii) Taking the necessary technical and administrative measures to preserve personal data, (ix) Complying with the relevant legislation and the Board's regulations in transferring personal data to third parties in line with the requirements of the purpose of processing, (x) Showing the necessary sensitivity regarding the processing and protection of sensitive personal data.

We provide detailed explanations about these basic principles in this Policy.

#### 1.1. Purpose and Scope of the Policy

The purpose of this Policy is to set forth the security measures and precautions to protect the data which is processed using the methods that Pfizer adopts and employs for processing personal data in accordance with the law, and to inform the persons whom personal data is processed by Pfizer and to

provide transparency.

In this context, this Policy has been prepared to inform the public about the processing, storage, destruction, anonymization and protection of the personal data of the Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties, collected by Pfizer through automatic or non-automatic means provided that it is part of any data recording system.

## **1.2. Implementation of the Policy and Relevant Legislation**

Relevant legal regulations which are in force on processing and protection of personal data shall be implemented primarily. In the event of a conflict between the Policy and applicable legislation in force, Pfizer agrees to implement the legislation in force.

## **1.3. Enforcement of the Policy**

This Policy shall enter into force on January 3, 2019 by the approval of Pfizer and it shall be accessible to the Data Subjects upon their request.

# **2. PROTECTION OF PERSONAL DATA**

## **2.1. Establishing the Security of Personal Data**

In accordance with Article 12 of the Law, Pfizer takes all the necessary measures and conducts the necessary inspections and is subjected to inspections by other authorities to prevent the unlawful processing of the personal data being processed by Pfizer, and to establish the security of personal data and to prevent unauthorized persons from accessing the personal data.

In this context, in the Personal Data Guide (Technical and Administrative Measures) published by the Board; (i) Authority Matrix, (ii) Authorization Control, (iii) Access Logs, (iv) User Account Management, (v) Network Security, (vi) Application Security, (vii) Encryption, (viii) Penetration Test, (ix) Intrusion Detection and Prevention Systems, (x) Log Records, (xi) Data Masking, (xii) Data Loss Prevention Software, (xiii) Backup, (xiv) Firewalls, (xv) Current Anti Virus Systems, (xvi) Deletion, Destruction and Anonymization, (xvii) Explained Key Management as technical measures that can be taken by data controllers. Likewise, in the same Personal Data Guide (Technical and Administrative Measures) published by the Board; (i) Preparation of Personal Data Inventory, (ii) Preparation and implementation of Corporate Policies (Access, Information Security, Use, Storage and Destruction, etc.), (iii) Concluding Contracts (Between Data Controller - Data Controller, Data Controller - Data



Processor), (iv) Signing Confidentiality Commitments, (v) Conducting Internal Random or Periodic Audits, (vi) Conducting Risk Analysis, (vii) Adding Lawful Provisions to the Employment Contract and Disciplinary Regulation, (viii) Making Corporate Communication Principles Compliant with the Law (Crisis Management, Board and Relevant Person Informing Processes, Reputation Management, etc.), (ix) Conducting Training and Awareness Activities (within the framework of Information Security and Law) and (x) Establishing the Notification Process to the Data Controllers Registry Information System (VERBIS) as administrative measures that can be taken by data controllers

Pfizer takes the following administrative and technical measures in line with Guidelines on Personal Data Security (Technical and Administrative Measures) explained above and published by the Board:

- Determining current risks and threats,
- Training Pfizer employees and creating awareness,
- Establishing policies and procedures on personal data security,
- Reducing the amount of personal data being processed by Pfizer,
- Concluding an Agreement between the Processors and Pfizer in accordance with the Law,
- Taking administrative and technical measures in order to establish cybersecurity (e.g. Erasure of unused software and services, creating firewalls, patch management and software updates, access restrictions, creating access authorisation and control matrix, using antivirus products, establishing SSL connection etc.),
- Monitoring personal data security (e.g. logging, establishing an official reporting procedure to report security problems, vulnerability scans and penetration tests),
- Encrypting and storing personal data in the cloud and using crypto key, and
- Developing data backup strategies.

### **2.1.1. Technical and Administrative Measures to Maintain Lawful Processing of Personal Data**

In line with the technical and financial possibilities, Pfizer takes the administrative and technical measures listed below with a view to maintaining lawful processing of personal data. Those measures are:

- monitoring personal data processing activities carried out within Pfizer using established technical systems,
- reporting technical measures to the related person when necessary,
- employing qualified personnel on technical matters,
- concluding agreements and documents governing the legal relationship between Pfizer and

Pfizer Employees in a way to stipulate that personal data are not processed, disclosed, or used unless otherwise is enforced by the Law, and creating awareness thereof among Pfizer Employees,

- informing and training Pfizer Employees periodically on personal data protection law and lawful processing of personal data,
- taking data inventories by analysing the business processes and determining personal data processing activities carried out by business units and the requirements to ensure that these activities comply with the Law,
- implementing policies and training people, including but not limited to, who have periodic access grant to corporate systems of Pfizer (and other natural persons when necessary) so as to fulfil legal conformity requirements, create awareness within the Company, ensure the sustainability of practices and perform regular inspections, and
- concluding agreements and documents governing the legal relationship between Pfizer and Institutions, Suppliers, Business Partners, Health Care Professionals, Patients, Visitors, Website Visitors and other Third Parties that We Cooperate With Pfizer Employees in a way to stipulate that personal data are not processed, disclosed, or used reciprocally unless otherwise is enforced by the Law, and creating awareness thereof among Pfizer Employees.

