www.zimed.com.tr

zimed®

KİŞİSEL VERİLERİN İŞLENMESİ & KORUNMASI POLİTİKASI

PROCESSING AND PROTECTION OF PERSONAL DATA

TR ENG

innovation to move

TR

ENG

İÇİNDEKİLER

TR

ENG

KİŞİSEL VERİLERİN İŞLENMESİ VE KORUNMASI POLİTİKASI

1. AMAÇ VE KAPSAM

Zimed Medikal San. Ve Tic. LTD. ŞTİ.'nin Kişisel Verilerin İşlenmesi ve Korunması Politikası ("Politika"), kişisel verilere ilişkin mevzuat çerçevesinde kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasa'da öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması amaçlanarak hazırlanmıştır.

"Politika" hazırlanırken öncelikle şirket organizasyon şeması dahilinde çalışma birimlerinin hangi verileri, neden topladıkları ve bu verileri neden üçüncü kişilere aktarma gereksinimi olduğunu **belirlemek** ve şirketin kişisel veri işleme usulünü **anlamak** temel ilke olarak belirlenmiştir. İlgili mevzuatın gereksinimleri "Politika"ya aktarılırken, özelleştirilerek, şirketin hangi verileri neden temin ettiğini, bu verileri neden işlediğini sade ve anlaşılır bir dil ile **izah etmek** kişisel verilerin korunması gerekliliği dahilinde duyulan hassasiyet çerçevesinde ilke edinilmiştir. Ayrıca, şirket organizasyonu içinde ve organizasyon dışında veri gizliliğinin korunması için gerekli idari ve teknik tedbirleri almak ve verileri işlenen bireyleri bilgilendirmek ve aydınlatmak hedeflenmektedir.

Politika kapsamına şirket tarafından verileri işlenen tüm gerçek ve tüzel kişiler girmektedir.

İş bu politika kapsamında şirket organizasyonunda yer alan işlem ve faaliyetler çerçevesinde işlenen veriler, verilerin kategorizasyonu, veri alıcı grupları, veri toplama hukuki sebebi ve yöntemi, verilerin aktarıldığı üçüncü kişi grupları, verilerin işleme süreleri, verilerin silinme süreleri hakkında özelleştirilmiş bilgilere yer verilmeye çalışılmıştır. Ancak hali hazırdaki işleme faaliyetlerinin dışında şirket tarafından veri işleme yapılması/yapılacak olması halinde harici bir aydınlatma metni dahilinde, işbu politikada belirtilen temel ilke ve prensiplere uyulmak kaydıyla işleme faaliyeti yürütülmesi ve aydınlatma yapılması mümkündür. Bu durumda yapılan aydınlatma işbu politikanın ayrılmaz bir parçasını teşkil edecek olup, İşbu politikada yer almadığı iddia edilemeyecektir. Nitekim Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5. maddesi kapsamında aydınlatmanın sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle yapılması mümkündür.

2. TANIMLAR

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Şirket	ZİMED MEDİKAL SANAYİ VE TİCARET LİMİTED ŞİRKETİ
Çerez (Cookie)	Kullanıcıların bilgisayarlarına yahut mobil cihazlarına kaydedilen ve ziyaret ettikleri web sayfalarındaki tercihleri ve diğer bilgileri depolamaya yardımcı olan küçük dosyalardır.
İlgili Kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir.
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
İrtibat Kişisi	Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişi. (İrtibat kişisi Veri Sorumlusunu temsile yetkili değildir. Adından anlaşılacağı üzere yalnızca veri sorumlusu ile ilgili kişilerin ve Kurumun iletişimini "irtibatı" sağlamak üzere görevlendirilen kişidir.)
Kanun/KVKKK	7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.
Kayıt Ortamı	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
Kişisel Verilerin Yok Edilmesi	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
Kurul	Kişisel Verileri Koruma Kurulu.
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, Şirket, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler.
Periyodik İmha	Kişisel verilerin işlenmesi için aranan şartların tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.
Politika	Şirket tarafından oluşturulan kişisel veri koruma politikası.
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
Yönetmelik	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği.
Kaynak:	6698 sayılı Kişisel Verilerin Korunması Kanunu- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik - Veri Sorumluları Sicili Hakkında Yönetmelik - Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ - Veri Sorumlusuna Başvuru ve Usul Esasları Hakkında Tebliğ Veri sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

3. VERİ SORUMLUSU KİMLİĞİ

Bu politikanın kapsamına giren her türlü kişisel veri işleme faaliyeti için veri sorumlusunun kimliğine ilişkin bilgiler aşağıda verilmektedir.

Veri Sorumlusu	**ZİMED MEDİKAL SANAYİ VE TİCARET LİMİTED ŞİRKETİ**
Adres	Aydınlar Mahallesi 03070 Cad. No :4 ŞEHİTKAMİL/GAZİANTEP
Telefon	0 342 238 43 44
Fax	0 342 238 44 11
KEP	zimedmedikal@hs01.kep.tr
İnternet Sitesi	***www.zimed.com.tr***

4. KİŞİSEL VERİLERİN KORUNMASI ORGANİZASYON YAPISI

Bu Politika kapsamına giren kişisel veri işleme faaliyetleri bakımından veri sorumlusu, **ZİMED MEDİKAL SANAYİ VE TİCARET LİMİTED ŞİRKETİ** 'dir.

Şirketimiz, kişisel verilerin korunması mevzuatına uyumun sürdürülebilir kılınmasını teminen bir organizasyon yapısı oluşturmuş ve bu kapsamda bir uyum programını hayata geçirmiştir. Bu çerçevede, Şirketimizin "**İdari İşler Departmanı**" bünyesinde bir "**Kişisel Verileri Koruma Birimi**" kurulmuş ve İrtibat Kişisi görevlendirilmiştir.

5. KİŞİSEL VERİLERİ KORUMA BİRİMİ

Kişisel verileri koruma mevzuatına sürdürülebilir uyumu sağlama yönündeki kararlılığımızı göstermek ve kişisel verilerin korunması sistemimizin etkinliğini temin etmek amaçlarıyla Şirketimiz bünyesinde bir KVKK Birimi kurulmuştur. KVKK Birimi Başkanı ve KVKK Birimi üyeleri yönetim kurulu tarafından belirlenir.

