

# KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

## İÇİNDEKİLER

BİYOTEM HAKKINDA.....	2
KİŞİSEL VERİ İŞLEME İLKELERİ.....	2
İLGİLİ KİŞİ KATEGORİLERİ.....	3
NE ZAMAN KİŞİSEL VERİ TOPLARIZ?.....	3
ÇALIŞAN ADAYLARININ KİŞİSEL VERİLERİNİN İŞLENMESİ.....	3
ZİYARETÇİLERİN KİŞİSEL VERİLERİNİN İŞLENMESİ.....	3
KAPALI DEVRE KAMERA KAYDI YOLUYLA KİŞİSEL VERİLERİN İŞLENMESİ.....	4
KİŞİSEL VERİLERİ HANGİ AMAÇLARLA KULLANIYORUZ?.....	4
KİŞİSEL VERİLERİ HANGİ HUKUKİ SEBEPLERLE İŞLİYORUZ?.....	6
KİŞİSEL VERİLERİ NE ZAMAN PAYLAŞIRIZ?.....	7
KİŞİSEL VERİLERİ NE KADAR SÜREYLE SAKLARIZ?.....	8
KİŞİSEL VERİLERİ NASIL İMHA EDİYORUZ?.....	9
KİŞİSEL VERİLERİ NASIL KORUYORUZ?.....	17
KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HAKLARINIZ NELERDİR?.....	20
İLGİLİ KİŞİLERİN HAKLARINI İLERİ SÜREMEYECEĞİ DURUMLAR NELERDİR?.....	22
EK – KISALTMALAR.....	23

Biyotem olarak kişisel verilerin korunması ve özel hayatın gizliliği konularına önem veriyoruz. Ticari faaliyetlerimizi yerine getirirken müşterilerimiz, tedarikçilerimiz, iş ortaklarımız, bunların çalışanları ve yetkilileri ve diğer tüm üçüncü kişilere ait elde ettiğimiz kişisel verileri hukuka uygun toplamakta, depolamakta ve saklama amacı ortadan kalktıktan sonra imha etmekteyiz.

İşbu Politika’da kullanılan tüm tanım ve ifadeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK”) ve ikincil mevzuatta kendilerine atfedilen anlamları ifade edecektir. Bu Politika’daki “siz” ifadesi şahsınızı ifade etmektedir. Kişisel veri kavramı, hem genel hem de özel nitelikli kişisel veriyi kapsayacak şekilde kullanılmaktadır. Politika’daki terim ve kısaltmaları EK – Kısaltmalar bölümünde ayrıntılı olarak inceleyebilirsiniz.

## **BİYOTEM HAKKINDA**

Kayıtlı merkez adresi Sağlık Mahallesi Marmara Sk. No: 16/12-13-14 Sıhhiye/Çankaya Ankara olan ve Ankara Ticaret Sicil Odası’na 225835 sicil numarası ile kayıtlı olan Biyotem Sağlık Malzemeleri ve Hizmetleri Pazarlama Turizm Anonim Şirketi (“**Biyotem**” veya “**Şirket**” veya Politika’da “biz” olarak ifade edilecektir.), Politika’daki kişisel veri işleyen veri sorumlusu olarak düşünülmelidir.

Biyotem, teşhis ve tedavide kateterin kullanıldığı her alanda; nefroloji, girişimsel radyoloji, üroloji, gastroentoloji, kardiyoloji, nöroloji, onkoloji, hematoloji ve kalp ve damar cerrahisi gibi dallarda sağaltım pazarına günün en ileri teknolojisinin ürünlerini sunmaktadır. Nefroloji, hemodiyaliz ve onkoloji ürünleri, Biyotem kuruluşlarının çalışma alanında her zaman önemli bir konumdadır. Bu sağaltım dalında da, Biyotem günümüzün hasta memnuniyeti açısından en yararlı, en gelişmiş ürünlerini ve hizmetlerini, sayın hekimlerimizin kullanımına sunar.

## **KİŞİSEL VERİ İŞLEME İLKELERİ**

Biyotem tarafından işlenen tüm kişisel veriler, KVKK ve ilgili mevzuatlara uygun şekilde işlenmektedir. KVKK’nın 4. maddesinde düzenlenen kişisel veri işleme ilkeleri kişisel veri işleme sırasında esas aldığımız ilkelerdir. Bu ilkeler aşağıdaki gibidir:

- **Hukuka ve Dürüstlük Kuralına Uygun İşleme:** Şirketimiz, kişisel verilerin işlenmesinde hukuksal düzenlemelerle getirilen ilkeler ile genel güven ve dürüstlük kuralına uygun hareket etmektedir. Bu kapsamda Şirketimiz, kişisel verilerin işlenmesinde orantılılık gerekliliklerini dikkate almakta, kişisel verileri amacın gerektirdiği dışında kullanmamaktadır.
- **Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olmasını Sağlama:** Biyotem, İlgili kişilerin (ilgili kişilerin) temel haklarını ve kendi meşru menfaatlerini dikkate alarak işlediği kişisel verilerin doğru ve güncel olmasını sağlamaktadır.
- **Belirli, Açık ve Meşru Amaçlarla İşleme:** Şirketimiz, meşru ve hukuka uygun olan kişisel veri işleme amacını açık ve kesin olarak belirlemektedir. Şirketimiz, kişisel verileri sunmakta olduğu ürün ve hizmetler ile bağlantılı olarak kişisel veri işlemektedir.
- **İşleme Amaçları ile Bağlantılı, Sınırlı ve Ölçülü Olma:** Biyotem, kişisel verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işlemekte ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınmaktadır.
- **İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç için Gerekli Olan Süre Kadar Muhafaza Etme:** Şirketimizin yukarıdaki ilkelere uygun hareketlerine rağmen yükümlülükleri sona ermez. Toplanan ve depolanan kişisel veriler, ancak ilgili mevzuatta belirtildiği veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmektedir. Biyotem, mevzuat düzenlemelerinde öngörülmüş olan

ve kişisel veri saklamaya imkan tanıyan düzenlemelere uygun hareket eder. Kanuni saklama süreleri dolduktan sonra kişisel verileri vakit kaybetmeksizin siler, imha eder veya anonim hale getirir.