### **2.1.2. Technical and Administrative Measures Taken to Deny Unlawful Access to Personal Data**

As long as it is technologically and financially possible, Pfizer takes the following technical and administrative measures which are necessary to prevent personal data from being disclosed, accessed or transferred in an imprudent or unauthorized way or from being accessed in any other unlawful way. Those measures are:

- taking technical precautions based on the latest technological developments and updating or renewing them when necessary,
- adopting technical solutions regarding access and authorization pursuant to the legal conformity requirements which are determined based on process,
- restricting access authorisations and reviewing them regularly,
- reporting technical measures when necessary and finding technological solutions after re-assessing the matters that pose risk,
- installing software and hardware involving anti-virus systems and firewalls,
- employing qualified personnel on technical matters,
- training Pfizer Employees on technical measures to avoid unlawful access to personal data,
- designing and implementing access and authorization processes of personal data within the

Company in accordance with the legal conformity requirements on processing of personal data based on process,

- informing Pfizer Employees that they cannot disclose the personal data unlawfully or use the personal data except for processing purposes and this liability shall remain in force even after the termination of their job, and legally ensuring their commitment on this liability,
- adding provisions to the agreements concluded with persons to whom personal data transferred lawfully by Pfizer in a way that persons to whom personal data is transferred take the necessary security measures and ensure those measures are implemented within their institution.

### **2.1.3. Security and Storage of Personal Data**

As long as it is technologically and financially possible, Pfizer takes the following technical and administrative measures which are necessary to store the personal data in a secure place and to prevent personal data from being erased, lost or altered for unlawful purposes. Those measures are:

- using up-to-date systems to store the personal data in secure places,
- employing expert personnel on technical matters,
- installing technical security systems for storage, reporting technical measures to the person concerned when necessary and finding technological solutions after re-assessing the matters that pose risk,
- using backup programs lawfully in order to ensure secure storage of personal data,
- logging access to the data storage where personal data are stored, and reporting unauthorised access or access attempts instantly to the persons concerned,
- training Pfizer Employees on how to ensure secure storage of personal data,
- If Pfizer outsources the storage of personal data due to technical requirements, provisions enforcing that persons to whom personal data is transferred take the necessary security measures and ensure those measures are implemented within their institution are included in the agreements signed with the companies that the personal data is transferred to lawfully.

### **2.1.4. Inspection of the Measures Taken to Protect Personal Data**

In accordance with Article 12 of the Law, Pfizer conducts the necessary inspections and is subject to inspections by other authorities. The results of aforementioned inspections are reported to the concerned units as part of Pfizer's internal processes, and the required activities are undertaken to improve the measures taken.

### **2.1.5. Measures to Be Taken In the Event of Unauthorized Disclosure of Personal Data**

If the personal data being processed in accordance with Article 12 of the Law is acquired unlawfully by others; Pfizer ensures that the concerned data subject, Pfizer Committee on Data Protection and the Board are informed of such situation as soon as possible.

### **2.2. Protection of Sensitive Personal Data**

The Law also imposes certain regulations on the processing and protection of sensitive personal data since some personal data are of special nature. In accordance with the Law, personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive personal data.

As a global pharmaceutical company, we care and pay special attention to the processing and protection of sensitive personal data lawfully. Therefore, Pfizer takes the technical and administrative measures and conducts the necessary inspections periodically in order to protect the personal data.

### **2.3. Fostering Awareness of Personal Data Processing and Protection Among the Executives and Employees of Pfizer, Cooperated Institutions, Suppliers and Business Partners, and Health Care Professionals and Other Third Parties and Inspection Thereof**

As Pfizer, we arrange trainings for people who hold the title of ‘processor’ upon the instruction and request of Pfizer pursuant to the Law in order to prevent personal data from being accessed and processed unlawfully and to foster awareness about data protection. We are also working with expert people on personal data protection when necessary. Such trainings are repeated periodically and we update the trainings based on recent regulatory changes.

## **3. PROCESSING OF PERSONAL DATA**

### **3.1. Personal Data Processing**

In accordance with Article 20 of the Law on Privacy of Private Life and Articles 4 and 6 of the Law, Pfizer processes personal data in compliance with the following principles: lawfulness and conformity with rules of *bona fides*, accuracy and being up to date, where necessary; being processed for specific, explicit and legitimate purposes, being relevant with, limited to and proportionate to the purposes for

which they are processed. In accordance with the following principles, Pfizer stores the personal data for the period of time which is required to fulfil the processing purpose and/or accepted on sectoral basis.

- i. Processing Lawfully and in Good Faith:** Pfizer acts in accordance with the principles stipulated by legal regulations on processing personal data and general principles of good faith. For this reason, Pfizer does not process or use any personal data outside the “purposes for which they are processed”.
- ii. Ensuring That Personal Data Are Accurate and -When Necessary- Updated:** Pfizer ensures that personal data are accurate and updated, and takes the necessary measures accordingly as it is stated in this Policy.
- iii. Processing for Specific, Explicit and Legitimate Purposes:** Pfizer explicitly and specifically determines the purpose of personal data processing which is legitimate and lawful. Pfizer processes the personal data which are linked to the commercial activity that Pfizer is carrying out and only the required amount thereof. Pfizer sets out the purpose for which personal data are processed before starting the activity of processing personal data.
- iv. Being Purpose-Related, Limited and Proportionate:** Pfizer processes the personal data in a suitable way to achieve the purposes, and avoids processing the personal data which are not related to the purpose or not necessary.
- v. Storing Personal Data for the Period of Time Which Is Required for Their Processing Purpose or Provided For by the Relevant Legislation:** Pfizer stores the personal data only for the period of time which is set forth in the relevant legislation or accepted in sectoral basis, or which required to fulfil the purpose of processing and/or within the period which is set forth in Pfizer’s erasure policy. Therefore, Pfizer first determines if relevant legislation stipulates a period of time for storing the personal data. If it is set forth, Pfizer acts accordingly; otherwise, we store the personal data for the period of time which is required to achieve the purpose of processing and/or accepted on sectoral basis and/or determined by Pfizer. In case aforementioned period ends or the causes disappeared, personal data are erased, destructed or anonymised by Pfizer. Personal data are kept for possible future use by Pfizer only if there are legitimate interests.

Protection of personal data is a Constitutional right. Fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence. Pursuant to Article 20 of the Constitution, personal data may be processed only in cases envisaged by law or with the explicit consent of the data subject. In accordance with the third paragraph of Article 20 of the Constitution and Article 5 of the Law, Pfizer processes personal data if one or more conditions listed in the article of the Law are met, and only in cases envisaged by law or with the explicit consent of the data subject. Pursuant to Articles 8 and 9 of the

Law, Pfizer transfers personal data in accordance with the Law and the regulations issued by the Board.

