TTGO TIP TEKNOLOJILERI GELIŞTIRME OFISI VE BILIŞIM BIYOMEDIKAL TURIZM LIMITED ŞIRKETI
KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1. İmha Politikasının Amacı

İşbu Kişisel Verileri Saklama ve İmha Politikası (**"Politika"**) TTGO Tıp Teknolojileri Geliştirme Ofisi ve Bilişim Biyomedikal Turizm Limited Şirketi (**"Şirket"**) olarak veri sorumlusu sıfatıyla elimizde bulundurduğumuz kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu (**"KVKK"**) ve ilgili yasal mevzuat uyarınca Şirket tarafından re'sen veya veri sahibinin talebi üzerine kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin Şirket tarafından uygulanacak usul ve esasların belirlenmesi amacıyla hazırlanmıştır.

Çalışanlarımıza, çalışan adaylarımıza, müşterilerimize, ziyaretçilerimize, yöneticilerimize, bayilerimize, işbirliği içerisinde olduğumuz, hizmet/ürün aldığımız ve/veya hizmet/ürün verdiğimiz şirketlerin çalışanlarına ve diğer üçüncü kişilere ait olup Şirketimiz nezdinde bulunan kişisel veriler bu Politika kapsamı dahildedir. Anılan kişilere ait kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika hükümleri uygulanacaktır.

2. Kişisel Verilerin Saklandığı Ortamlar

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda tutulabilir. Şirket her durumda veri sorumlusu sıfatıyla hareket etmekte ve kişisel verileri KVKK'ya, **Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikası**'na (ilgili politikaya www.solograce.com adresinden ulaşabilirsiniz) ve işbu Kişisel Verileri Saklama ve İmha Politikası'na uygun olarak işlemektedir ve korumaktadır.

Ortamların Güvenliğinin Sağlanması

Şirket, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli teknik ve idari tedbirleri almaktadır. Bu kapsamda Şirket personeli bilgilendirilmekte ve düzenli olarak güncel mevzuat kapsamında eğitim verilmektedir. Bilgisayar sistemleri kapalı devredir.

İşbu tedbirler, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

3.1. Teknik Tedbirler

Şirket, işlediği kişisel verilerle ilgili olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri yapılmakta, yapılan testlerin sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.

- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.
- Görev değişikliği yapılan veya işten çıkarılan personelin bu alandaki yetkileri kaldırılmaktadır.
- Şirket bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurulmakta ve/veya sözleşmeli firmalar tarafından teknik hizmet alınmaktadır.

2.2 İdari Tedbirler

Şirket, işlediği kişisel verilerle ilgili olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Şirket çalışanlarının veri güvenliği ve kişisel verilerin gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için belli aralıklarla çalışmalar yapılmaktadır.
- Veri güvenliği alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Kişisel veri güvenliği sorunları raporlanmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokol imzalanmakta ve/veya ilgili üçüncü kişilerden gizlilik yükümlülüklerine uyması için taahhüt alınmaktadır.

2.3 Şirket İçi Denetim

Şirket, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Politika ile Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikası hükümlerinin uygulanmasına ilişkin Şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da sair bir şekilde Şirket sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, Şirket bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.

3. Saklama ve İmha Nedenleri

Şirket bünyesinde tutulan kişisel veriler KVKK ve Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikamız uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

Şirket bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da KVKK'nın 5'inci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde işbu Politika uyarınca **silinir, yok edilir veya anonim hale getirilir.**

Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler aşağıdakilerden ibarettir:

- Kanunlarda açıkça öngörülmesi.
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

4. İmha Yöntemleri

Şirket, KVKK'ya ve sair mevzuat ile Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikası'na uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Politika'da belirtilen süreler içinde re'sen siler, yok eder veya anonim hale getirir.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

5.1. Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri
Karartma: Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilmesi şeklinde yapılır.

Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri
Yazılımdan güvenli olarak silme: Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

5.2. Yok Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri
Fiziksel yok etme: Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.

Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri
Fiziksel yok etme: Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, kullanılamaz halde fiziksel zarar verilmesi (delme , kırma), yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, kullanılamaz halde fiziksel zarar vermek (delme , kırma), toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.
De-manyetize etme (degauss): Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
Üzerine yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.

Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri
Yazılımdan güvenli olarak silme: Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

5.3. Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri çıkarma: İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da bir kaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.

Bölgesel gizleme: Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.

Genelleştirme: Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.

Alt ve üst sınır kodlama/Global kodlama: Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategori edilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategori edilir. Aynı kategori içinde kalan değerler birleştirilir.

Mikro birleştirilme: Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.

Veri karma ve bozma: Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

Şirket, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. Şirket, bu anonimleştirme yöntemlerini kullanırken K-Anonimlik (K-Anonymity), L-Çeşitlilik (L-Diversity) ve T-Yakınlık (T-Closeness) istatistik yöntemlerini kullanabilir.