## İLGİLİ KİŞİ KATEGORİLERİ

Şirketimiz tarafından kişisel verileri işlenen çalışanlar, stajyer ve alt işveren çalışanları da dahil olmak üzere, dışındaki ilgili kişilerin kategorileri aşağıdaki tabloda yer almaktadır. Çalışanlarımızın kişisel verilerinin işlenmesine ilişkin ayrı bir politika oluşturulmuş ve şirket içinde uygulamaya alınmıştır. Aşağıdaki kategorilerin dışında yer alan kişiler de KVKK kapsamında Şirketimize taleplerini yöneltebilecek olup; bu kişilerin talepleri de değerlendirmeye alınacaktır.

İLGİLİ KİŞİ KATEGORİSİ	AÇIKLAMA
<b>Müşteri</b>	Ürün ve mallarımızı satın alan gerçek ya da tüzel kişilerdir.
<b>Potansiyel Müşteri</b>	Ürünlerimizi satın alma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek veya tüzel kişiler.
<b>Ziyaretçi/ Üçüncü Kişi/ Çalışan Adayı</b>	Şirketimizin sahip olduğu veya bir organizasyon gerçekleştirdiği fiziksel tesislerine ve şubelerine (ofisler vb.) çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler; şirketimizin sözleşmesel ilişki içerisinde bulunmadığı üçüncü kişiler ile şirketimiz ile iş sözleşmesi amacıyla Biyotem'e başvuran çalışan adayları bu kapsamdadır.

## NE ZAMAN KİŞİSEL VERİ TOPLARIZ?

Kişisel verileri aşağıdaki durumlarda toplarız:

- Ürünlerimizi satın alındığında;
- Ürün ve hizmet tedarik ettiğimiz zamanlarda;
- Tanıtım amaçlı bültenlerimize abone olduğunuzda,
- Bizimle e-posta ya da telefon gibi araçlar vasıtasıyla şikayet ya da geri bildirim iletmek için iletişime geçtiğinizde,
- Biyotem'e iş başvurusu yaptığınızda,

## ÇALIŞAN ADAYLARININ KİŞİSEL VERİLERİNİN İŞLENMESİ

Çalışan adaylarından gelen iş başvuruları çerçevesindeki özgeçmiş bilgileri, dış hizmet aldığımız istihdama ilişkin danışmanlık şirketleri veya Biyotem tarafından sağlıklı değerlendirmelerin yapılabilmesi için insan kaynakları süreç ve prosedürleri de takip edilerek işlenmektedir.

Çalışan adayları, iş başvurusu yaparken kişisel verilerini iletmeden önce ayrı bir belge ile KVKK'ya uygun bir şekilde detaylı olarak aydınlatılmakta ve gerekli durumlarda kişisel veri işleme faaliyetleri için açık rızaları alınmaktadır.

## ZİYARETÇİLERİN KİŞİSEL VERİLERİNİN İŞLENMESİ

Şirket merkezine ve şubelerine gelen ziyaretçilerin giriş-çıkış sırasında Şirketimizin, çalışanlarımızın ve ziyaretçilerimizin fiziki güvenliğinin sağlanması, işyeri kurallarının denetlenmesi amaçlarıyla kişisel

veriler işlenmektedir. Bu kapsamda ziyaretçi giriş çıkış takibi amacıyla ziyaretçilerimizin isim – soy isim ve TC kimlik numaraları kimlikleri ile teyit edilerek ziyaretçi defterine not edilebilmektedir. Ancak ziyaretçi şirket içinde bulunduğu süre boyunca kimliği tutulmamakta, ziyaretçi defterine bahsedilen kayıt yapıldıktan sonra kimlik ziyaretçiye geri verilmektedir.

Ziyaretçi, bilgileri alınmadan önce güvenlik girişinde yer alan bir aydınlatma metni ile kişisel verilerinin işlenmesine ilişkin aydınlatılmaktadır. Ancak bu kapsamda şirketimizin meşru menfaati bulunduğu için KVKK m. 5/2/f uyarınca ziyaretçinin açık rızası alınmamaktadır. Bu veriler, sadece fiziki olarak ziyaretçi kayıt defterinde tutulmakta ve şirket güvenliğini tehdit eden şüphe yaratacak bir durum olmadıkça başka bir ortama aktarılmamaktadır. Ancak suçun önlenmesi, şirket güvenliğinin sağlanması gibi durumlarda bu bilgiler kullanılabilir.

## **KAPALI DEVRE KAMERA KAYDI YOLUYLA KİŞİSEL VERİLERİN İŞLENMESİ**

Şirketimizin ve tesislerimizin güvenliğinin sağlanması amacıyla güvenlik kameraları kullanılmaktadır. Biyotem, güvenlik kamerası ile izleme faaliyeti kapsamında, şirket fiziki yerleşkelerinin ve şirket içinde bulunan kişilerin can ve mal güvenliğini sağlamak, suistimalleri önlemek gibi amaçlar mevcuttur.

Biyotem tarafından güvenlik kameraları ile yapılan kişisel veri işleme faaliyetleri, Anayasa'ya, KVKK'ya, ve ilgili mevzuata uygun bir biçimde yürütülmektedir.

Biyotem, KVKK m. 4'e uygun olarak, kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü bir biçimde işlemektedir. Kişinin mahremiyetini güvenlik amaçlarını aşan şekilde müdahale sonucu doğurabilecek şekilde izlemeye tabi tutulmamaktadır. Bu kapsamda CCTV kaydı yapılan ortak alanlarda uyarı levhaları yerleştirilerek ilgili kişiler bilgilendirilmektedir. Ancak Şirketimizin CCTV kayıtlarının tutulmasında meşru menfaatinin mevcut olması sebebiyle açık rızaları alınmamaktadır. Ayrıca KVKK m. 12'ye uygun olarak, CCTV izleme faaliyeti sonucunda elde edilen kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır.

Bunun yanında CCTV kamerası bulunan alanlara, kameraların izleme alanlarına, kayıtların tutulma sürelerine ilişkin bir prosedür hazırlanmış ve Şirketimizde uygulama alınmıştır. CCTV kamerası yerleştirilmeden önce bu prosedür dikkate alınmakta ve kamera daha sonra yerleştirilmektedir. Güvenlik amacını aşan ve kişilerin mahremiyetini aşan ölçüde kamera yerleştirilmesine izin verilmemektedir. CCTV kamera görüntülerine yalnızca belli sayıda Şirket personeli erişmekte ve bu yetkiler düzenli olarak gözden geçirilmektedir. Bu kayıtlara erişimi olan personel, kişisel verileri hukuka uygun bir şekilde koruyacaklarına ilişkin taahhüname imzalamaktadır.