Pursuant to Article 10 of the Law, Pfizer enlightens the data subjects about their personal data which are processed and provides information if data subjects request it. Pfizer therefore enlightens about the identity of his representative, if any; the purpose of data processing; to whom and for what purposes the processed data may be transferred, the method and legal reason of collection of personal data, and the rights that the data subject has.

It is set forth in Article 20 of the Constitution that everyone has the right to be informed of their personal data. Therefore “to request information” is stated among the rights of data subject in Article 11 of the Law. Within this scope, Pfizer provides the required information in case Data Subject request information pursuant to Article 20 of the Constitution and Article 11 of the Law.

### **3.2. Processing of Sensitive Personal Data**

As a global pharmaceutical company, we care and act accordingly to the regulations envisaged by the Constitution and the Law on the processing of sensitive personal data lawfully.

In Article 6 of the Law, the personal data which pose the risk of causing victimisation or discrimination when processed unlawfully are defined as “sensitive”. Sensitive data are the personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data.

Sensitive personal data are processed by Pfizer under the following conditions provided that the measures set forth in the Guidelines on Personal Data Security (Technical and Administrative Measures) issued by the Board in accordance with the Law and the Board Decision numbered 2018/10 and dated January 3, 2018 on “Sufficient Measures That Must Be Taken for Processing of Sensitive Personal Data” which was published in the Official Gazette dated March 13, 2018 and numbered 30356 are taken:

- If the data subject gives explicit consent or
- If the data subject does not give explicit consent,
  - Sensitive personal data of the data subject, excluding those relating to health and sexual life, are processed under the conditions envisaged by the laws;
  - Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of

public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

### **3.3. Transfer of Personal Data**

Pfizer may transfer the personal data and sensitive personal data of data subjects to the third parties provided that the necessary security measures are taken in line with lawful processing purposes of personal data. Pfizer therefore acts in accordance with the regulations which are envisaged in Article 8 of the Law.

In accordance with legitimate and lawful purposes for processing personal data, Pfizer may transfer personal data to the third parties in a limited way and provided that one or more of the conditions set forth in the second paragraph of Article 5 of the Law are met, and that;

- the data subject gives explicit consent,
- an explicit regulation exists in the laws regarding the transfer of personal data,
- it is mandatory for the protection of life or physical integrity of the data subject or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
- processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract,
- it is mandatory for Pfizer to be able to perform his legal obligations,
- the data concerned is made available to the public by the data subject,
- data processing is mandatory for the establishment, exercise or protection of any right,
- it is mandatory for the legitimate interests of Pfizer, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

#### **3.3.1. Transfer of Sensitive Personal Data**

Pfizer may transfer sensitive personal data of the data subject for legitimate and lawful processing purposes with due diligence, taking due security measures and the measures issued by the Board under the following conditions:

- If the data subject gives explicit consent or
- If the data subject does not give explicit consent,

- Sensitive personal data of the data subject, excluding those relating to health and sexual life (race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data) are processed under the conditions envisaged by the laws;
- Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

### **3.4. Transfer of Personal Data Abroad**

Pfizer may transfer the personal data and sensitive personal data of data subjects to the third parties provided that the necessary security measures are taken in line with lawful processing purposes of personal data.

Pfizer may transfer personal data abroad provided that the Board announces that the foreign countries provide sufficient protection (“Countries Providing Sufficient Protection”) or the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer (“Foreign Country Where the Controller Guarantees Sufficient Protection”), where sufficient protection is not provided. Pfizer therefore acts in accordance with the regulations which are envisaged in Article 9 of the Law.

Pfizer can transfer personal data abroad for legitimate and lawful processing purposes only with explicit consent of the data subject. In cases where explicit consent of the data subject does not exist, Pfizer may transfer personal data to the Countries Providing Sufficient Protection or Foreign Countries Where the Controller Guarantees Sufficient Protection provided that one of the conditions set forth below exist:

- the data subject gives explicit consent,
- an explicit regulation exists in the laws regarding the transfer of personal data,
- it is mandatory for the protection of life or physical integrity of the data subject or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid,
- processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract,



- it is mandatory for Pfizer to be able to perform his legal obligations,
- the data concerned is made available to the public by the data subject,
- data processing is mandatory for the establishment, exercise or protection of any right,
- it is mandatory for the legitimate interests of Pfizer, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

### **3.4.1. Transfer of Sensitive Personal Data Abroad**

Pfizer can transfer sensitive personal data abroad for legitimate and lawful processing purposes only with explicit consent of the data subject. In cases where explicit consent of the data subject does not exist, Pfizer may transfer personal data to the Countries Providing Sufficient Protection or Foreign Countries Where the Controller Guarantees Sufficient Protection provided that one of the conditions set forth below exist:

- If the data subject gives explicit consent or
- If the data subject does not give explicit consent,
  - Sensitive personal data of the data subject, excluding those relating to health and sexual life (race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data) are processed under the conditions envisaged by the laws;
  - Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

## **4. CATEGORISATION, PROCESSING PURPOSES AND RETENTION PERIOD OF THE PERSONAL DATA PROCESSED BY PFIZER**

### **4.1. Categorisation of Personal Data**

In accordance with Pfizer's legitimate and lawful purposes for processing personal data, Pfizer processes the personal data which are categorised below in a limited way, provided that one or more of the conditions set forth in Article 5 of the Law are met, and in compliance with the principles set forth in

Article 4 in relation to processing of personal data and general principles provided for by the Law and all the obligations regulated under the Law and limited to those Data Subjects who are within the scope of this Policy provided that the relevant persons are informed pursuant to Article 10 of the Law. Related data subjects of those data categories are provided in Article 5 of this Policy.