KVKK Birimi Başkanı'nın izin ve/veya sair nedenlere bağlı olarak Şirketimizde bulunmaması durumunda, yerine vekalet edecek kişi KVKK Birimi Başkanı tarafından geçici olarak görevlendirilir. Bu durumda geçici olarak görevlendirilen kişi, Kişisel Verilerin Korunması Politikası kapsamında KVKK Birimi Başkanı'na atanan tüm görevlerin yerine getirilmesinden sorumludur.

5.1 İrtibat Kişisi

Şirketimizin kişisel verilerin korunması mevzuatına uyuma yönelik almış olduğu önlemlerin etkinliğini takip etmek üzere İrtibat Kişisi belirlenmiştir. İrtibat Kişisi'nin başlıca sorumluluğu, KVKK Birimi'nin Merkezi Politikalar görev ve sorumluluklarını yerine getirmesine yönelik çalışmaktır. İrtibat Kişisi, KVKK Birimi üyesi olup, ihtiyaç halinde KVKK Birimi'ni toplantıya çağırır.

İrtibat Kişisi aynı zamanda Şirketimizin veri sorumluları sicili ve Kişisel Verileri Koruma Kurulu nezdinde KVKK Mevzuatı kapsamında irtibat kişisi olarak hareket eder.

İrtibat Kişisi'nin izin ve/veya sair nedenlere bağlı olarak Şirketimizde bulunmaması durumunda, yerine vekalet edecek kişi KVKK Birimi tarafından geçici olarak görevlendirilir. Bu durumda geçici olarak görevlendirilen kişi, Kişisel Verilerin Korunması Politikası kapsamında İrtibat Kişisi'ne atanan tüm görevlerin yerine getirilmesinden sorumludur.

6. KİŞİSEL VERİLERİNİZİN İŞLENMEAMAÇLARI, İŞLEDİĞİMİZ KİŞİSEL VERİLERİNİZ, TOPLANMA YÖNTEMLERİ VE HUKUKİ SEBEPLERİ

6.1 İşlenme Amaçları

Kişisel verileriniz KVKKK' da öngörülen sınırlara riayet edilerek kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel, belirli, açık ve meşru amaçlar çerçevesinde, amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmakta, kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar kişisel verileri muhafaza etmektedir.

Şirketimiz, ürün ve hizmetlerinden yararlanan müşterilerimiz dahil ve fakat bunlarla sınırlı olmamak üzere potansiyel müşterilerimiz, çalışanlarımız, stajyerlerimiz, çalışan adaylarımız, hissedarlarımız, yetkililerimiz, tedarikçilerimiz, danışmanlarımız, yetkili satıcılarımız, iş birliği yaptığımız şirketler ve bunların çalışanları, hissedarları, yetkilileri, ziyaretçilerimiz, internet sitemizi ziyaret eden kullanıcılarımız, kısaca faaliyetlerimiz sırasında şirketimizle irtibat halinde olan kişilere ait kişisel bilgileri; kimlik, iletişim bilgileri, faaliyet alanı çerçevesindeki her türlü ürüne ilişkin kullanım alışkanlığı, finansal veriler, sağlık verileri, talep ve şikayet yönetim verileri gibi verileri işlemekte ve bu verileri, veri sahiplerinin Zimed Medikal ürün ve hizmetlerinden yararlanabilmesi, pazarlama, işin ifası, sözleşme gereklerinin yerine getirilmesi, şirketin mali ve hukuki yükümlülüklerinin yerine getirilebilmesi amaçlarıyla veri sahiplerini aydınlatma ve yasa gereği açık rıza alınması gereken durumlarda rıza almak koşuluyla aşağıda belirtilen kriterlere esas alarak işlemektedir.

Şirketimiz KVKK 5. Madde 2. Fıkrasında ve 6. Maddenin 3. Fıkrasında belirtilen kişisel veri işleme şartları içerisindeki amaçlarla ve koşullarla sınırlı olarak, kişisel verileri aşağıdaki amaç ve koşullarla işlemektedir. Bu amaç ve koşullar şunlardır;

Sözleşmelerinin gereklerinin yerine getirilmesi,
Araştırma, geliştirme ve üretim faaliyetleri,
Fatura tanzimi ve tahsilat işlemlerinin gerçekleştirilmesi,
Satış sonrası hizmetlerinin ifası,

TR

ENG

Müşterilere; ürün, hizmet tanıtımı, bilgilendirme, reklam, kampanya ve diğer faydaların sunulması, ticari elektronik iletilerin gönderilmesi, anket uygulamaları, istatistik analizler vasıtasıyla çeşitli avantajlar sağlanması,
Hizmet kalitesini geliştirici çalışmalar yapılması ve daha iyi hizmet sunulması,
Dış kaynaklardan hizmet alımı yapılması,
Kimlik teyidi,
Talep ve Şikayetlerin değerlendirilmesi ve cevap verilmesi,
İlgili iş ortakları ve sair 3. Kişilerle finansal mutabakat sağlanması,
Resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temini,
Müşteri memnuniyetinin ölçülmesi,
Çalışanlar bakımından; Özlük dosyasının oluşturulması, işin gereklerini sürekli olarak yerine getirmeye ehil olup olmadığının tespiti, sağlık dosyası oluşturulması, iş güvenliği önlemlerinin alınması,
Çalışan adayları ve stajyerler bakımından başvuru süreçlerinin yürütülmesi,
İnsan kaynakları süreçlerinin planlanması,
Bilgi güvenliği süreçlerinin yürütülmesi,
Yasal yükümlülüklerinin yerine getirilmesi,
Raporlama ve risk yönetimi işlemlerinin icrası/takibi
Hukuk işlerinin icrası/takibi,
Ziyaretçi kayıtlarının oluşturulması ve takibi
Saklama ve Arşiv faaliyetlerinin yürütülmesi.

6.2 İşlediğimiz Kişisel Verileriniz

Kimlik Bilgileri : İsminiz, soy isminiz, T.C. kimlik numaranız, anne adı, baba adı, doğum yeri ve tarihi, personel sicil numaranız, uyruk bilginiz ve Şirket'e tarafınızca açık rızanız dahilinde temin edilen sair bilgiler.

İletişim Bilgileri : İkamet adresiniz, işyeri adresiniz, telefon numaranız ve e-posta adresiniz, KEP adresi ile var ise tarafınızla iletişim kurulması için tercih ettiğinizi bildirdiğiniz cep telefonu numaranız, faks numaranız veya size ulaşabilmemiz için rızanız ile temin etmiş olduğunuz diğer iletişim kanallarına ilişkin bilgileriniz.