Şirket merkez adresimiz, şubelerimiz ve bayiliklerimiz içerisindeki giriş kapıları, bina dış cephesi ve ziyaretçi bekleme salonları gibi tesislerimizde bulunan toplam 10 adet güvenlik kamerası vasıtasıyla görüntü kaydı yapılmakta ve kayıt işlemi tarafımızca denetlenmektedir.

## **KİŞİSEL VERİLERİN KULLANILMA AMAÇLARI**

Kişisel verileri kullanım amaçlarımız, aramızdaki iş ilişkisinin türüne (Örn. müşteri, çalışan, iş ortağı vb.) göre değişiklik göstermektedir. Temel olarak kişisel verileri işleme amaçlarımız aşağıda yer almaktadır.

## **Kişisel veri işleme amaçları**

Potansiyel tedarikçi/iş ortaklarını değerlendirme

Müşteri ilişkilerinin kurulması ve yönetimi, Tedarikçi/iş ortaklarımızla sözleşme sürecinin yürütülmesi ve sonuçlandırılması

Yasal yükümlülüklere uyum

Şirket menfaatlerinin korunması ve güvenliğinin sağlanması

## **Örnekler**

Risk kurallarımız gereği inceleme ve çıkar çatışması sürecimizin yürütülmesi

Şirketimizin sunduğu mal ve hizmetlerin satış işlemlerinin gerçekleştirilmesi, teklif sunulması, mal tedariki, faturalandırma, sözleşme kurulması ve ifa edilmesi, sözleşme sonrası hukuki işlem güvenliğinin sağlanması, mal ve numune sevkiyatının sağlanması, lojistik süreçlerin yönetilmesi, ürün ve hizmet geliştirmek, yeni teknoloji ve uygulamaların değerlendirilmesi ile Şirketimizin ticari ve iş stratejilerinin belirlenmesi ve uygulanması, operasyonların yönetilmesi (talep, teklif, değerlendirme, sipariş, bütçelendirme, sözleşme), ürün/proje/imalat/yatırım kalite süreçleri ve operasyonları, finans operasyonları, mali işlerin yönetilmesi, ticari ilişki içerisinde olduğu tüzel/gerçek kişilere alternatifler sunabilmek

Vergi ve sigorta süreçlerinin yürütülmesi, 5651 sayılı Kanun ve sair mevzuat, 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve sair mevzuat, 5237 sayılı Türk Ceza Kanunu ve 6698 sayılı Kişisel Verilerin Korunması Kanunu başta olmak üzere, ilgili mevzuattan kaynaklanan yasal yükümlülüklerimizin yerine getirilmesi, resmi kurumlar nezdindeki süreçlerin yürütülmesi, kayıt tutma ve bilgilendirme yükümlülükleri, uyum ve denetim, resmi mercilerin denetim ve teftişleri, yasal haklarımızın ve davalarımızı takibi ve sonuçlandırılması, resmi mercilerin talebi üzerine veri ifşası gibi tabi olduğumuz kanun ve düzenlemelere uyum kapsamında gerekli süreçlerin yürütülmesi, düzenleyici ve denetleyici kurumlarla, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde KVKK'da belirtilmiş yasal yükümlülüklerin yerine getirilmesini sağlamak üzere belirlenmiş gereklilik ve zorunluluklar kapsamında,

Şirket çıkarlarının ve menfaatlerinin korunması için gerekli denetim faaliyetlerinin yürütülmesi, çıkar çatışması kontrollerinin yapılması, Şirketimizle iş ilişkisinde olan kişilerin hukuki ve ticari güvenliğinin temini, şirket cihaz ve varlıklarının korunması için CCTV kayıtlarının tutulması, teknik ve idari güvenlik önlemlerinin alınması, sunduğumuz hizmetlerin geliştirilmesi için gerekli çalışmaların yürütülmesi, işyeri kurallarının uygulanması ve denetlenmesi, kalite süreçlerinin yönetilmesi, sosyal sorumluluk aktivitelerinin planlanması ve icrası, kaza, şikayet, kayıp çalıntı vb. durumların raporlanarak gerekli müdahalenin yapılması ve önlem alınması, bakım ve onarım yapılması sırasında oluşabilecek tehlikeli durumlar için uyulması gereken kuralların aktarılması ve taşeronların mesleki yeterliliklerinin ölçülmesi, firma çalışanlarının giriş ve çıkışlarının düzenini sağlamak ve güvenlik açısından gerekli bilgileri edinmek, gerekli kalite ve standart denetimlerimizi yapabilmek ya da kanun ve yönetmelikler ile belirlenmiş raporlama ve sair yükümlülüklerimizin yerine getirilmesi, tedarikçilerin sahaya kabulünün uygunluğunun değerlendirilmesi

**Kişisel veri işleme amaçları****Örnekler**

Şirket ticari faaliyetlerinin planlanması ve icrası

Şirket'in kısa, orta ve uzun vadede ticari politikalarının tespit edilmesi, planlanması ve uygulanması, ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Şirketimiz tarafından yürütülen iletişim, pazar araştırması ve sosyal sorumluluk aktiviteleri, satın alma, gümrük işlemlerinin yürütülmesi, ithalat ihracat operasyonlarında serbest dolaşıma girmiş eşyanın nakliyesinin organizasyonu,

Hak ve menfaatlerin korunması

Şirketimiz aleyhine açılan dava, soruşturma vb. hukuki hak taleplerine karşı savunma

**KİŞİSEL VERİLERİ İŞLEME HUKUKİ SEBEPLERİ**

Kişisel verileri başta 6102 sayılı Türk Ticaret Kanunu, 6098 sayılı Türk Borçlar Kanunu, 213 sayılı Vergi Usul Kanunu, elektronik ticaret mevzuatı olmak üzere KVKK m. 5'te düzenlenen aşağıdaki hukuki sebeplere dayanarak işliyoruz:

**Hukuki Sebep****Örnekler**

KVKK ve sair mevzuat uyarınca açık rıza almamız gereken durumlarda rızaya dayanarak işlemekteyiz.

Sağlık verisi işlemek için rıza alıyoruz.

