KİŞİSEL VERİLERİN KORUNMASI VE GİZLİLİK POLİTİKASI

A. KAPSAM

Kişisel Verilerin Korunması ve Gizlilik Politikası ("Politika"), kişisel verilerin işlenmesine yönelik kurallar bütününü açıklayarak gerekli bilgilendirmeleri yapmak amacıyla hazırlanmış olup, Akdeniz Onkoloji Radyoterapi ve Sağlık Hiz. Ltd. Şti. & Onko Ankara Onkoloji Merkezi Sağlık Hizmetleri Ltd. Şti. ("Şirket") Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.

B. TANIMLAR

Kişisel veri:	Kimliği belirli veya belirlenebilir her türlü bilgidir ve kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hallerini kapsar.
Özel nitelikli kişisel veri:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.
Açık rıza:	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim hale getirme:	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
Kişisel veri envanteri:	Şirketin iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdığı envanterdir.
Kişisel verileri işleme:	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 işlemdir. Verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türleri bu kapsama girmektedir.
Kişisel veri sahibi:	Kişisel verisi işlenen gerçek kişi
Veri kayıt sistemi:	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi

Veri sorumlusu:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri işleyen:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Kişisel Verilerin Korunması Kanunu ("KVKK"):	İşbu Politikaya konu olmakla birlikte, 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanan 24 Mart 2016 tarihli ve 6698 sayılı Kanun
Kurul:	Kişisel Verileri Koruma Kurulu
Kurum:	Kişisel Verileri Koruma Kurumu
Politika:	Kişisel Verilerin Korunması ve Gizlilik Politikası

C. DEĞİŞİKLİKLER

Kanun kapsamındaki ek mevzuatların yürürlüğe girmesi ile birlikte veya muhtelif zamanlarda işbu Politikada yapılacak olan değişiklikler Şirket'in kurumsal Internet sitesinden takip edilebileceği gibi, işbu Politikanın güncel versiyonuna yine bu kurumsal siteden ulaşılabilmektedir.

1 AMAÇ

Şirket, ürün ve hizmetlerini sunma faaliyetini gerçekleştirebilmek ve hizmetlerinin kesintisiz ilerleyebilmesini sağlamak adına, sözlü, yazılı ya da elektronik ortam üzerinden temin edebildiği kişisel verileri, Veri Sorumlusu sıfatıyla, hukuka uygun bir biçimde işlemektedir.

İşbu Politikanın amacı, Şirket'in yürüttüğü bu işleme faaliyetleri ve kişisel veriler ile ilgili sistemler konusunda açıklamada bulunarak ilgili kişileri bilgilendirmek ve böylece kişisel veriler hususunda şeffaflık sağlamaktır.

Bu bağlamda Şirket, KVKK kapsamında kişisel verilerin işlenmesini, bu işlemeye konu alınan veri sahiplerini ve bu kişilerin haklarını işbu Politikada detaylandırarak açıklamış bulunmaktadır.

2 KİŞİSEL VERİ

2.1 Kişisel Veri İşlemesine İlişkin Genel İlkeler

Şirket, KVKK'nın 4. maddesinin 2. fıkrası uyarınca ve işbu Politikanın **'Kişisel Verilerin İşlenme Amaçları'** bölümünde örneklendirilmiş olan amaçlar kapsamında, aşağıdaki ilkelere uygun olarak kişisel veri işlemektedir:

- Hukuka ve dürüstlük kurallarına uygun olma
- Doğru ve gerektiğinde güncel olma
- Belirli, açık ve meşru amaçlar için işlenme
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

2.2. Şirket Tarafından İşlenen Kişisel Veriler, İşleme Amaçları, Aktarımı, Toplama Kanalları, Saklama Süreleri ve Veri Sahibinin Hakları

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunmasını amaçlayan KVKK'nın "Veri Sorumlusunun Aydınlatma Yükümlülüğü" başlıklı 10. maddesi ile 10 Mart 2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ uyarınca veri sorumlusu sıfatıyla Şirket bünyesinde işlenen kişisel veriler hakkındaki Aydınlatma Metni internet sitemizdeki https://www.onko.com.tr/index.html linki üzerinde genel yer almaktadır.