Çalışma ve Eğitim Bilgileriniz: Şirkete başvuru (iş başvurusu, sertifikalı/sertifikasız eğitimlere katılma başvurusu) için doldurmuş olduğunuz başvuru formu, kayıt evrakı kapsamında ve/veya Şirket resmi e-posta adresi adresine gönderilen iş başvuru formlarında yahut Şirket tarafından sağlanan çevrimiçi ya da fiziki başka başvuru usulleri kullanılmak suretiyle kimlik bilgileriniz, iş durumunuza ait bilgiler, iletişim bilgileriniz ile eğitim durumunuza ait (Üniversite mezunu, yüksek lisans mezunu gibi) bilgileriniz ve geçmiş mezuniyet bilgileriniz, katıldığınız kurs/seminer bilgileriniz, sertifika bilgileriniz ile ulusal yahut uluslararası sınav sonuçlarınız.

Finansal/Mali Bilgileriniz :Maaş ve yan hakların ödenmesi, fazla ve yersiz alınan ödemelerin iadesi, gibi ödemelerin yapılabilmesi amacıyla edinilen; banka isim ve şube bilgisi, banka hesap no bilgisi, IBAN no bilgisi.

Görsel/İşitsel Bilgiler :Şirket'in düzenlediği konferans, seminer ve benzeri etkinliklerde etkinlikle ilgili olarak; etkinliği tanıtmak, duyurmak, yaygınlaşmasını sağlamak gibi amaçlar için etkinliğin gerçekleştiği yerin ve katılanların durağan veya akan görüntüleri ve/veya sesleri ile Şirket merkez, şube ve temsilciliklerinde güvenliği sağlamak için kurulmuş olan kameraların sağladığı görsel/işitsel bilgiler. Söz konusu etkinliklerde elde edilen görsel/işitsel bilgiler Şirket faaliyetlerini aşmayacak ve etkinliğin amacı ile sınırlı olacak şekilde Şirket'in internet sitesinde, Şirket tarafından kullanılan sosyal paylaşım platformlarında, Şirket tarafından basılan eserlerde kullanılabilecektir. Yahut Şirket'in izniyle ve kontrolü altında basılmak/yayınlanmak üzere 3. kişilere gönderilebilecektir. Bu kullanım usulü güvenlik kamera görüntülerini kapsamayacak olup, ilgili görsel/işitsel kişisel veriler kullanılmadan önce (Misalen; etkinliğin başında) katılımcılara ayrıca bilgilendirme yapılacak olup, açık rızaları alınacaktır.

Özel Nitelikli Kişisel Veriler : Şirket bünyesinde mevzuat kaynaklı çalıştırma yükümlülüklerini yerine getirebilmek amacıyla çalıştırılan engelli ve hakkında mahkûmiyet kararı verilmiş ve/veya güvenlik tedbiri uygulanmış kişilere ilişkin ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin özel nitelikli kişisel veriler, Şirketimiz medikal tıbbi ürünler imal ettiğinden, bünyesinde çalışan kişilerin bulaşıcı hastalıkların önlenmesi amacıyla sağlık raporu talep edilmekte ve aylık düzenli sağlık kontrollerinden geçirilmektedir.

Şirket'in bu amaçlar haricinde başka herhangi bir doğrudan özel nitelikli kişisel veri işleme amacı olmamakla birlikte Şirket'e sunmuş olduğunuz kimlik belgesi, fotoğraflar yahut etkinlikler kapsamında durağan/akan görüntülerden elde edilen veriler kapsamında dolaylı olarak edinilme ihtimali olan din, kılık-kıyafet, felsefi inanç, siyasi düşünce ve sağlık verileriniz (örneğin fotoğraftan anlaşılan kıyafet, cihaz ve protezler) ile Şirket tarafından sağlanan bir evrakta ihtiyari olarak belirttiğiniz özel nitelikli sair bilgiler.

6.3 Kişisel Verilerinizin Toplanma Yöntemleri

Kişisel verileriniz iş başvuru formu, internet üzerinden doldurulan iş başvuru formları, güvenlik kamera kayıtları ve ŞİRKET resmi e-mail adresi olan info@zimed.com.tr adresine, zimedmedikal@hs01.kep.tr KEP adresine veya +90 342 238 44 11 numaralı faks adresine, kişisel veri gönderilmesi durumunda söz konusu iletişim kanalları vasıtasıyla toplanmaktadır.

Kişisel veriler, fiziken evrak gönderilmesi, şirketin sağladığı bir evrakın fiziken doldurulması, , +90 342 238 43 44 numaralı hatların veya şirkete ait diğer dâhili numaraların aranması suretiyle de toplanmaktadır.

Kişisel verileriniz ayrıca otomatik yollarla https://www.zimed.com.tr adresi ve uzantılarında kullanılan çerezler (cookie) vasıtasıyla da toplanmaktadır. Söz konusu çerezler, yalnızca ziyaretçinin siteyi tam verimlilikte kullanabilmesi için gerekli çerezler olup ziyaretçinin tercihlerini hatırlamak amacıyla kullanılmakta ve başka bir kişisel veri temin etmemektedir. Çerez politikamıza www.zimed.com.tr adresinden ulaşabilirsiniz.

6.4 Kişisel Veri İşlemenin Hukuki Sebepleri

KVKKK, kişisel verilerin işlenme şartlarını 5.maddesinin 2. fıkrasında listelemektedir. Eğer bir veri sorumlusu tarafından kişisel verilerin işlenme amaçları, KVKK'da listelenmiş olan kişisel veri işleme şartları çerçevesinde değerlendirilebiliyorsa, o veri sorumlusu kişisel verileri hukuka uygun olarak işleyebilmektedir. Bu kapsamda Şirket tarafından da güdülmekte olan kişisel veri işleme amaçlarının, KVKKK'da düzenlenen kişisel veri işleme şartları kapsamında değerlendirilebildiği durumlarda Şirket tarafından kişisel veri işleme faaliyetleri gerçekleştirilmektedir. Şirket kişisel veri işleme şartları kapsamına girmeyen herhangi bir kişisel veri işleme faaliyetinde bulunmamaktadır.