Geçerli mevzuatın izin verdiği herhangi bir durumda

Vergi Usul Kanunu m. 230 kapsamında fatura üzerinde ilgili kişinin adına yer verilmesi

Herhangi bir kişinin hayati önem taşıyan menfaatlerini koruma zorunluluğu olduğunda

Baygınlık geçiren çalışanın sağlık bilgisinin kendi menfaati ve fiziki bütünlüğü için doktora verilmesi

Sözleşme kurmamız, sözleşmenin ifa edilmesi ve yükümlülüklerimizi bir sözleşme kapsamında yerine getirmemiz gereken durumlarda

Müşteri ile sözleşmesel ilişki kapsamında müşterinin banka hesap bilgilerinin alınması

Hukuki yükümlülüklerimizi yerine getirme

Vergisel yükümlülüklerimizin yerine getirilmesi, mahkeme kararıyla talep edilen bilgilerin mahkemeye sunulması

Kişisel verilerin alenileştirilmiş olması halinde

Sizinle iletişime geçmemiz için bize e-posta göndermeniz, çalışan adayının iletişim bilgilerini iş başvurusu toplanan internet sitesine yazması, sosyal medya kanalları gibi vasıtalarla sizin alenileştirdiğiniz kişisel verilerin alenileştirilme amacı çerçevesinde kullanılması

## **Hukuki Sebep**

Bir hakkın tesisi veya korunması için veri işlememizin zorunlu olması, hukuki haklarımızı kullanma ve aleyhimize açılan hukuki taleplere karşı savunma yapma

Temel hak ve özgürlüklere zarar vermemek koşulu ile meşru menfaatimiz çerçevesinde

## **Örnekler**

İspat/delil niteliğinde olan belgelerin saklanması ve gerektiğinde kullanılması

Şirket iletişim ağlarımızın ve bilgilerimizin güvenliğini sağlamak, Şirket faaliyetlerimizi yürütmek, şüpheli işlemleri tespit etmek ve risk kurallarımıza uyum amacıyla araştırma yapmak, teknik ve güvenlik açısından IT hizmetlerinin sağlanması amacıyla depolama, barındırma, bakım, destek hizmetlerinden yararlanmak, Şirket faaliyetlerimizin verimliliğini sağlamak ve teknolojinin imkanlarından yararlanmak için bulut teknolojisinden faydalanmak

Kişisel verilerin açık rıza ile işlendiği hallerde, açık rızanın geri alınması durumlarında söz konusu kişisel veri işleme süreci sonlanacak olup kanunda öngörülen asgari saklama sürelerinin de dolmasıyla ilgili kişisel veriler silinecektir.

## **KİŞİSEL VERİLERİN PAYLAŞIMI**

### **Yurtiçinde kişisel verilerin aktarımı**

Biyotem, kişisel veri aktarılması konusunda başta KVKK m. 8 olmak üzere KVKK'da öngörülen ve Kurul tarafından alınan karar ve ilgili düzenlemelere uygun bir şekilde hareket etmektedir. Kural olarak Şirketimiz tarafından ilgili kişilere ait kişisel veriler ve özel nitelikli veriler ilgili kişinin açık rızası olmadan başka gerçek kişilere veya tüzel kişilere aktarılamaz.

Ayrıca, KVKK'nın 5. ve 6. maddelerinde öngörülen durumlarda ilgilinin rızası olmaksızın da aktarım mümkündür. Biyotem, kişisel verileri KVKK'da ve ilgili diğer mevzuatta öngörülen şartlara uygun olarak ve mevzuatta belirtilen güvenlik önlemlerini alarak; (şayet veri sahibi kişi ile imzalı mevcut bir sözleşme var ise, söz konusu sözleşmede) KVKK veya ilgili diğer mevzuatta aksi düzenlenmediği sürece Türkiye'de bulunan üçüncü kişilere aktarabilir.

### **Yurtdışına kişisel veri aktarımı**

Biyotem, iş faaliyetleri ve ticari ilişkileri gereğince yurtdışına herhangi bir veri aktarımı yapmamaktadır.

KVKK m. 9 uyarınca kural olarak kişisel verilerin yurt dışına aktarımı için ilgili kişinin açık rızasını aramaktayız. Ancak KVKK m. 9 uyarınca, KVKK m. 5/2 ya da m. 6/3'te düzenlenen şartlardan birinin varlığı ve kişisel verilerin aktarılacağı yabancı ülkede

- Yeterli korumanın bulunması; ve
- Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarım yapılabilir.

### **Yurt içinde paylaşım yapılan taraflar**

Kişisel veriler ancak gerekli olan aşağıdaki amaçlar çerçevesinde paylaşılır. Bu durumlar haricinde kişisel verileri paylaşmamaya önem gösteriyoruz. Kişisel veri paylaşımı yaptığımız taraflar aşağıda yer almaktadır:

- **Hizmet sağlayıcılar ve iş ortakları:** Biyotem'in ticari faaliyetlerini yürütürken ürün satışı, satış sonrası desteği, gibi amaçlarla iş ortaklığı kurduğu tarafları tanımlamaktadır. Birçok işletme gibi, biz de bazı veri işleme faaliyetleri kapsamında işlevler ve hizmetlerin en verimli şekilde ve güncel teknolojilere uygun yürütülmesi için bilgi ve iletişim teknolojisi sağlayıcıları, danışmanlık hizmetleri sağlayıcılar, kargo şirketleri, seyahat acenteleri, bilişim ve teknoloji desteği, insan kaynakları danışmanlığı gibi güvenilir üçüncü şahıslarla çalışabilir ve bu kapsamda faaliyetlerimizi yürütmek için veri paylaşımında bulunabiliriz. Bu paylaşım iş ortaklığının kurulma ve ifa edilme amaçlarının yerine getirilmesini temin etme amacıyla sınırlı olarak yapılmaktadır. Şirketimizin faaliyetlerini en verimli şekilde yürütmek ve teknolojinin imkanlarından maksimum düzeyde faydalanmak için bulut bilişim teknolojileri kullanmakta ve bu kapsamda bulut bilişim hizmeti sunan firmalar aracılığı ile kişisel verilerinizi yurt içinde ve yurt dışında işleyebilmekteyiz.
- **Resmi merciler:** Kanunların gerektirdiği durumlarda veya haklarımızı korumamız gerektiğinde, kişisel verilerinizi ilgili resmi, adli ve idari merciler ile paylaşabiliriz (örn. Vergi daireleri, kolluk kuvvetleri, mahkemeler ve icra daireleri).
- **Özel hukuk kişileri:** İlgili mevzuat hükümlerine göre Şirketimizden bilgi ve belge almaya yetkili özel hukuk kişilerinin hukuki yetkisi dahilinde talep ettiği amaçla sınırlı olarak kişisel veri paylaşımı yapılabilmektedir (Örn. İş Sağlığı ve Güvenliği Şirketi).
- **Profesyonel danışmanlar:** Bankalar, sigorta şirketleri, denetçiler, avukatlar, mali müşavirler ve diğer danışmanlar gibi profesyonel danışmanlarla kişisel verilerinizi paylaşabiliriz.
- **Kurumsal işlemlerle bağlantılı diğer şahıslar:** Biyotem'in sahip olduğu bir işletmenin satışı, yeniden yapılanma, birleşme, ortak girişim ya da işimizin, varlıklarımızın veya hisselerimizin diğer türlü tasarruflar (herhangi bir iflas veya benzeri bir süreçle bağlantılı olanlar dahil) gibi kurumsal işlemlerin yürütülmesi için zaman zaman kişisel verilerinizi paylaşabiliriz.