3 KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEDBİRLER

3.1 Kişisel Veri Güvenliğine İlişkin İdari Tedbirler

3.1.1 Mevcut Risk ve Tehditlerin Belirlenmesi

Şirket, işlemekte olduğu kişisel verilere dair risk ve tehditleri belirlemek için sahip olduğu "Kişisel Veri Envanteri"nden yararlanır. Bu envanter içerisinde kişisel verilerin işlendiği süreçler Şirket tarafından güncel tutulacaktır.

Şirket söz konusu riskleri belirlerken, işlemekte olduğu kişisel verilerin özel nitelikli olup olmadığı, gerektirdiği gizlilik seviyesi ve ortaya çıkabilecek bir güvenlik ihlali sonucunda potansiyel zararın ne olacağını belirler.

3.1.2 Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Şirket, çalışanlarını kişisel verilerin korunması ve siber güvenlik ile ilgili olarak eğitimlere tabi tutar ve konu ile ilgili farkındalık çalışmaları gerçekleştirir.

Kişisel verilerin hukuka aykırı olarak açıklanması veya paylaşılması en sık görülen ihlallerden birini teşkil etmektedir. Bu tip ihlallerin önüne geçilmesi amacıyla Şirket tarafından;

- Kişisel veriler ile çalışan herkese bu konuda farkındalık eğitimleri verilir.
- Kişisel verilere ilişkin rol ve sorumluluklar, çalışanların iş tanımında açıkça belirlenir.
- Kişisel veriler ile ilgili olarak "yasaklanmadıkça her şey serbesttir" değil, "izin verilmedikçe her şey yasaktır" prensibi ile hareket edilmesi sağlanır.
- Çalışanların işbu Politika ve sair diğer politika ve prosedürlere uymaları sağlanır, uymama durumunda disiplin süreçleri devreye alınır.

3.1.3 Kişisel Verilerin Mümkün Olduğunca Azaltılması

Kanun ve sair mevzuatta öngörülen "kişisel verileri doğru ve gerektiğinde güncel tutma", "amacın gerektirdiği süre kadar muhafaza etme" gibi şartların yerine getirilebilmesi için Şirket;

- Uhdesinde bulunan kişisel verileri düzenli olarak tarayarak herhangi bir amaca hizmet etmeyen ve güncel olmayan verilerden gerekli olanları günceller, geri kalanını siler, yok eder ya da anonim hale getirir.
- İhtiyaç olmasına rağmen sık erişim gerektirmeyen kişisel verilerin daha güvenli ortamlarda muhafazası sağlanır.
- Yetkilendirmeler kontrol edilerek kişisel verilere sadece görmesi gereken pozisyonlarda çalışan kişilerin erişebilmesi sağlanır.

- Silme, yok etme ve anonimleştirme ile ilgili her türlü politika ve prosedürün güncel tutulması sağlanır ve bunlar sistemli olarak uygulanır.

3.1.4 Veri İşleyenler ile İlişkilerin Yönetimi

Şirket, bilgi teknolojileri ile ilgili hizmet alımlarında sözleşme düzenlediği veri işleyenlerin bilgi güvenliğine en az kendisi kadar önem verdiklerinden ve müşterek sorumluluğun bilinciyle hareket ettiklerinden emin olur ve bunu sözleşmesel olarak da güvenceye alır.

Veri işleyenler, mevzuattaki tanım ile paralel olarak yalnız Şirket'in talimatları doğrultusunda, Şirket ile akdedilmiş sözleşme çerçevesinde kalmak suretiyle ve mevzuata uygun olarak kişisel verileri işler. Veri işleyenler süresiz sır saklama yükümlülüğü altında tutulur.