KVKKK'da yer alan kişisel veri işleme şartları şunlardır;

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

Özel nitelikli kişisel veriler için de temel işleme şartı açık rızadır ve Şirket temelde özel nitelikli kişisel veri işleme amacı gütmemektedir. Ancak faaliyetimiz gereği işlememiz gereken veya açık rızanız ile onay verdiğiniz özel nitelikli kişisel verileriniz de mevzuat dahilinde ölçülü olarak işlenmektedir.

KVKK'da özel nitelikli kişisel verilerin işlenebilmesi için sayılan şartlar şunlardır;

İlgili kişinin açık rızasının bulunması,
Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler için kanunlarda açıkça öngörülmesi,
Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak,
Kamu sağlığının korunması,

Koruyucu hekimlik,
Tıbbî teşhis,
Tedavi ve bakım hizmetlerinin yürütülmesi,
Sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla,
Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

Bir kişisel veri işleme faaliyetini hukuka uygun kılan bir veya birden fazla kişisel veri işleme şartı aynı anda bulunabilmektedir.

Söz konusu amaçlarımızı gerçekleştirebilmek için yukarıda belirttiğimiz verilerinizin işlenmesi gereği hasıl olmaktadır. Şirketimize, kimlik bilgileri aktarılırken aslında işleme amaçlarımız dahilinde olmayan veriler de tarafımıza aktarılabilmektedir. İdari ve teknik tedbirler dahilinde söz konusu verileri mevzuatta öngörülen süreler sonunda siliyor ve/veya anonim hale getiriyoruz ancak her koşulda bu durumu temin etmek mümkün olmamaktadır. Bu halde, söz konusu verilerin işlenmesi amacıyla açık rızanıza başvurmak gerekmektedir.

7. KİŞİSEL VERİLERİN AKTARIMI

Kişisel verileriniz bu Aydınlatma Metninde gösterilen amaçlar için gerektiğinde ve buradaki vasıtalarla, yetkili kamu kurum ve kuruluşları, yargı mercileri, infaz mercileri, emniyet birimleri ile sözleşmeli ürün ve hizmet alınan tedarikçiler ile paylaşılmaktadır. Şirketimiz hukuka uygun olan kişisel işleme amaçları doğrultusunda, gerekli güvenlik önlemlerini alarak kişisel veri sahibinin verilerini ve özel nitelikli kişisel verilerini 3. Kişilere aktarabilmektedir. Kişisel veriler, veri sahibinin açık rızası olmasa dahi, aşağıda belirtilen şartlardan bir ya da birkaçının mevcut olması halinde, şirketimiz tarafından yürürlükteki mevzuata ve düzenlemelere uygun olarak hukuki, teknik ve idari tedbirler alınmak kaydıyla 3. Kişilere aktarılabilecektir.

Kişisel verilerin aktarılmasına ilişkin ilgili faaliyetlerin kanunlarda açıkça öngörülmesi,
Kişisel verilerin şirket tarafından aktarılmasının bir sözleşmenin kurulması veya ifası ile doğrudan doğruya ilgili ve gerekli olması,
Kişisel verilerin aktarılmasının şirketimizin hukuki yükümlülüğünün yerine getirebilmesi için zorunlu olması,
Kişisel verilerin veri sahibi tarafından alenileştirilmiş olması,
Kişisel verilerin şirket tarafından aktarılmasının şirketin veya veri sahibinin veya 3. Kişilerin haklarının tesisi, kullanılması veya korunması için zorunlu olması,
Veri sahibinin temel hak ve özgürlüklerine zarar vermemek kaydıyla şirket meşru menfaatleri için kişisel veri aktarılması faaliyetinde bulunulmasının zorunlu olması
Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünü koruması için zorunlu olması.

Yukarıdakilere ek olarak kişisel veriler, kurul tarafından yeterli korumaya sahip olduğu ilan edilen yabancı ülkelere yukarıdaki şartlardan herhangi birinin varlığı halinde aktarılabilecektir. Yeterli korumanın bulunmaması durumunda ise mevzuatta öngörülen veri aktarım şartları doğrultusunda, Türkiye deki ve ilgili yabancı ülkedeki veri sorumlularını yeterli korumayı, yazılı olarak taahhüt ettiği ve kurulun izninin bulunduğu yabancı ülkelere aktarılabilecektir.

8. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASI

Özel nitelikli kişisel veriler, şirketimiz tarafından, işbu politikada belirtilen ilkelere uygun olarak ve kurulun belirleyeceği yöntemler de dahil olmak üzere gerekli her türlü idari ve teknik tedbirler alınarak ve aşağıdaki şartların varlığı halinde aktarılabilecektir;

Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda açıkça öngörülmesi halinde veri sahibini açık rıza aranmaksızın işlenebilecektir. Aksi halde veri sahibinin açık rızası alınacaktır.
Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile bu hizmetlerin planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar

TR

ENG

tarafından açık rıza alınmaksızın işlenebilecektir. Aksi halde veri sahibinin açık rızası alınacaktır. Yukarıdakiler ek olarak kişisel veriler, yeterli korumaya sahip yabancı ülkelere yukarıdaki şartlardan herhangi birinin varlığı halinde aktarılabilecektir. Yeterli korumanın bulunmaması durumunda ise, mevzuatta öngörülen veri aktarım şartları doğrultusunda, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt ettiği ve yeterli korumayı taahhüt eden veri sorumlusunun bulunduğu yabancı ülkelere aktarılabilecektir.

9. İLGİLİ KİŞİNİN HAKLARI

KVKK kapsamında ;

Kişisel Verilerinizin işlenip işlenmediğini öğrenme,
Kişisel Verileriniz işlenmişse buna ilişkin bilgi talep etme,
Kişisel Verilerinizin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
Yurtiçinde veya yurtdışında Kişisel Verilerinizin aktarıldığı üçüncü kişileri bilme,
Kişisel Verilerinizin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,
KVKK mevzuatında öngörülen şartlar çerçevesinde Kişisel Verilerinizin silinmesini veya yok edilmesini isteme,
v. ve vi. maddeleri kapsamında yapılan işlemlerin 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 halinde bu zararın giderilmesini talep etme haklarına sahipsiniz.

Haklarınızı Nasıl Kullanabilirsiniz?