### **KİŞİSEL VERİLER NE KADAR SÜREYLE SAKLANIR?**

Kişisel veriler, yalnızca toplandıkları amacı yerine getirmek için gerekli süre boyunca saklanır. Amaç ortadan kalktıktan sonra mevzuatta yer alan asgari saklama sürelerinin de sonlanmasından itibaren ilgili kişisel veriler KVKK'ya uygun şekilde imha edilir.

Kişisel verilerin imha sürelerini belirlerken aşağıdaki kriterler dikkate alınır:

- İlgili veri kategorisinin işleme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre;
- İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre;



- İlgili veri kategorisinin işleme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre;
- İlgili veri kategorisinin işleme amacına bağlı olarak saklanması yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre;
- Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı;
- Veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre; ve
- Veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi.

## **KİŞİSEL VERİLERİ NASIL İMHA EDİYORUZ?**

Türk Ceza Kanunu'nun 138. maddesi ve KVKK'nın 7. maddesi düzenlemesi doğrultusunda kişisel veriler ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde Şirketimizin kendi kararına istinaden veya kişisel veri sahibinin bu yönde bir talebi olması halinde silinir, imha edilir veya anonim hâle getirilir.

Bu kapsamda Kişisel Verileri Saklama ve İmha Politikası hazırlanmıştır. Biyotem'in ilgili mevzuat hükümleri gereğince kişisel verileri muhafaza etme hak ve/veya yükümlülüğü olan durumlarda veri sahibinin talebini yerine getirmeme hakkı saklıdır. Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlendiğinde, veriler silinirken/yok edilirken kişisel verinin sonradan kullanılmayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Şirketimiz, kendisi adına kişisel verileri işlemesi için bir kişi veya kuruluş ile anlaştağında, kişisel veriler bu kişi veya kuruluşlar tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir. Şirketimiz, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktağında kişisel verileri anonimleştirebilmektedir.

## **KİŞİSEL VERİ İMHA YÖNTEMLERİ**

### **Kişisel verilerin silinmesi**

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir. Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimizce, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirler alınır.

### Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

## Kişisel Verilerin Silinmesi Yöntemleri

<b>VERİ KAYIT ORTAMI</b>	<b>AÇIKLAMA</b>
<b>Sunucularda Yer Alan Kişisel Veriler</b>	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
<b>Elektronik Ortamda Yer Alan Kişisel Veriler</b>	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
<b>Fiziksel Ortamda Yer Alan Kişisel Veriler</b>	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
<b>Taşınabilir Medyada Bulunan Kişisel Veriler</b>	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Kişisel veriler, çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365 Salesforce, Dropbox gibi: Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

Kâğıt Ortamında Bulunan Kişisel Veriler: Kâğıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmelidir. 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 ilgili kullanıcılara görünmez hale getirilmesi şeklinde yapılır.

Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

### **Kişisel Verilerin Yok Edilmesi**

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri yok edebilir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

<b>VERİ KAYIT ORTAMI</b>	<b>AÇIKLAMA</b>
<b>Fiziksel Ortamda Yer Alan Kişisel Veriler</b>	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
<b>Optik / Manyetik Medyada Yer Alan Kişisel Veriler</b>	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süresi sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

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.

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.

Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

Karartma: Kişisel verilerin fiziksel olarak okunamayacak hale getirilmesidir.

### **Kişisel Verilerin Yok Edilmesi Yöntemleri**

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir:

**Yerel Sistemler:** Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir. i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerlerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir. ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz

haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Kati hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir. iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilir yok etme yöntemleri aşağıda yer almaktadır:

İ) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. iii) Manyetik bant: Verileri esnek bant üzerindeki mikro miknatis parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro miknatis parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir. Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir. Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir: i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi, ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı servis gibi üçüncü kurumlara gönderilmesi, iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

## **Kişisel Verilerin Anonim Hale Getirilmesi**

Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Biyotem, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya alıcı grupları tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. Şirketimiz, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almaktadır.

KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemler KVK Kanunu kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır.

### Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması, söz konusu kişisel verilerin geri dönülemez şekilde diğer verilerle eşleştirilememesi anlamına gelmektedir.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır. Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleyme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıdaki açıklanmaktadır:

**Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri:** Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar.

### Değişkenleri Çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

### Kayıtları Çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satirin çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır. Örneğin anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edilmiş olsun. Böyle bir durumda tüm anket sonuçlarından “sektör” değişkenini çıkartmaktansa sadece bu kişiye ait kaydı çıkartmak tercih edilebilir.

### Bölgesel Gizleme

Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer “bilinmiyor” olarak değiştirilir.

### ç. Genelleştirme

İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir. Örneğin TC Kimlik No 12345678901 olan bir kişi e-ticaret platformundan çocuk bezi aldıktan sonra aynı zamanda ıslak mendil de almış olsun. Yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan çocuk bezi alan kişilerin %xx’i aynı zamanda ıslak mendil de satın alıyor şeklinde bir sonuca ulaşılabilir.

### Alt ve Üst Sınır Kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

### Global Kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

### Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır. Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul’da yaşadığı bilinen bir kadına dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul’da yaşadığını bildiği bir kadının nüfus kaydının İstanbul’da olup olmadığını

tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

**Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri:** Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

#### Mikro Birleştirme

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. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

#### Veri Değiş Tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiflerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirilerek veri tabanının dönüştürülmesidir.

#### Gürültü Ekleme

Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

#### **Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler**

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilmesi ihtimali ortaya çıkabilmektedir.

Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

#### K-Anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır

### L-Çeşitlilik

K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

### T-Yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

### **Anonim Hale Getirme Yönteminin Seçilmesi**

Şirketimiz, yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak ve sahip olunan veri kümesine dair aşağıdaki özellikler dikkate alınarak karar vermektedir;

Verinin niteliği,  
Verinin büyüklüğü,  
Verinin fiziki ortamlarda bulunma yapısı,  
Verinin çeşitliliği,  
Veriden sağlanmak istenen fayda / işleme amacı,  
Verinin işleme sıklığı,  
Verinin aktarılacağı tarafın güvenilirliği,  
Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,  
Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,  
Verinin dağıtıklık/merkezilik oranı,  
Kullanıcıların ilgili veriye erişim yetki kontrolü ve  
Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

Bir veri anonim hale getirilirken, Şirketimiz kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmektedir.

### **Anonimlik Güvencesi**

Şirketimiz, bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilirken, anonim hale getirilmiş veri kümesinin bin başka veri kümesiyle birleştirilerek anonimliğin bozulmaması, bin ya da birden fazla değer bir kaydı tekil hale getirebilecek şekilde anlamlı bin bütün oluşturulmaması, anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi noktalarına dikkate dilemekte olup, Şirketimizce anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değişikçe kontroller yapılmakta ve anonimliğin korunduğundan emin olunmaktadır.

### **Anonim Hale Getirilmiş Verilerin Tersine İşlem İle Anonimleştirilmenin Bozulmasına Dair Riskler**

Anonim hale getirme işlemi, kişisel verilere uygulanan ve veri kümesinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski



bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir. Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır. Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere “anonimliğin bozulmasına yönelik saldırılar” denilmektedir. Bu kapsamda, Şirketimizce anonim hale getirilmiş kişisel verilerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski olup olmadığı araştırılarak ona göre işlem tesis edilmektedir.

## **KİŞİSEL VERİLERİ NASIL KORUYORUZ?**

Kişisel verilerin korunması ve hukuka aykırı bir şekilde erişimini önlemek için KVK Kurumu'nun yayınladığı Kişisel Veri Güvenliği Rehberi doğrultusunda Biyotem tarafından gerekli idari ve teknik tedbirler alınmakta, Şirket içinde prosedürler düzenlenmekte, aydınlatma ve açık rıza metinleri hazırlanmakta ve KVKK m. 12/3 uyarınca KVKK hükümlerinin uygulanmasını sağlamak için gerekli denetimler yapılmakta veya dışardan hizmet alımı yoluyla yaptırılmaktadır. Bu denetim sonuçları Şirketin iç işleyişi kapsamında değerlendirilir ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülür.

Yukarıda belirtilen kişisel verileriniz, Şirketimize ve/veya tedarikçilerimize ait fiziki arşivler ve bilişim sistemlerine nakledilerek, hem dijital hem de fiziki ortamda muhafaza altında tutulabilecektir. Kişisel verilerin güvenliğini sağlamak için alınan teknik ve idari tedbirler aşağıda iki başlık altında detaylı bir şekilde açıklanmaktadır.

### **Teknik Tedbirler**

Toplanan kişisel verilerin korunması için Secure Socket Layer (SSL) adı verilen standart teknoloji de dahil olmak üzere, genel kabul görmüş standart teknolojileri ve işletme güvenliği yöntemlerini kullanılmaktadır. Ancak, İnternet'in özelliği dolayısıyla bilgilere yetkisiz kişiler tarafından ağlar üzerinden gerekli güvenlik önlemleri olmaksızın erişilebilmektedir. Teknolojinin güncel durumuna, teknolojik uygulamanın maliyetine ve korunacak verilerin niteliğine bağlı olarak, verilerinizin imha, kayıp, tahrifat, izinsiz ifşa veya izinsiz erişim gibi risklerden korumak için teknik ve idari tedbirleri almaktayız. Bu kapsamda birlikte çalıştığımız hizmet sağlayıcılarla veri güvenliğine ilişkin sözleşmeler akdetmekteyiz.

- 1) **Siber Güvenliğin Sağlanması:** Kişisel veri güvenliğinin sağlanması için siber güvenlik ürünleri kullanılmaktadır ancak aldığımız teknik tedbirler bununla sınırlı değildir. Güvenlik duvarı ve ağ geçidi gibi tedbirler ile internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattını oluşturulmaktadır. Bununla birlikte hemen hemen her yazılım ve donanım bir takım kurulum ve yapılandırma işlemlerine tabi tutulmaktadır. Yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları olabileceği dikkate alınarak, kullanılmayan yazılım ve servisler cihazlardan kaldırılmaktadır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilmektedir. Yama yönetimi ve yazılım güncellemeleri ile yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi sağlanmaktadır.
- 2) **Erişim Sınırlamaları:** Kişisel veri içeren sistemlere erişim yetkileri sınırlandırılmakta ve düzenli olarak gözden geçirilmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmakta ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmaktadır. Söz konusu şifre ve parolalar oluşturulurken, kişisel

bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmaktadır. Buna bağlı olarak, erişim yetki ve kontrol matrisi oluşturulmaktadır.

- 3) Şifreleme: Güçlü şifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişkileri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılması yapılmaktadır.
- 4) Anti Virüs Yazılımları: Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılmakta, ayrıca bunlar güncel tutularak gereken dosyaların düzenli olarak taranmaktadır. Farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi sağlanmaktadır.
- 5) Kişisel Veri Güvenliğinin Takibi: Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi, Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi, Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi), Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması, Yapılmaktadır. Yine çalışanların sistem ve servislerdeki güvenlik zaaflarını ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulmaktadır. Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmakta ve güvenli bir şekilde saklanmaktadır.
- 6) Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması: Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemleri alınmaktadır. Kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunmakta ve bu ortamlara giriş / çıkışlar kontrol altına alınmaktadır.

Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalinin önlemek için ağ bileşenleri arasında erişim sınırlandırılabilen veya bileşenlerin ayrılması sağlanmaktadır. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilir.

Aynı seviyedeki önlemler Şirket yerleşkesi dışında yer alan ve Şirkete ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınmaktadır. Nitekim, kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmektedir. Çalışanların şahsi elektronik cihazları ile bilgi sistem ağına erişim sağlaması durumunda bunlar için de yeterli güvenlik tedbirleri alınmaktadır.

Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması yöntemi uygulanmaktadır. Bu kapsamda

şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda saklanmakta ve yetkisiz erişim önlenmektedir.

Kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmakta, söz konusu evraklara yetkisiz erişim önlenmektedir.