Herhangi bir veri ihlali durumunda, durum derhal Şirket'e bildirilir ve bu durum sözleşmesel olarak da kayıt altına alınır. Şirket, bu tip veri ihlallerini mevzuat gereği olarak veri sahibi ilgililer ile Kurula bildirecektir.

Şirket ile veri işleyenler arasında akdedilecek sözleşmelerde, sözleşmenin niteliksel olarak elverdiği ölçüde ayrı bir madde olarak veri işleyene aktarılan veri kategorileri ve türleri belirtilir.

Şirket "Veri Sorumlusu" sıfatıyla veri işleyenin kişisel verini içeren sistemleri üzerinde gerekli denetimleri yapar veya yaptırır, denetim sonucunda ortaya çıkan raporları ve hizmet sağlayıcıyı yerinde inceleyebilir. Bu durum sözleşme içerisinde de karşılıklı olarak mutabakata bağlanır.

3.2 Kişisel Veri Güvenliğine İlişkin Teknik Tedbirler

3.2.1 Siber Güvenliğin Sağlanması

Şirket, siber güvenlik amacıyla gerekli yazılımları geliştirir ve gerekmesi halinde hizmet ve ürün alımı yapar.

Şirket, hâlihazırda sahip olduğu ürünleri düzenli olarak tarayarak gerekmeyen ve güncelliğini yitirmiş olan ürünlerin yüklü oldukları cihazlardan kaldırılmasını sağlar, halen gerekenlerin ise güncelliğini düzenli olarak kontrol eder ve güncel olduklarından emin olur. Şirket gerekli görmesi halinde yama yönetimi ile ilgili geliştirmeler yapar ya da ürün satın alır.

Kişisel veri içerir sistemlerine erişimin kontrollü olarak sağlanması amacıyla Şirket, erişim ve yetki yönetimini güncel tutar ve güvenli şifre kullanımı konusunda çalışanlarını bilgilendirir. Şirket bu amaçla bir "erişim ve yetki kontrol matrisi" ve erişime dair politika ve prosedürler oluşturur.

Şirket, şifre yönetimi ile ilgili olarak gerekli geliştirmeleri yapar ya da ürün satın alır. Bu amaçla belli sayıdan fazla şifre giriş denemesinin önlenmesi, düzenli olarak parola değiştirilmesinin sağlanması, parolaların güvenliğini yüksek seviyede tutacak karmaşıklıkta seçildiğinden emin olunması, iş akdine son verdiği çalışanların yetkilerinin zaman kaybetmeksizin kaldırılmasının sağlanması gibi konularda gerekli tedbirleri alacağını kabul ve beyan eder.

Şirket, ağları ve bilgisayarları düzenli olarak tarayarak tehlikeleri tespit eden antivirüs türevi yazılımların kullanıldığından emin olmak ve bunların güncelliğini sağlamak için gerekli tedbirleri alır.

Kişisel veri temininde Şirket ağı dışında kalan Internet sitelerinden yararlanıldığı durumlarda, söz konusu siteler ile bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirildiğinden emin olunması gerekmektedir.

3.2.2 Kişisel Veri Güvenliğinin Takibi

Kişisel veri güvenliğinin takibi amacıyla Şirket;

- Ağlarında hangi yazılım ve servislerin çalıştığının kontrolünü sağlar.
- Ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi amacıyla gerekli tedbirleri alır.
- Log yönetimi yapar.
- Güvenliğe dair ihlallerin hızlı bir şekilde raporlanması için çalışanların bilinçlendirilmesini sağlar ve buna dair bir "raporlama prosedürü" oluşturur. Bu raporlar sistem tarafından otomatik olarak oluşturulabilir ve sistem yöneticisi tarafından gerektiğinde ilgili birime konsolide edilerek sunulabilir.
- Kişisel verilerin sistemsel olarak güvenliğinin sağlanmasına dair her türlü raporlama aracının düzenli kontrolü ve uyarıların dikkate alınmasını sağlar.
- Düzenli olarak zafiyet taramaları ile sızma testi yapar veya yaptırır.
- Herhangi bir siber saldırı durumunda delillerin eksiksiz toplandığından ve güvenli bir şekilde saklandığından emin olur.