Personal Data or Sensitive Personal Data	Description
<b>Identity Information</b>	Driver’s license, ID card, passport or any other documents containing information such as name-surname, T.R. identity number, nationality, mother’s full name, father’s full name, place of birth, date of birth and gender; and tax number, social security institution (SSI) number, signature, license plate.
<b>Contact Information</b>	Phone number, address, electronic mail (email) address, fax number, IP address.
<b>Sensitive Personal Data</b>	Medical data such as prescription, doctor’s certificate, medical analysis and radiology reports, medical report, blood type, genetic data etc., and personal data relating to religion, membership to associations, etc.
<b>Information about Physical Environment Security</b>	Personal data related to the records and documents which are created in the physical environment which Pfizer owns or rents (Pfizer Headquarters and/or Pfizer Offices), e.g. CCTV records, records collected at a checkpoint.
<b>Financial Information</b>	Personal data processed concerning any information, document and record that shows any type of financial outcome created depending on the type of legal

	relationship between Suppliers, Business Partners, HCPs and other third parties or other personal data owners; and bank account number, IBAN number, credit card information, financial profile, data on assets and income.
<b>Visual/Audio Information</b>	Any kind of photo, video and voice recording.
<b>Employee's Professional Information</b>	Professional information which provides a basis for employee personal rights of natural persons who have worked or will work with Pfizer (including Former Employees and Job Candidates of Pfizer), e.g. resume, medical report, bank account details, detailed breakdown of insurance provided from SSI, passport photo, copy of ID card etc.
<b>Information about Request/Complaint Management</b>	Any kind of personal data collected as part of the execution of processes such as Product Safety, Quality, Medical Information etc.; and data concerning the reception and evaluation of any request or complaint addressed to Pfizer.
<b>Information about Process Security</b>	Personal data processed to ensure the technical, administrative, legal and commercial security of both the data subject and the Company during the business operations of Pfizer.
<b>Information about Risk Management</b>	Personal data processed for the management of commercial, technical and administrative risks with methods used in

	accordance with customary law, commercial usage and rules of <i>bona fides</i> .
<b>Compliance Information of Legal Actions</b>	Personal data processed as part of determining and pursuing Pfizer's legal rights and claims, in compliance with legal obligations and policies of Pfizer.
<b>Information about Audit and Inspection</b>	Personal data processed in compliance with Pfizer's legal obligations and the Company policies.
<b>Information about Reputation Management</b>	Personal data associated with a person and collected in order to protect the commercial reputation of Pfizer.

#### 4.2. Purposes of Processing Personal Data

Pfizer processes personal data limited to the purposes and conditions for processing personal data which are set forth in the second paragraph of Article 5 of the Law and the third paragraph of Article 6 thereof. Your personal data may be processed by Pfizer if one of the following conditions exists:

- If processing of your personal data is clearly provided for by the laws.
- If processing of your personal data is necessary or directly related to the conclusion or fulfilment of a contract.
- If processing of your personal data is mandatory for Pfizer to be able to perform its legal obligations.
- If you made your personal data available to the public, provided that it is processed by Pfizer in a way limited to your reasons for making it available to public.
- If processing of your personal data is mandatory for the establishment, exercise or protection of Pfizer's or your rights.
- If processing of your personal data is mandatory for the legitimate interests of Pfizer, provided that this processing shall not violate your fundamental rights and freedoms.
- If processing of personal data by Pfizer is mandatory for the protection of life or physical integrity of the data subject or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.

- If processing of sensitive personal data of the data subject, excluding those relating to health and sexual life, is provided for by laws.
- Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

Within this scope, Pfizer processes your personal data for the following purposes:

- to perform internal operations and business activities of the Company, ensure the security of the Company's operations and undertake necessary activities to conduct effectiveness, efficiency, aptness analyses of business activities.
- to perform recruitment processes,
- to manage and execute strategy planning activities and relationship with Business Partners or Suppliers,
- to manage and execute promotional activities, to carry out marketing and sales activities, to maintain processes of creating and developing commitment to the products and/or services offered by the Company and to perform market research to market and sell the products and services,
- to carry out production and/or operation processes,
- to manage and carry out Product Safety, Medical Information and Notification of Side effects,
- to maintain business continuity and operating necessary processes for corporate governance activities,
- to plan, perform and maintain congressional activities,
- to maintain and carry out clinical research activities,
- to manage and maintain the relationships with Patients, Cooperated Institutions and HCPs,
- to manage and carry out registration processes of Pfizer,
- to manage and carry out quality processes of Pfizer,
- to plan and perform institutional sustainability activities,
- to manage events,
- to carry out/monitor processes of financial reporting and risk management,
- to plan, assess and monitor purchasing activities,
- to enforce/pursue the legal affairs of Pfizer,
- to maintain activities which have a legal, technical and administrative outcome, to inform authorities in accordance with the legislation and to carry out activities regarding legal claims

and legal affairs,

- to keep data accurate and updated,
- to plan and carry out corporate communication activities,
- to carry out corporate governance activities,
- to manage requests and complaints,
- to comply with regulations,
- to inform authorities in accordance with the legislation,
- to keep records of visitors,
- to ensure the security of the headquarters and/or premises of Pfizer,
- to plan and carry out logistic activities,
- to carry out activities regarding information security processes and information technology infrastructure,
- to plan and carry out processes of emergency management and to maintain processes of occupational health and/or safety,
- to carry out activities regarding group companies and maintain access to information for the employees,
- to manage social media accounts and websites.

Within the scope of this Policy, personal data of persons whose personal data are processed are collected in written or electronic form via electronic mail (email), text message (sms), websites of Pfizer, online or paper application form, communication form and any other form, telephone and voice mail services, complaint management systems, customer relationship management systems, social media mediums, voice recordings and video recordings for the purposes set forth heretofore and explained in this Policy.

If the processing activity which is carried out for aforementioned purposes does not meet any of the conditions provided for in the Law, Pfizer shall obtain your explicit consent regarding such processing activity.