Şirketimiz, KVKK m. 12 uyarınca kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde bu durumu en kısa sürede KVK Kurulu'na ve ilgili kişilere bildirir. KVK Kurulu, gerekli görmesi halinde bu durumu internet sitesinde veya başka bir yöntemle ilan edebilir.

- 7) Kişisel Verilerin Bulutta Depolanması: Kişisel verilerin bulutta depolanması durumunda, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının Şirket tarafından değerlendirilmesi gerekmektedir. Bu kapsamda, bulutta depolanan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolü uygulanmaktadır. Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması sağlanmaktadır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmeye yarayabilecek şifreleme anahtarlarının tüm kopyaları yok edilmektedir. Kişisel verilerin bulunduğu veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri ilgililere anlık olarak iletilmektedir.
- 8) Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakım: Şirket tarafından yeni sistemlerin tedariki, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmaktadır.
- 9) Kişisel Verilerin Yedeklenmesi: Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde Şirket yedeklenen verileri kullanarak en kısa sürede faaliyete geçmeyi sağlamaktadır. Yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olup, veri seti yedekleri ağ dışında tutulmaktadır.

## **İdari Tedbirler**

- Şirketimizin yürütmüş olduğu tüm faaliyetler detaylı olarak tüm iş birimleri özelinde analiz edilmiş ve bu analiz neticesinde süreç bazlı bir kişisel veri işleme envanteri hazırlanmıştır. Bu envanterdeki riskli alanlar tespit edilerek gerekli hukuki ve teknik tedbirler sürekli olarak alınmaktadır. (Örn. KVKK kapsamında hazırlanması gereken belgeler bu envanterdeki riskler göz önüne alınarak hazırlanmıştır)
- Şirketimiz tarafından gerçekleştirilen kişisel veri işleme faaliyetleri bilgi güvenliği sistemleri, teknik sistemlerle ve hukuki yöntemlerle denetlenmektedir. Kişisel veri güvenliğine ilişkin politika ve prosedürler belirlenmekte bu kapsamda düzenli kontroller yapılmaktadır.
- Biyotem, bilgi teknolojileri ihtiyaçlarını karşılayabilmek için zaman zaman harici hizmet sağlayıcı firmalardan hizmet alabilmektedir. Bu durumda söz konusu veri işleyen harici hizmet sağlayıcıların en az Şirketimizin sağladığı güvenlik önlemlerini sağladığından emin olarak işlem yapılmaktadır. Bu durumda, veri işleyen ile yazılı bir sözleşme imzalanarak imzalanan bu sözleşmede asgari olarak aşağıdaki hususlara yer verilmektedir:
  - Veri işleyen'in sadece veri sorumlusu'nun talimatları doğrultusunda sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve KVKK ve sair mevzuata uygun bir şekilde hareket etmesi,
  - Kişisel Veri Saklama ve İmha Politikası'na uygun bir şekilde hareket etmesi,

- Veri İşleyen'in işlediği kişisel verilere ilişkin süresiz süreli sır saklama yükümlülüğüne tabi olması,
  - Herhangi bir veri ihlali olması durumunda Veri İşleyen'in bu durumu derhal Veri Sorumlusu'na bildirmekle yükümlü olması,
  - Şirketimiz'in veri işleyen'in kişisel veri içeren sistemleri üzerinde gerekli denetimleri yapacağı veya yaptıracağı, denetim sonucu ortaya çıkan raporları ve hizmet sağlayıcı firmayı yerinde inceleyebileceği,
  - Kişisel verilerin güvenliği için gerekli teknik ve idari tedbirleri alacağı; ve
  - Ayrıca, Veri İşleyen ile aramızdaki ilişkinin niteliği elverdikçe Veri İşleyen'e aktarılan kişisel verilerin kategori ve türleri de ayrı bir maddede belirtilmektedir.
- Kurum'un rehber ve yayınlarında vurguladığı üzere veri minimizasyonu prensibi çerçevesinde kişisel veriler mümkün olduğunca azaltılmakta ve gerekli olmayan, güncelliğini yitirmiş ve bir amaca hizmet etmeyen kişisel veriler toplanmamakta ve eğer KVKK'dan önceki dönemde toplandıysa Kişisel Veri Saklama ve İmha Politika'sına uygun bir şekilde imha edilmektedir.
  - Teknik hususlar konusunda uzman personel istihdam edilmektedir.
  - Şirketimiz çalışanlarının işe alınma süreçlerinde imzalanacak İş Sözleşmelerinde gizliliğe ve veri güvenliğine ilişkin olarak hükümler belirlemiştir ve çalışanlardan bu hükümlere uymasını istemektedir. Çalışanlar, kişisel verilerin korunması hukuku ve bu hukuka uygun olarak gerekli önlemlerin alınması konusunda düzenli olarak bilgilendirilmekte ve eğitilmektedir. Çalışanların rol ve sorumlulukları bu kapsamda gözden geçirilmiş ve görev tanımları revize edilmiştir.
  - Teknolojik gelişmelere uygun şekilde teknik önlemler alınmakta, alınan önlemler periyodik olarak kontrol edilmekte, güncellenmekte ve yenilenmektedir.
  - Erişim yetkileri sınırlandırılmakta, yetkiler düzenli olarak gözden geçirilmektedir.
  - Alınan teknik önlemler düzenli olarak yetkilisine raporlanmakta, risk oluşturan hususlar yeniden gözden geçirilerek gerekli teknolojik çözümlerin üretilmesi için çalışılmaktadır.
  - Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.
  - Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için yedekleme programları kullanılmaktadır.
  - Saklanma alanlarına yönelik güvenlik sistemleri kullanılmakta, alınan teknik önlemler periyodik olarak iç kontroller gereği ilgisine raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözümler üretilmektedir. Fiziksel ortamda saklanan dosyalar/çıktılar çalışılan tedarikçi firmalar aracılığı ile saklanmakta ve sonrasında belirlenen prosedürlere uygun olarak imha edilmektedir.
  - Kişisel Verilerin Korunması konusu üst yönetim tarafından da sahiplenilmekte, bu konuda özel bir Komite oluşturulmuş (KVK Komitesi) ve çalışmaya başlamıştır. Şirket KVK Komitesi'nin çalışma kurallarını düzenleyen bir yönetim politikası Şirket içinde yürürlüğe alınmış ve KVK Komitesi'nin görevleri detaylı bir şekilde açıklanmıştır.