Şirketimizin internet sitesinden (www.zimed.com.tr bağlantısını kullanarak) indirebileceğiniz başvuru formunu talebiniz/şikâyetiniz doğrultusunda doldurarak, söz konusu formu e posta adresi (info@zimed.com.tr) üzerinden tarafımıza iletebilir veya formu fiziki olarak doldurarak Aydınlar Mah. 03070 Cad. No.:4 ŞEHİTKAMİL 27580 GAZİANTEP/TURKEY adresine kargo/posta vasıtasıyla gönderebilirsiniz.

Talebinizi üstte gösterilen yöntemlerden birisini kullanarak tarafımıza iletmeniz durumunda KVKK md. 13/2 gereğince, talebiniz en geç 30 gün içinde değerlendirilecek ve tarafınıza konuyla ilgili bilgi verilecektir. Eğer talebiniz kabul edilirse, gerekli işlemler derhal veri sorumlusu şirket tarafından yerine getirilecektir.

Talepler kural olarak ücretsiz karşılanır ancak, talebin gereğini yerine getirmek masraf gerektiriyorsa "Veri Sorumlusuna Başvuru Usul ve Esasları Hk. Tebliğ" madde 7'de öngörülen; *"İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, 10 sayfaya kadar ücret alınmaz. 10 sayfanın üzerindeki her sayfa için 1 TL işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez."* Hükmü gereğince ŞİRKET tarafından ücret istenebilecektir.

10. KİŞİSEL VE ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNDE KANUNİ İSTİSNALAR ve AÇIK RIZA AÇIKLAMASI

KVKK aşağıdaki sıralanan hallerde veri sorumlusunun ilgili kişinin açık rızası olmaksızın veri işleme faaliyetinin yürütülebileceğini belirtmiştir.

İşbu Politika'da belirtilen işleme amaç ve şartları dikkate alındığında **kanuni istisnalar kapsamına giren** veri işleme şartları bakımından ilgili kişilerin rızalarının alınması gereği bulunmamaktadır. Ancak istisnaların ve işleme ilkelerinin yorumlanmasından ortaya çıkabilecek ihtilafların bertaraf edilmesi, bir belge içinde yer alan birden fazla verinin bir kısmının istisna kapsamına girerken, diğer kısmının istisna kapsamında değerlendirilmemesi, veri sorumlusunun meşru menfaat kavramının farklı yorumlanması, KVKK ve ilgili mevzuatı dahilinde içtihat ve yüksek mahkeme kararlarının az sayıda olması; kanunen işlenmesi, saklanması ve aktarılması zorunlu verilerin düzenleyici işlemlerde tek tek sayılmaması, saklama sürelerinin belirtilmemesi ve/veya muğlak olması ve/veya fiili uygulamada talep edilmesi ile yaptırımların ağır olması hususları birlikte değerlendirildiğinde, şirket tarafından ilke olarak ilgili kişilerin "açık rızalarına" başvurma yönteminin benimsenmesi arzu edilmektedir.

Ancak bu hal hiçbir koşulda şirketin istisna hükümlerden yararlanmayacağı ve/veya her durumda açık rıza alma yolunu seçeceği şeklinde yorumlanmamalıdır. Şirket kanuni istisna kapsamında yer alan işleme faaliyetlerinden açık rıza almadan yararlanabilecektir.

10.1 Kişisel Verilerin Açık Rıza Olmaksızın İşlenmesi:

Aşağıdaki şartlardan birinin varlığı hâlinde, **ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:**

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.

10.2 Özel Nitelikli Kişisel Verilerin Açık Rıza Olmaksızın İşlenmesi:

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, Şirket, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

Yukarıda belirtilen sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.

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

Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

10.3 KVKK'nın Uygulanamayacağı Tam İstisna Halleri

Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek ve tüzel kişiler tarafından tamamen **kendisiyle veya aynı konutta yaşayan aile fertleriyle** ilgili faaliyetler kapsamında işlenmesi.

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 istihbarat faaliyetleri** kapsamında işlenmesi.

Kişisel verilerin **soruşturma, kovuşturma, yargılama veya infaz işlemlerine** ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

10.4. Kısmi İstisna Halleri:

KVKK'nın amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri aşağıdaki hâllerde uygulanmaz:

Kişisel veri işlemenin **suç işlenmesinin önlenmesi veya suç soruşturması** için gerekli olması.

TR

ENG

İlgili kişinin kendisi tarafından **alenileştirilmiş** kişisel verilerin işlenmesi.
Kişisel veri işlemenin 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 işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

11. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN BİLGİLER

11.1 Kişisel Verilerin Elde Edildiği Kanallar

Şirket faaliyetleri dâhilinde olan kişisel veri elde etme kanalları aşağıda listelenmektedir:

Yönetim Kurulu ve diğer İdari Birimler Toplantı Tutanakları
İcra Kurulu, Departmanlar ve Çalışma Grupları Faaliyet Belgeleri, Toplantı Tutanakları ve Çalışma Belgeleri
Çalışanların Özlük Dosyası Belgeleri
Faaliyetler ve Sözleşmeler Dahilindeki İşlemlerin İfa Edilmesi İçin Finans Verileri
Kartvizitler
CCTV(Kapalı Devre Kamera Kayıtları),
SMS/E-Posta,Telefon
İnternet Sitesi, Uygulamalar, Çerezler (Cookies) ve Benzer Takip Teknolojileri (ERP),
Faks,
Posta, Kargo ya da Kurye Hizmetleri,
Diğer Fiziki ve Elektronik Ortamlar.

Teknolojik gelişmelere bağlı olarak şirket tarafından yukarıdaki kişisel veri elde etme kanallarına yeni eklemeler yapılabilecek ya da mevcut kanallardan bazılarının kullanılmasından vazgeçilebilecektir. Böyle durumlarda da şeffaflığı ve hesap verilebilirliği korumak adına Politika'nın güncellenmesi yoluyla kullanılan kanalların doğru bir şekilde ifade edilmesi sağlanacaktır.

12. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

Şirket kişisel verilerini işlemekte olduğu veri sahiplerinin kişisel verilerini elektronik ve fiziki ortamlarda gerekli teknik ve idari güvenlik tedbirlerini alarak saklamaktadır.

Şirketin kişisel verileri saklama süresi ilgili mevzuatta belirlenen süreler dikkate alınarak hesaplanmaktadır. Bununla beraber, Şirket faaliyetlerinin yürütülmesi amacıyla Şirketin bireylerle iletişim halinde olması Şirket mevzuatındaki amacı gerçekleştirmek bakımından önem taşımaktadır. Bu nedenle ilgili mevzuatta öngörülen sürelerin haricinde Şirket bireylerin "açık rıza"larını temin etmek suretiyle özellikle "ad/soyad/görev/iletişim" bilgilerini her daim güncelleyerek saklamayı arzu etmektedir.