On the other hand, Pfizer shall process the personal data collected during the recruitment process of Job Candidates, who are categorised as the data subjects from whom Pfizer collects the most personal data, and sensitive personal data collected from them depending on the job's nature for the purposes explained below:

- Evaluating the qualifications, experience, interest and suitability of a Job Candidate for the vacant position,
- Conducting research about the Job Candidate contacting third parties,

- Contacting the Job Candidate about their application and recruitment process,
- Reaching out the Job Candidate in the event of a vacant position,
- Meeting the requirements of the relevant legislation and/or the demands of authorised organisations and institutions,

Within this scope, personal data of the Job Candidates are collected for a predetermined purpose **(i)** through their application form either on paper or in digital format and **(ii)** résumés sent to Pfizer by email, post, reference etc. and **(iii)** via recruitment and/or consultancy companies, online recruitment platforms, **(iv)** during video conference or face to face interviews, **(v)** through recruitment tests to determine talent and personality traits which are conducted and evaluated by experienced experts, **(vi)** throughout the recruitment process, and **(vii)** following the recruitment.

If Job Candidates desire, they can submit their requests for the rights stemming from being a Data Subject and deriving from the Law, using the method explained in Article 9 of this Policy.

#### **4.3. Retention Period of Personal Data**

Pfizer shall store personal data for a period of time as provided for by the relevant laws and legislation.

If such period of time is not provided by the relevant legislation, personal data shall be processed for the period of time requiring them to be processed, which depends on the activity carried out by Pfizer to process such data, in accordance with the practices of Pfizer and commercial usage. After that, they shall be erased, destroyed or anonymised.

In the event that the purpose for processing of such personal data no longer exists and the retention period determined by Pfizer ends, personal data may only be stored provided that they are evidentiary for possible legal disputes or with a view to claiming a right regarding the personal data or raising a defence. Retention periods are determined based on limitation periods for claiming aforementioned right and the requests that Pfizer has received before on the same subject even though the limitation period ended. In this case, personal data shall not be accessed for any other purpose and may only be accessed if they are required for a relevant legal dispute. In the event that such limitation periods end, personal data shall be erased, destroyed or anonymised.

## **5. CATEGORISATION OF DATA SUBJECTS WHOSE PERSONAL DATA ARE PROCESSED BY PFIZER**

Although the personal data of the data subject categories listed below are processed by Pfizer, the scope of application of this Policy is limited to Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.

Although the categories of persons whose personal data are processed by Pfizer are within the scope stated above, persons outside these categories may also submit their requests to Pfizer within the scope of the Law; The requests of these people will also be evaluated within the scope of this Policy.

The table below details the categories of personal data owners that we define as Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties and the types of personal data processed by the people in these categories.

<b>Categorisation of Personal Data</b>	<b>Categorisation of Data Subjects</b>
<b>Identity Information</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.
<b>Contact Information</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.
<b>Sensitive Personal Data</b>	Patients, Website and Application Users, Job Candidates, and other Third Parties
<b>Information about Family Members and Relatives</b>	Patients, Website and Application Users, Job Candidates, and other Third Parties
<b>Information about Physical Environment Security</b>	Visitors



<b>Financial Information</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners; Health Care Professionals and other Third Parties
<b>Visual/Audio Information</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners; Health Care Professionals, Patients, Visitors, Job Candidates and other Third Parties
<b>Employee's Professional Information</b>	Employees of Pfizer, Former Employees of Pfizer, Job Candidates and other Third Parties
<b>Information about Request/Complaint Management</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners; Health Care Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties
<b>Information about Process Security</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners; Health Care Professionals, Patients, Former Employees of Pfizer, Visitors, Website and Application Users, Job Candidates and other Third Parties
<b>Information about Risk Management</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.
<b>Compliance Information of Legal Actions</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors,

	Website and Application Users, Job Candidates and other Third Parties.
<b>Information about Audit and Inspection</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.
<b>Information about Reputation Management</b>	Executives and Employees of Cooperated Institutions, Suppliers and Business Partners, Healthcare Professionals, Patients, Visitors, Website and Application Users, Job Candidates and other Third Parties.

## **6. THIRD PARTIES TO WHOM PERSONAL DATA ARE TRANSFERED BY PFIZER AND PURPOSES OF TRANSFERRING**

Pursuant to Articles 8 and 9 of the Law, Pfizer may transfer the personal data of data subjects which are managed by the Policy to the person categories listed below:

- i.** Business Partners of Pfizer (including doctors, pharmacists, patients),
- ii.** Suppliers of Pfizer,
- iii.** Global companies and associates of Pfizer (Pfizer Inc., especially Pfizer PFE İlaçları A.Ş. etc.),
- iv.** Executives of Pfizer,
- v.** Legally competent public institutions and organisations (e.g. Ministry of Health, Directorate of Customs, Courts etc.)
- vi.** Legally competent private entities,
- vii.** Authorised employees of Pfizer.

Extent of above-mentioned persons to whom personal data are transferred and purposes of transferring are set forth below.

In accordance with Article 10 of the Law, Pfizer shall inform the data subjects about the persons to whom their personal data are transferred.

## **7. PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT IN PFIZER HEADQUARTERS AND PREMISES AND APPLICATIONS USED FOR WEBSITE VISITORS AND INSIDE PFIZER**

### **7.1. Personal Data Processing Activities Carried Out in Pfizer**

In order to establish security, Pfizer carries out activities of CCTV monitoring in Pfizer Headquarters (“**Headquarters**”) and personal data processing aimed at monitoring the entrance and exit of visitors.

Pfizer processes personal data by using CCTV and recording entrance and exit of visitors.

Pfizer monitors the entrance of Headquarters and inside the building with CCTV cameras, aiming to protect its interests regarding ensuring the security of the Company and other persons (Employees of Pfizer, visitors etc.). Within this scope, Pfizer acts in compliance with the Law and other relevant legislation. Video surveillance complies with the Law on Private Security Services and the relevant legislation, and Pfizer acts in accordance with the regulations in the Law regarding CCTV monitoring for security purposes. Therefore, data subjects shall be informed under Article 10 of the Law. As part of the obligation to inform, Pfizer shall put up an explanatory statement at the entrances of Pfizer Headquarters and publish this Policy on the website. There are also notice signs in the areas which are being monitored, informing people of the monitoring activity.