5. Saklama Süreleri

Veri Sahibi	Veri Kategorisi	Saklama Süresi
Çalışan	Çalışan kimlik bilgisi, özlük bilgisi, iletişim bilgisi, hukuki iletişim bilgisi, maaş bilgisi, meslek deneyim bilgisi ve alınan eğitimler, çalışan performans ve uyum bilgisi, ceza mahkumiyeti ve güvenlik, iş kıyafet ölçüleri, yan haklar bilgisi, finans bilgileri, lokasyon verileri, araç/plaka bilgileri, lokasyon bilgisi.	İş sözleşmesinin bitmesinden itibaren 10 yıl.
Çalışan	Donanımsal ve yazılımsal erişim süreçleri ile elde edilen veriler.	İş sözleşmesinin bitmesinden itibaren 2 yıl.
İş Ortağı/Çözüm Ortağı/Danışman	İş Ortağı/Çözüm Ortağı (Bayi/Franchise/Tedarikçi)/Danışman ile Şirket arasındaki iş ilişkisinin/ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, bunların çalışanlarına ait veriler.	İş Ortağı/Çözüm Ortağı/ (Bayi/Franchise/Tedarikçi)/Danışman ile Şirket arasındaki iş ilişkisi/ticari ilişki süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md. 146 ile Türk Ticaret Kanunu md. 82 uyarınca 10 yıl.
İnternet Sitesi Ziyaretçisi	İnternet sitesi ziyaretçisine ait ad, soyad, e-posta adresi, çerezler ve log kayıtları.	6 ay, en fazla 2 yıl süre ile saklanır. Çevrimiçi ziyaretçilere ilişkin bilgiler 2 yıl saklanır.

Ziyaretçi	Şirket internet ağının kullanılması, internete giriş ve uzaktan bağlantı esnasında işlenen trafik bilgileri; IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri vb. veriler.	2 yıl.
Ziyaretçi	Çağrı merkezi aramalarında alınan ses kayıtları.	2 yıl.
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler.	Söz konusu pozisyon için işe alım bittiğinde ilgili cv ve özgeçmişler imha edilmektedir. Daha sonra açılacak pozisyonlarda değerlendirmeleri için CV'lerini ve özgeçmişlerini saklamak konusunda adaylardan izin alındığı taktirde, ilgili veriler 1 sene saklanmaktadır.
Stajyer	Stajyere ait staj dosyasında yer alan bilgiler.	Staj ilişkisinin bitimini takip eden takvim yılbaşından itibaren 10 yıl.
Müşteri	Müşteri'ye ait ad, soyad, iletişim bilgileri, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri.	Müşteri'nin satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md. 146 ile Türk Ticaret Kanunu md. 82 uyarınca 10 yıl.
Müşteri	Müşteri kamera görüntüleri, araç plaka bilgisi.	2 yıl.
Potansiyel Müşteri	Potansiyel müşteri ile Şirket arasındaki ticari ilişkinin kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler.	2 yıl.
Tüketici	Şirket'in tüketiciler ile akdettiği mesafeli satış sözleşmeleri aracığı ile elde ettiği veriler.	3 yıl.
Şirket/Şahıs Şirketi	Hukuki İşlem.	Hukuki işlemin sona ermesini takip eden 10 yıl.
Müşteri/Tedarikçi/Franchise	Sözleşmelerin hazırlanması.	Sözleşmenin sona ermesini takip eden 10 yıl.

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

6. İmha Süreleri

Şirket, KVKK, ilgili mevzuat, Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikası ve işbu Politika uyarınca sorumlu olduğu kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanunun 13'ncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. Şirket'in talebi almış sayılması için ilgili kişinin talebini **Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikasına** uygun olarak yapmış olması gerekir. Şirket, her halde yapılan işlemle ilgili ilgili kişiye bilgi verir.
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

7. Periyodik İmha

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

8. İmha İşleminin Hukuka Uygunluğunun Denetimi

Şirket, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Gizlilik Politikasına ve işbu Politika'ya uygun olarak yapar. Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

9. Teknik Tedbirler

- Şirket, işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
- Şirket, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- Şirket, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
- Şirket, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

10. İdari Tedbirler

- Şirket, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel verilerin gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- Şirket, bilgi güvenliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- Şirket, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- Şirket, imha işlemlerinin hukuka ve işbu Politikada belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- Şirket, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

11. Kişisel Veriler ve Uyumluluk

İşbu Politikanın uygulanmasından, başta İnsan Kaynakları Departmanı/Birimi olmak üzere, kişisel veri işleyen her bir birim ve departman bizzat sorunludur. Hukuk danışmanları ilgili kanunların takibi,

yorumlanması ve KVKK süreçlerinin hukuki takibinin yapılması konularında rehber ve danışman konumundadır.

12. Güncelleme ve Uyum

Şirket, KVKK'da yapılan değişiklikler nedeniyle, KVK Kurul kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda Kişisel Verilerin İşlenmesi, Korunması ve Gizliliği Politikasında ya da işbu Politikada değişiklik yapma hakkını saklı tutar.

İşbu Politika'da yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar Politikanın sonunda açıklanır.
Son Güncelleme Tarihi: 04 Nisan 2024