KVKK'da yer alan kişisel veri işleme şartlarının varlığını ortadan kaldıracak kişisel veri işleme amaçlarının sona ermesi halinde, Şirket tarafından kişisel veriler imha edilecektir. Söz konusu imha işlemleri ilgili mevzuatın hükümlerine uygun olarak **6 aylık periyotlarla** gerçekleştirilmekte ya da veri sahiplerinden gelen taleplerin gerektirmesi halinde neticeye bağlanmaktadır. Yönetmeliğin 12. maddesi gereğince ise, ilgili kişinin silme ve/veya yok etme taleplerini Şirket mevzuatta başkaca bir süre öngörülmediği takdirde en geç **30 gün** içinde yerine getirerek ilgili kişiye bilgi verecektir.

Kişisel Verilerin imhası ile ilgili tutanaklar ise Şirket tarafından mevzuat gereğince başkaca bir süre belirlenmediği takdirde **3 yıl** süre ile saklanacaktır.

Şirket tarafından kişisel verilerin imhası, kişisel verilerin yer aldığı ortamlara göre silme, anonimleştirme ya da yok etme teknikleri kullanılarak yerine getirilmektedir. Söz konusu teknikler hakkında detaylı bilgiler Kurul tarafından yayınlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi içerisinde yer almaktadır.

Kişisel verilerin **ilgili kullanıcılar için** hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemine kişisel verinin **silinmesi denir**. İlgili Kullanıcı tabiri ise, verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir. Bu halde Şirket imha sistemi kapsamında verilerin işlenme amaçları dahilinde öncelikli olarak "Silme" prosedürü uygulanacaktır.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 7/5. maddesi gereğince veri işleme sebeplerinin ortadan kalkması halinde ve/veya ilgili kişinin talebi üzerine (Eğer ki KVKKm. 5/2 ve 6/3 dahilinde yer alan açık rıza alınmasına gerek olmayacak şekilde veya KVKK m. 28 dahilinde kanuni istisna kapsamına girmiyorsa) Şirket bünyesinde oluşturulan "KVKK Birimi" tarafından kişisel verileri **ilgili kullanıcılar için** hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek şekilde **silinecektir.**

ŞİRKET için esas imha usulü "silme" olmakla beraber, eğer ki tüm şartlar sağlanmış ve değerlendirme sonucunda uygun bulunmuşsa "yok etme" veya "anonim hale getirme" imha usulleri de ŞİRKET tarafından uygulanabilecektir.

13. KİŞİSEL VERİLERİN ÜÇÜNCÜ KİŞİLERLE PAYLAŞILMASI

Şirket faaliyetlerinin gereklilikleri nedeniyle Şirket tarafından kişisel verilerin yurtiçinde veya yurtdışında bulunan kişilerle/kurumlarla paylaşılması söz konusu olabilmektedir. Söz konusu paylaşımların gerçekleştirilebilmesi için Şirket tarafından KVKK'nın gereklerine ve veri işleme şartlarını sağlayan amaçların varlığına büyük bir özen gösterilmektedir. Ayrıca veri paylaşımları sırasında mevzuatın gerekliliklerine uygun seviyede güvenlik önleminin sağlanması amacıyla gereken teknik ve idari önlemler alınmaktadır.

Şirket tarafından kişisel veri paylaşımlarının takip edilmesi amacıyla, paylaşım yapılan kişiler aşağıda yer alan kategorilere ayrılmıştır:

Yurtiçi aktarım: Bilindiği üzere, KVKK 8/2.a ve b maddesi gereğince kişisel verilerin KVKK 5/2 ve 6/3 maddesi kapsamında işlenmesi halinde açık rıza alınmaksızın yurtiçinde aktarılması mümkündür. Şirket tarafından ilgili hükümler gözetilerek 3. kişilere aktarım yapılmakta olup, söz konusu hükümler kapsamına girilmemesi halinde ise ilgili kişilerin açık rızasına başvurulmaktadır.

Yurtdışı aktarım: tarafından kural olarak yurtdışı aktarım yapılmamaktadır. Ancak, Şirket tarafından işlenen veri ve belgelerin Şirket dışında bulunan bilgisayarlarda tutulması, e-mail gönderilmesi ve kayıtlara söz konusu bilgisayarlardan erişilmesi, bu verilerin tutulduğu, aktarıldığı sistemlerin ve/veya e-mail sağlayıcılarının veri tabanlarının yurtdışında konumlandırılmış olması mümkün olabilmektedir. İlaveten özellikle yurtdışı organizasyon, etkinlik düzenlemelerinde, otel konaklamaları, vizelerin alınması, uçak biletlerinin alınması, yurtdışı etkinliğin yürütülmesi ve planlanmasında kişisel verilerin yurtdışına aktarılması zarureti bulunabilmektedir. Bu halde ise KVKK'nın9. maddesi hükümlerine riayet edilmek suretiyle aktarım yapılacaktır.

14. AYDINLATMA YÜKÜMLÜLÜĞÜ

KVKK'nın 10. maddesi uyarınca Şirket; kişisel verilerin elde edilmesi sırasında aşağıdaki bilgileri ilgili veri sahiplerine sunarak KVKK'da bahsedilen aydınlatma yükümlülüğünü yerine getirecektir:

Veri sorumlusunun ve varsa temsilcisinin kimliği,
Kişisel verilerin hangi amaçla işleneceği,
İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
Kişisel veri toplamanın yöntemi ve hukuki sebebi,
11 inci maddede sayılan diğer hakları.

Şirket, aydınlatma yükümlülüğünü yerine getirmek amacıyla, Şirket faaliyetlerini yürütürken veri sahipleriyle temas edilen noktalarda kullanılmak üzere uygun aydınlatma metinleri hazırlamakta ve bunları veri sahiplerine sunmaktadır. Ayrıca bu politika da aydınlatma yükümlülüğünün yerine getirilmesi amacına hizmet etmektedir.