Pursuant to Article 4 of the Law, Pfizer shall process personal data in connection with, limited to and proportionate to the purposes for which they are processed, and therefore, maintain video surveillance activity for its intended purpose. Pfizer shall determine the areas to monitor on CCTV, number of cameras and retention periods of video recordings in a limited way, without going beyond the security purposes. Furthermore, video recording activities are maintained without violating privacy of the persons.

Pfizer takes the necessary technical and administrative measures to ensure the security of personal data acquired through video recordings resulting from CCTV monitoring activity of Pfizer. Within this scope, only limited number of Pfizer employees have access to those video recordings.

Also, Pfizer carries out personal data processing activity to monitor the entrance and exit of visitors in Pfizer Headquarters for the purposes of this Policy and ensuring security. Names, surnames and T.R. Identity Numbers of the Visitors coming to Pfizer Headquarters are processed accordingly. In this

context, Visitors are informed through the explanatory statements which are hung at the entrances. Data which are collected to monitor the entrance and exit of visitors shall be processed only for this purpose and the relevant personal data shall be recorded physically on the data registry system.

### **7.1 Website and Pfizer Mobile Application Visitors**

Pfizer records the visits of the persons who visit the website and mobile application of Pfizer with the aim of ensuring they are made in accordance with their purposes, and showing customised content to the visitors and carrying out online activities (e.g. cookies etc.), using technical methods which record Internet transactions on the website and/or application. Pfizer sets forth the detailed explanation regarding aforementioned activities that are carried out on the website and the protection and processing of personal data, in the texts of relevant websites and applications entitled “Data Privacy and Security Policy”.

Pfizer uses various systems in order to carry out its activities. Employees of Pfizer may process personal data on those systems in accordance with the job that they are carrying out and the definition of the job in line with the following purposes:

- to perform internal operations and business activities of the Company, ensure the security of the Company’s operations and undertake necessary activities to conduct effectiveness, efficiency, aptness analyses of business activities.
- to perform recruitment processes,
- to manage and execute strategy planning activities and relationship with Business Partners or Suppliers,
- to manage and execute promotional activities, to carry out marketing and sales activities, to maintain processes of creating and developing commitment to the products and/or services offered by the Company and to perform market research to market and sell the products and services,
- to carry out production and/or operation processes,
- to manage and carry out Product Safety, Medical Information and Notification of Side effects,
- to maintain business continuity and operating necessary processes for corporate governance activities,
- to plan, perform and maintain congressional activities,
- to maintain and carry out clinical research activities,
- to manage and maintain the relationships with Patients, Cooperated Institutions and HCPs,
- to manage and carry out registration processes of Pfizer,
- to manage and carry out quality processes of Pfizer,
- to plan and perform institutional sustainability activities,

- to manage events,
- to carry out/monitor processes of financial reporting and risk management,
- to plan, assess and monitor purchasing activities,
- to enforce/pursue the legal affairs of Pfizer,
- to maintain activities which have a legal, technical and administrative outcome, to inform authorities in accordance with the legislation and to carry out activities regarding legal claims and legal affairs,
- to keep data accurate and updated,
- to plan and carry out corporate communication activities,
- to carry out corporate governance activities,
- to manage requests and complaints,
- to comply with regulations,
- to inform authorities in accordance with the legislation,
- to keep records of visitors,
- to ensure the security of the headquarters and/or premises of Pfizer,
- to plan and carry out logistic activities,
- to carry out activities regarding information security processes and information technology infrastructure,
- to plan and carry out processes of emergency management and to maintain processes of occupational health and/or safety,
- to carry out activities regarding group companies and maintain access to information for the employees,
- to manage social media accounts and websites.

## **8. CONDITIONS FOR ERASURE, DESTRUCTION AND ANONYMISATION OF THE PERSONAL DATA**

Despite being processed under Article 138 of Turkish Criminal Code and the provisions of Article 7 of the Law, personal data shall be erased, destroyed or anonymised by Pfizer ex officio or upon the demand of data subject, upon disappearance of reasons which require the process. Therefore, Pfizer shall erase, destroy or anonymise the personal data using the following methods and techniques.

## 8.1. Erasure and Destruction of Personal Data

- i. Destroying Physically: Personal data may be processed manually provided that they are part of a data registry system. That kind of personal data are erased/destroyed physically in a way that they cannot be used later. For instance, tearing and shredding a printed résumé is an example of destroying physically.
- ii. Secure Erasure: For the erasure/destruction of the data which are processed in fully or partially automatic ways and kept in digital environment, methods are used to enable erasure of such data irretrievably. In cases where digital erasure/destruction is not possible, Pfizer prevents the use of such data by restricting access to them in a way provided for by laws. In some cases, Pfizer may outsource the service of secure erasure to get those data erased.

## 8.2. Anonymisation of Personal Data

Anonymisation of personal data is defined as making personal data impossible to be associated with any identified or identifiable natural person under no circumstances, including matching of the personal data with other data. Pfizer may anonymise the personal data which is processed lawfully and in compliance with Article 28 of the Law when the reasons requiring data processing no longer exist. Accordingly, personal data may be processed by Pfizer for research, planning and statistical purposes after having been anonymised. Such processing is considered outside the scope of the Law, and the explicit consent of data subjects shall not be sought. The anonymisation techniques which are commonly used by Pfizer are as follows:

- i. **Masking**: It is a method which involves anonymisation of personal data by removing the basic identifier information from the dataset. For instance, preventing data subject from being identified and making them impossible to identify by removing or obfuscating T.R. Identity Number, which enables identification of the data subject.
- ii. **Aggregation**: Data aggregation is a method which combines multiple data entities into one, making personal data impossible to be associated with any person. For instance, processing X-year-old Y patients who participated in a training without indicating their date of birth.
- iii. **Generalisation**: Generalisation is a method which involves creating a more general values and makes personal data impossible to be associated with any person. For instance, showing the age of employees instead of date of birth.
- iv. **Swapping**: Data swapping is a method which swaps the subsets of a personal dataset, breaking the link between data