3.2.3 Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Şirket, kişisel verileri fiziksel ve mantıksal olarak tutmakta olduğu Genel Müdürlük, Arşiv, şubeler ve diğer yerlerde gerekli iç ve dış fiziksel güvenlik önlemlerini alır.

Şirket, bu önlemler kapsamında kişisel veri bulunduran yapıların deprem, yangın, sel gibi afetlere karşı korunmasını sağlar. Fiziksel ortamda tutulan kişisel verilerin güvenliği açısından, bunların bulunduğu yerlere giriş çıkışların kontrollü yapılması, ayrıca bu tip kişisel verileri işleyen çalışanların bilinçlendirilerek olası kayıp ve çalınma durumlarının önüne geçilmesini sağlar.

Şirket, kişisel veri ihlallerinin büyük bir kısmının kişisel veri içeren cihazların çalınması veya kaybolması sonucunda gerçekleştiğinin bilinciyle hareket eder ve bu durumun en aza indirgenmesi amacıyla gerekli tedbirleri alır. Bu tedbirler kapsamında erişim kontrolü yetkilendirmesi ve şifreleme yöntemleri gibi yollara başvurulabilir.

Şirket, şifreleme yöntemlerini kullanıyor olduğu durumlarda uluslararası kabul görmüş çözümlerden yararlanır ve asimetrik şifreleme yöntemlerinden yararlanılan durumlarda anahtar yönetimi süreçleri açısından gerekli tedbirleri alır.

3.2.4 Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

Şirket, BT sistemlerine yönelik tedarik, geliştirme ve bakım hizmetleri alımında güvenlik faktörünü ön planda tutmaya özen gösterir. Bu amaçla Şirket;

- Uygulama sistemleri üzerinden yapılacak olan kişisel veri girişlerinde, girilen kişisel verilerin veri bütünlüğünü bozmayacak şekilde çalıştığından emin olacak kontrol mekanizmalarının bulunduğundan emin olur.
- Kişisel veri içermekte olan, ancak bakım, arıza vb. bir nedenle tedarikçi 3. Kişi firmaya gidecek olan cihazların veri saklama ortamlarının gönderilmemesi sağlar, dışarıdan bir tedarikçi firma personeli Şirket'e gelmiş ise kurum dışına veri çıkmaması amacıyla gerekli önlemlerin alındığından emin olur.

3.2.5 Kişisel Verilerin Yedeklenmesi

Şirket, uhdesindeki kişisel verilerin güvenliğini sağlamak amacıyla bunların yedeğini ya da yedeklerini tutar.

Şirket, dosyaları şifreleyerek fidye talep eden kötü amaçlı yazılımlara (ransomware) yönelik veri yedekleme stratejileri geliştirir ve gerekli önlemleri alır.

Şirket, yedeklenen kişisel verilere sadece sistem yöneticisinin erişebildiğinden emin olur ve bu yedekleri ağ dışında saklar.

Şirket, söz konusu yedeklerin fiziksel güvenliklerine yönelik gerekli tedbirleri alır.

4 YÜRÜRLÜK VE GÜNCELLEMELER

İşbu Politika, Şirket Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girecektir. Politika, olağan olarak yılda bir defa gözden geçirilerek güncellenir. Ancak mevzuat değişiklikleri, atıf yapılan bir teknik standarttaki değişme, Kişisel Veri Koruma Kurulu'nun işlemleri ve/veya vereceği kararlar ile mahkeme kararları doğrultusunda Şirket bu Politikayı gözden geçirme ve gerekli durumlarda politikayı güncelleme, değiştirme veya ortadan kaldırıp yeni bir politika oluşturma hakkını saklı tutar. Politikanın yürürlükten kaldırılmasına ilişkin olarak karar verme yetkisi Şirket Yönetim Kurulu'na aittir.