15. VERİ SAHİBİNİN HAKLARI

KVKK' nın 11. maddesi kapsamında veri sahiplerine tanınan haklar aşağıda sıralanmaktadır:

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

TR

ENG

Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Şirket, her veri sahibinin KVKK' nın veri sahiplerine tanıdığı hakların rahatça kullanabilmesi konusunda mevzuatın gerekliliklerine uygun olarak gerekli idari ve teknik önemleri almaktadır. Veri sahipleri, yukarıda sayılan haklarını www.zimed.com.tr adresinde yayınlanan ya da Şirket merkezinden temin edebilecekleri başvuru formunu doldurarak aşağıdaki yöntemlerle Şirketimize iletebilirler.

Şirket, kişisel veri sahiplerinin yukarıda sıralanan haklarına ilişkin yazılı olarak ya da Kurul tarafından belirlenecek diğer yöntemlerle iletecekleri taleplerini, iletim tarihinden sonra en kısa sürede ve en geç otuz günde sonuçlandıracaktır. Kurul tarafından yayınlanan tarifeler çerçevesinde veri sahiplerinin başvuruları ücretlendirilebilecektir. İlgili Tebliğ'in 7. maddesi gereğince, İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir.Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez.

Veri sahipleri tarafından yapılan başvuruların yanıtlanması amacıyla Şirket tarafından başvurucunun kimliğinin doğrulanması, ilgisiz kişilere bir başka kişinin kişisel verilerinin hukuka aykırı olarak iletilmesinin önüne geçilmesi ile başvurucu talebinin netleştirilmesi amacıyla ek bilgi ve belge talep edilebilecektir. Söz konusu bilgi ve belgelerin paylaşılmaması halinde veri sahibinin başvurusu cevaplanamayabilecektir.

Başvurunun "kimlik sahibi" ve/veya yetkili kişi tarafından yapılmış olduğunun teyit edilmesi ciddi önem taşımaktadır. Keza amaç kişisel verilerin korunması iken, kimlik doğrulamanın yapılamamasından ötürü 3. kişilere kişisel verilerin verilmesi ve KVKK'nın 11. maddesinde izah edilen haklar dahilinde işlem yapılması ilgili kişinin korunması gereken menfaatini zedeleyecektir. Bu nedenle kimlik doğrulama işlemleri bakımından hassasiyetimizi anlayışla karşılayacağınızı ve Şirketimize yardımcı olacağınızı temenni etmekteyiz.

Şirket, talepleri en kısa sürede ve en geç 30 gün içinde sonuçlandırır. Değerlendirme sonucu yazılı olarak veya elektronik ortamda ilgiliye bildirilir ve talebin kabulü halinde KVKK' ya uygun şekilde gereği yapılır.

Kişisel Veri Sahiplerinin başvurularının reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde ilgili kişi cevabı öğrendiği tarihten itibaren 30 gün içinde Kişisel Verilerin Korunması Kurulu'na KVKK madde 14 uyarınca şikayette bulunabilir.

16. KİŞİSEL VERİLERİN GÜVENLİĞİNE İLİŞKİN TEDBİRLER

Şirket, işlemekte olduğu kişisel verilerin gizliliğinin ve güvenliğinin sağlanması konusunda, bir devlet Şirket olmanın da verdiği sorumluluk bilinciyle, gereken her türlü makul dikkat ve özeni sağlamaktadır. Şirket ,ilgili mevzuatının gerekliliklerı yanında KVKK' nın 12. maddesi çerçevesinde veri gizliliğinin ve güvenliğinin sağlanması için de gereken teknik ve idari tedbirlerini makul düzeyde almaktadır. Söz konusu idari ve teknik güvenlik tedbirleriyle birlikte kişisel verilerin hukuka aykırı işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ile kişisel verilerin uygun güvenlik düzeyinde muhafaza edilmesi hedeflenmektedir.

Şirket, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi (veri işleyen) tarafından işlenmesi hâlinde, yukarıda belirtilen tedbirlerin ilgili veri işleyenler tarafından da alınması için gerekli tedbirleri alacaktır.

Kişisel verilerin üçüncü kişiler tarafından hukuka aykırı olarak ele geçirilmesi halinde, ilgili mevzuat hükümleri uyarınca veri sahiplerine, Kurul'a ve diğer ilgili kamu kurum ve kuruluşlarına bildirimde bulunacaktır.

Kişisel verilerin güvenliğine ilişkin tedbirler alınırken Kurul tarafından yayınlanmış olan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) göz önünde bulundurulma ktadır.

İdari Tedbirler

Şirket bünyesinde bilgi güvenliği yönetim sisteminin kurulması ve işletilmesi,

Şirket personelleri ve ilgili taraflar ile taahhütnameler ve gizlilik sözleşmelerinin imzalanması,

İş süreçleri üzerinde risk analizlerinin gerçekleştirilmesi,

Kişisel veri envanterlerinin oluşturulması,

Bilgi güvenliği politika ve prosedürlerinin işletilmesi,

Bilgi güvenliği ve kişisel veri işleme faaliyetleri hakkında eğitimlerin düzenlenmesi ve değerlendirilmesi,

Çalışan bilgisayar vb. araç gereçlerine yetkisiz erişimlerin önüne geçmek adına söz konusu araç ve gereçleri yalnızca yetkili kişilerin kullanması,

Şirket içi ya da bağımsız denetimler ile faaliyetlerin gözden geçirilmesi,

Yapılan işlemler için objektif delil üretecek kayıtların oluşturulması,

Teknik Tedbirler

Sızma testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.

Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.

Sistemler üzerinde yazılımsal değişiklik ve/veya güncelleme yapılacağı zaman denemeler test ortamında yapılmakta, varsa güvenlik açıkları tespit edilerek gerekli tedbirler alınmakta ve yapılacak değişikliğe son hali bu işlemlerin ardından verilmektedir.

Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlerle ilgili teknik kontroller yapılmaktadır.

Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.

Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından buna uygun hazırlık çalışmaları yapılmıştır.

Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.

Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır.

Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir.

Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

17. İNCELEME VE DENETİM

Şirketimiz bünyesindeki KVKK Komitesi, kişisel verileri koruma kapsamında oluşabilecek hukuki, teknolojik ve organizasyonel değişim ve gelişmeleri takip ederek, şirketimizin bu gelişmelere uyumlu hale gelmesi için gerekli aksiyonların alınmasını sağlamaktadır.