## 9. RIGHTS OF DATA SUBJECTS AND ENFORCEMENT OF THOSE RIGHTS AND EXAMINATION THEREOF BY PFIZER

## **9.1. Rights of Data Subject**

Pursuant to Article 11 of the Law, data subjects have the following rights:

- To learn whether or not personal data is being processed,
- To request further information about processing if their personal data is processed,
- To learn the purpose of processing of their personal data and whether this data is used for intended purposes,
- To know the third parties to whom their personal data is transferred within the country or abroad,
- To request rectification of personal data if processed incompletely or inaccurately, and request notification of the operation carried out in this context to the third parties to whom personal data has been transferred,
- Even if their personal data are processed in compliance with the Law and other relevant provisions, if the reasons requiring data processing no longer exist, to request erasure or destruction of their personal data, and to request notification of the operation carried out accordingly to the third parties to whom personal data has been transferred,
- To object to the processing, exclusively by automatic means of their personal data, which leads to an unfavourable consequence for the data subject,
- To request compensation for the damage arising from the unlawful processing of their personal data.

### **9.1.1. Cases Where Data Subject Cannot Claim Their Rights**

In accordance with Article 28 of the Law, the provisions of the Law shall not be applied in the following cases. Therefore, data subjects cannot claim their rights which are set forth in Article 9.1.1 of this Policy regarding such cases where:

- personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymised,
- personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, privacy of private life or personal rights are not violated or they are processed so as not to constitute a crime,
- personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned to maintain national defence, national security, public security, public order or economic security,

- personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.

In accordance with the second paragraph of Article 28 of the Law, data subjects cannot claim their rights which are provided in Article 9.1.1 of this Policy, excluding the right to demand compensation, in cases where personal data processing:

- is required for the prevention of a crime or crime investigation,
- is carried out on the data which is made public by the data subject,
- is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorised for such actions, in accordance with the power conferred on them by the law,
- is required for the protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues.

### **9.1.2.Enforcement of the Rights of Data Subject**

Data Subjects may deliver their claims regarding the rights provided in Article 9.1 of this Policy by filling out and signing the KVKK Data Subject Request Form which can be found on [www.pfizer.com.tr](http://www.pfizer.com.tr) and submitting it along with other documents enabling identification of the data subject to the address of Esentepe Mah. Büyükdere Cad. Levent 199, No:199, İç Kapı No: 106, Kat: 26, 34394, Levent, Şişli / İstanbul.

A third person can also submit request on behalf of the Data Subjects provided that the data subject grants such person power of attorney which must be certified by notary public.

Data Subjects must lodge their application in Turkish. In the Application Form, you are asked to provide the following information:

- Name, surname and signature,
- Turkish identity number for Turkish citizens; nationality for foreigners,
- Passport number or identification number, if any,
- Residential address or office address for correspondence,
- Electronic mail address, if any, and telephone and fax number,
- Subject of the request,
- Additional information and documents, if any.



### **9.1.3.Data Subject’s Right to Complain to the Board**

Pursuant to Article 14 of the Law, if the application is declined, the response is found unsatisfactory or the response is not given in due time, the Data Subject may file a complaint with the Board within thirty (30) days as of they learn about the response of Pfizer, or within sixty (60) days as of the application date, in any case.

### **9.2. Process of Responding to Applications by Pfizer**

Applications to Pfizer must be made only for the cases in which Pfizer is deemed as the controller under the Law. Such cases shall exist where Pfizer collects personal data directly from the concerning person or where the data sharing between Pfizer Group Companies and Pfizer is deemed as data transferring between one collector to another. Otherwise, if the applications are in relation to the personal data processing activities where Pfizer Group Company is deemed as the controller, they must be lodged to the relevant Pfizer Group Company, not to Pfizer.

In the event that data subject delivers their request to Pfizer in accordance with the procedure set forth in Article 9.1.3 of this Policy, Pfizer shall conclude the request depending on the nature of request no later than thirty (30) days and free of charge. However, if additional fee is provided for by the Board, Pfizer shall charge the applicant a fee which is determined by the Board. In accordance with Article 7 of the “Communique on Procedures and Principles of the Application to Data Controllers” which was published in the Official Gazette dated March 10, 2018 and numbered 30356, in the event that the Data Subject is provided with response in written form, the data controller can charge 1 Turkish Lira per page if the response is ten (10) pages long or more. If the response is given through a recording medium such as CD or memory stick, then the fee that Pfizer will demand shall not be more than the cost of such recording medium.

Pfizer may request information from the applicant in order to determine whether s/he is the data subject or not, and address questions regarding his/her application. Pfizer may refuse the application, explaining the grounds for refusal in cases where:

1. personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymised,
2. personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defence, national security, public security, public order, economic security, privacy of private life or personal rights are not violated or they are processed so as not to constitute a crime,

3. personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorised and assigned to maintain national defence, national security, public security, public order or economic security,
4. personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings or execution proceedings.
5. personal data processing is required for the prevention of a crime or crime investigation,
6. personal data processing is carried out on the data which is made public by the data subject,
7. personal data processing is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorised for such actions, in accordance with the power conferred on them by the law,
8. personal data processing is required for the protection of State's economic and financial interests with regard to budgetary, tax-related and financial issues,
9. the request of data subject potentially violates the rights and freedoms of other persons,
10. the request takes disproportionate effort,
11. the requested information is already made public.

## **10. OTHER DOMESTIC POLICIES OF PFIZER ON PROTECTION AND PROCESSING OF PERSONAL DATA**

Pfizer shall create sub-policies for the internal use regarding the protection and processing of personal data which are related to the rules provided for by this Policy.