## **KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HAKLARINIZ NELERDİR?**

KVKK m. 11 uyarınca ilgili kişiler olarak kişisel verilere ilişkin aşağıdaki haklara sahipsiniz:

- Kişisel verilerinizin işlenip işlenmediğini öğrenme;
- Kişisel veriler işlenmişse buna ilişkin bilgi talep etme;
- Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme;
- Kişisel verilerin yurt içinde ve dışında aktarıldığı üçüncü kişileri bilme;
- Kişisel verilerinizin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinizin aktarıldığı üçüncü kişilere bildirilmesini isteme;

- KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerinizin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinizin aktarıldığı üçüncü kişilere bildirilmesini isteme;
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhinize bir sonucun ortaya çıkmasına itiraz etme;
- Kişisel verilerinizin kanuna aykırı olarak işlenmesi sebebiyle zarara uğramanız hâlinde uğradığınız zararın giderilmesini talep etme.

Bu taleplerinizi Başvuru Tebliği uyarınca aşağıda belirtilen yöntemle Şirketimize ücretsiz olarak iletebilirsiniz:

- 1) [https://www.biyotem.com.tr/kvkk/veri\\_sahibi\\_basvuru\\_formu.docx](https://www.biyotem.com.tr/kvkk/veri_sahibi_basvuru_formu.docx) adresinde bulunan formun doldurulup ıslak imzalı olarak imzalandıktan sonra Biyotem Sağlık Malzemeleri ve Hizmetleri Pazarlama Turizm Anonim Şirketi Sağlık Mahallesi Marmara Sk. No: 16/12-13-14 Sıhhiye, Çankaya/Ankara adresine şahsen iletilmesi (kimliğinizin ibraz edilmesi gerekeceğini hatırlatmak isteriz).
- 2) [https://www.biyotem.com.tr/kvkk/veri\\_sahibi\\_basvuru\\_formu.docx](https://www.biyotem.com.tr/kvkk/veri_sahibi_basvuru_formu.docx) adresinde bulunan formun doldurulup ıslak imzalı olarak imzalandıktan sonra Biyotem Sağlık Malzemeleri ve Hizmetleri Pazarlama Turizm Anonim Şirketi Sağlık Mahallesi Marmara Sk. No: 16/12-13-14 Sıhhiye, Çankaya/Ankara adresine noter kanalıyla gönderilmesi.
- 3) [https://www.biyotem.com.tr/kvkk/veri\\_sahibi\\_basvuru\\_formu.docx](https://www.biyotem.com.tr/kvkk/veri_sahibi_basvuru_formu.docx) adresinde bulunan başvuru formunun doldurulup 5070 Sayılı Elektronik İmza Kanunu kapsamındaki “güvenli elektronik imza” ile imzalandıktan sonra güvenli elektronik imzalı formun [bilgi@biyotem.com.tr](mailto:bilgi@biyotem.com.tr) adresine elektronik posta ile gönderilmesi.
- 4) Biyotem daha önce bildirilen ve Biyotem sisteminde kayıtlı bulunan e-posta adresinizi kullanmak suretiyle yazılı olarak iletilmesi.

Başvuru sırasında tam isim ve başvuru yazılı ise imza, T.C. Kimlik Numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirim esas elektronik posta adresi, telefon ve faks numarası, talep konusu, bulunması zorunludur. Ek bilgi ve belgeler de başvuruya eklenebilir.

İlgili kişiler adına üçüncü kişiler tarafından talepte bulunamaz. İlgili kişinin kendisi dışında bir kişinin talepte bulunması için konuya ilişkin olarak düzenlenmiş ve noterce onaylanmış bir vekâletnamenin ıslak imzalı bir kopyası bulunmalıdır. Başvuruda talep edilen hususun açık ve anlaşılır olması gerekmektedir.

Bu kapsamda yapılan başvurular, mümkün olan en kısa zaman diliminde ve en çok 30 gün içerisinde sonuçlandırılacaktır. Söz konusu başvurular ücretsizdir. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, KVK Kurulu'nca belirlenen tarifedeki ücret alınabilir. Biyotem, başvuruda bulunan kişinin ilgili kişi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir. Biyotem, ilgili kişinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

KVKK m. 14 uyarınca şirketimize başvurunuzun reddedilmesi, verdiğimiz cevabı yetersiz bulmanız veya süresinde başvuruya cevap vermediğimiz hâllerinde; Şirketimizin cevabını öğrendiğiniz tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde KVK Kurulu'na şikâyette bulunabilirsiniz.

## İLGİLİ KİŞİLERİN HAKLARINI İLERİ SÜREMEYECEĞİ DURUMLAR NELERDİR?

İlgili kişiler, KVKK'nın 28. maddesi gereğince aşağıdaki haller KVKK kapsamı dışında tutulduğundan, ilgili kişilerin bu konularda yukarıda sayılan haklarını ileri süremezler:

- 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 istihbari faaliyetler kapsamında işlenmesi.
- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

KVKK'nın 28/2 maddesi gereğince; aşağıda sıralanan hallerde İlgili kişiler zararın giderilmesini talep etme hakkı hariç, 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 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.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması

Politika Güncelleme Tarihi : 24/02/2020

## EK – KISALTMALAR

KISALTMALAR	
<b>5651 sayılı Kanun</b>	İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
<b>Anayasa</b>	Türkiye Cumhuriyeti Anayasası
<b>Başvuru Tebliği</b>	Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
<b>İlgili Kişi/İlgili Kişiler</b>	Biyotem ve/veya Biyotem’in müşterileri, ticari ilişki içinde bulunduğu kurumsal müşterileri, iş ortakları, hissedarları, yetkilileri, aday çalışanları, stajyerleri, ziyaretçileri, tedarikçileri, işbirliği içinde çalıştığı kurumların çalışanları, üçüncü kişiler ve burada sayılanlarla sınırlı olmamak üzere diğer kişiler gibi kişisel verisi işlenen gerçek kişiyi ifade eder.
<b>Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik</b>	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
<b>KVKK</b>	Kişisel Verilerin Korunması Kanunu
<b>KVK Kurulu</b>	Kişisel Verileri Koruma Kurulu
<b>KVK Kurumu</b>	Kişisel Verileri Koruma Kurumu
<b>m.</b>	Madde
<b>Örn.</b>	Örnek
<b>Politika</b>	İşbu Biyotem Kişisel Verilerin Korunması Politikası
<b>Şirket/ Biyotem</b>	Biyotem Sağlık Malzemeleri ve Hizmetleri Pazarlama Turizm Anonim Şirketi
<b>Türk Ceza Kanunu</b>	5237 sayılı Türk Ceza Kanunu