## **11. MANAGEMENT OF THE POLICY OF PFIZER ON PROTECTION AND PROCESSING OF PERSONAL DATA**

Pfizer has built a management team to act in compliance with the Law and to ensure the Policy on Protection and Processing of Personal Data is enforced. Therefore, in order to ensure the implementation and management of this Policy and other policies set forth in Article 10 thereof within Pfizer, in accordance with the decision of the Corporate Management, Pfizer Data Governance Team has been formed of 4 persons: one data controller representative, one contact person, one IT expert and one lawyer. Duties of Pfizer Data Governance Team are as follows:

- To introduce and enforce basic policies and make changes, if necessary, regarding the protection and processing of personal data, and submit them to the Management of Pfizer for approval,

- To decide on how policies on protection and processing of personal data will be implemented and inspected, and submit the matters on intra-company transfers and facilitation of coordination to the Pfizer for approval,
- To determine actions to be taken in order to ensure compliance to the Law and the relevant legislation and submit them to the Management of Pfizer for approval, and communicate such actions to the Management of Pfizer so as to be supervised and facilitated coordination therein,
- To create awareness on protection and processing of personal data within Pfizer and in the institutions that Pfizer cooperates with,
- To ensure that Pfizer determines the risks involved in personal data processing activities, and to submit the suggestions for improvement to the Management of Pfizer for approval,
- To ensure that trainings are organised to inform data subjects on protection of personal data, implementation and dissemination of policies, personal data processing activities and legal rights of data subjects,
- To communicate the applications of data subjects to the Management of Pfizer so as to be finalized thereby,
- To follow the developments and regulations on protection of personal data, and to communicate suggestions on actions to be taken in Pfizer in accordance with those developments and regulations,
- To maintain relationship with the Board and the Authority in coordination with the Management of Pfizer,
- To carry out other duties assigned by the Company Management on protection of personal data.

## ANNEX 1- ABBREVIATIONS AND TERMS

**Law:** Law on Protection of Personal Data dated March 24, 2016 and numbered 6698 which was published in the Official Gazette dated April 7, 2016 and numbered 29677.

**Board:** the Personal Data Protection Board

**Authority:** the Personal Data Protection Authority

**Company:** Pfizer PFE İlaçları Anonim Şirketi

**Personal Data:** Any kind of information regarding an identified or identifiable natural person. Therefore, processing of personal data regarding legal entities is not within the scope of the Law. (e.g. name-surname, Turkish ID No, address, date of birth, credit card number etc.)

**Data Subject:** A natural person whose personal data are processed. (e.g. job candidates, doctors, Business Partners of Pfizer etc.)

**Sensitive Personal Data:** Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data.

**Processing of Personal Data:** Any operation carried out upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.

**Explicit Consent:** Specific, informed and freely given consent.

**Anonymisation:** Alteration of personal data personal data irretrievably and in a way it is no longer qualified as personal data. (e.g. rendering personal data impossible to link with a natural person using certain techniques such as masking, aggregation, data corruption etc.)

**Destruction:** Erasure, destruction or anonymisation of personal data.

**Processor:** The natural or legal person who processes personal data on behalf of the controller upon their authorization. (e.g. a cloud computing company storing the data of Pfizer etc.)

**Controller:** The person who determines the purposes and means of processing personal data and

manages the data registry system where data are kept systematically.

**Contact Person:** The real person notified by the data controller during registration to the Registry for the communication to be established with the Institution, regarding the obligations of legal entities resident in Turkey and the legal entity data controller representative who are not resident in Turkey within the scope of the Law and secondary regulations to be issued based on this Law.

**Third Party:** Any natural person whose personal data are processed within the scope of the Policy. (e.g. persons who report side effects etc.)

**Application Form:** Application form containing the application that data subjects made to claim their rights. It can be found on the website of Pfizer for the applications to the Controller made by the data subject or his/her representative in accordance with the Law.

**Pfizer Group Companies:** All the other companies that Pfizer İlaçları Limited Şirketi is associated with either directly or indirectly (associates, partners etc.) including. Pfizer PFE İlaçları A.Ş. and Pfizer Inc.

**Job Candidate:** Natural persons who applied for a job in Pfizer or submitted their résumé and relevant information to Pfizer.

**Executives and Employees of the Institutions That We Cooperate:** Stakeholders, executives and employees of the institutions that Pfizer maintains any kind of business relationship with (including but not limited to hospitals, ministries, consultants, associations).

**Supplier:** Natural or legal entities that supply Pfizer any service/product based on a contract when Pfizer carries out the business operations of Pfizer.

**Executives and Employees of Suppliers:** Stakeholders, executives and employees of the Suppliers.

**Business Partners:** Parties that Pfizer forms business partnership with in order to carry out business operations.

**Executives and Employees of Business Partners:** Stakeholders, executives and employees of the Business Partners.

**Health Care Professionals (“HCPs”):** Physician, dentist, pharmacist, nurse, midwife, optician and the other professions that are defined in additional article 13 of the Law numbered 1219 that Pfizer is in collaboration with in order to protect public health and inform the public.

**Patient:** Natural persons who are in need of medical services and use pharmaceuticals of Pfizer and/or participate in clinical researches/observational studies. (e.g. patients who report side effects)

**Visitor:** Natural persons who has physically been in and visited Pfizer Headquarters for various purposes.

**Website and Mobile Application Visitor:** Natural persons who visit the website of Pfizer.

**Pfizer Headquarters:** Headquarters of Pfizer which is located at the address of Esentepe Mah. Büyükdere Cad. Levent 199, No:199, İç Kapı No: 106, Kat: 26, 34394, Levent, Şişli / İstanbul.

**Executive:** Board members of Pfizer and other authorised natural persons.

**SSL:** Secure sockets layer. It is the certificate which enables the data security and integrity between server and client.

**Secure Electronic Signature:** An electronic signature which makes it possible to identify the signatory based on a qualified electronic certificate and which is created by a secure electronic signature tool that is exclusively linked to and in possession of the signatory, and determines whether a change has been made in a signed electronic data.

**Registered Electronic Mail (ERM):** A qualified form of electronic mail which provides legal evidence regarding the use of electronic messages including their transfer and delivery.

**Mobile Signature:** It is an electronic signature created using a mobile device.