KVK Komitesi, kişisel veri işleme faaliyetleri ile bu faaliyetlere ilişkin her türlü hususu re'sen veya şikayet üzerine inceler, inceleme sonucunda KVK Politikalarında belirlenen kurallara ve/veya mevzuata uygun olmadığı tespit edilen hususlar ve bunlara ilişkin iyileştirme önerileri, KVK Komitesi tarafından yönetime raporlanır. Bu kapsamda gerekli çalışmaların yapılmasını irtibat kişisi takip eder.

KVK Komitesi, Şirketimizin kişisel verilerin korunmasını mevzuata uyumluluğunun teminine yönelik yılda en az (1) kez inceleme gerçekleştirir. Söz konusu inceleme bizzat KVK Komitesi tarafından yapılır.

Söz konusu inceleme faaliyetleri asgari olarak şunlardır;

KVK Politikalarının etkin ve doğru uygulanması, görev ve sorumlulukların yönetimce tayin edilmiş, çalışanlarca üstlenilmiş ve yerine getiriliyor olması,
Çalışanların eğitim ve farkındalık düzeyinin yeterli olması,
Kişisel veri işleme envanteri, aydınlatma beyanları ve diğer belgelerin doğru, eksiksiz ve güncel olması,
Kişisel veri güvenliğine yönelik alınan idari ve teknik tedbirlerin etkin ve yeterli olması,
Hukuki, teknolojik ve organizasyonel gelişmelere karşılık KVKK Politikalarının güncel olması.

İncelemeyi takiben tespit edilen iyileştirme noktaları, KVKK komitesi tarafından yönetime raporlanır ve bu kapsamda gerekli çalışmaların yapılması irtibat kişisi tarafından takip edilir. KVKK komitesi bu tespitler çerçevesinde yönetim onayıyla gerekli iyileştirmelerin yapılmasını sağlar.

18. ÇEREZLER ÜZERİNDEN TOPLANAN KİŞİSEL VERİLERİN İŞLENMESİ

Şirketimiz; Çerezleri, internet sayfalarımız işleyiş biçimini ve kullanımını geliştirmeye yönelik olarak kullanmakta ve dijital platformlarımızda geçirdiğiniz vakti daha verimli ve keyifli hale getirmeye çalışmaktadır.

Ayrıca internet sitelerimiz yaptığınız tercihleri hatırlamaya yönelik bazı çerezlerden yararlanmakta ve bu sayede size geliştirilmiş ve tercihlerinize yönelik kişiselleştirilmiş bir deneyim sağlamaktadır. Dijital platformlarımızda yer alan çerezler üzerinden kişisel verileriniz işlenmekte ve aktarılmaktadır.

Şirketimiz tarafından KVKK madde 12'ye uygun olarak, çerezler üzerinden toplanan kişisel verilerin güvenliğinin sağlanması için gerekli teknik ve idari tedbirler alınmaktadır.

Ayrıntılı bilgi www.zimed.com.tr bağlantısını kullanarak çerez politikamıza erişebilirsiniz.

19. DİĞER HÜKÜMLER

Şirket, bu Politika'nın diğer Şirket politikaları ile uyuşmaması durumunda, her iki politika arasında KVKK veya ilgili ikincil düzenlemeleri dikkate alarak uyum sağlayacaktır. Politika ile mevzuat arasında uyumsuzluk olması durumunda öncelikli olarak ilgili mevzuat uygulanacaktır.

Bu politika yayınlandığı tarihte yürürlüğe girer. Politika zaman içerisinde değişen durum ve ihtiyaçlar kapsamında güncellenebilecektir.

ENG

TR

CONTENTS

PROCESSING AND PROTECTION OF PERSONAL DATA

1. OBJECTİVE AND SCOPE

ZIMED MEDICAL SAN. ve Tic. Ltd. Ltd. Şti. when preparing the "Policy", first of all, it is determined as the basic principle to determine which data, why the working units collect and why they need to transfer this data to third parties within the scope of the Company Organization Chart. When the requirements of the relevant legislation are transferred to "policy ,, the principle has been acquired within the framework of the sensitivity of the need to protect personal data by privatization and why the company provides and why it works. In addition, it is aimed to take the necessary administrative and technical measures to protect data privacy within and outside the organization and to inform and enlighten the data processed.

All real and legal persons whose data are processed by the company are included in the scope of the policy.

Within the scope of this policy, the data processed within the framework of the transactions and activities included in the company organization, the categorization of the data, the data collection groups, the legal reason and method of data collection, third party groups to which the data is transferred, the processing times of the data, the deletion times of the data were tried to include customized information. However, in addition to the current processing activities, it is possible to carry out processing activity and lighting in case of data processing/to be made by the Company, provided that the basic principles and principles specified in this policy are followed. In this case, the lighting will constitute an integral part of this policy and it will not be claimed that it is not included in this policy. As a matter of fact, it is possible to make lighting by using physical or electronic environment such as oral, written, sound recording and call center within the scope of Article 5 of the Communiqué on Procedures and Principles to be followed in the fulfillment of the obligation of lighting.

2. DEFİNİTİONS

Open Consent	It refers to the consent of a particular subject, based on informing and described by free will.
Company	ZİMED MEDİKAL SANAYİ VE TİCARET LİMİTED ŞİRKETİ
Cookie	They are small files that are saved on users on their computers or mobile devices and help store their preferences and other information on the web pages they visit.
Relevant User	The person who is responsible for the technical storage, protection and backeting of the data is the person who processes personal data within the organization or in line with the authorization and instruction received from the data responsible for the data responsible for the except for the unit or unit.
Destruction	Deletion, destruction or anonymous of personal data.
Contact Person	In relation to the obligations of the legal entities settled in Turkey and the obligations of the representative of the Data Officer who is not established in Turkey on the basis of the law and the secondary regulations to be issued based on this law, the real person reported by the Data Officer for the communication to be established during the registration. (The contact person is not authorized to represent the data manager. As the name suggests, he is the person who is assigned to provide "contact ına the communication of the related persons and the institution.)
Law	The Law on the Protection of Personal Data No. 6698 dated March 24, 2016 and numbered 6698 published in the Official Gazette dated April 7, 2016 and numbered 29677.
Registration Environment	Any environment with personal data that is completely or partially automated or is processed by non -automatic ways, provided that it is part of the data recording system.
Personal Data	Any information about the identity of a specific or determined real person.
Personal Data Processing	Obtaining, saving, storage, storage, replacement, reorganization, rearrangement, rearrangement, transmission, transfer, acquiring, acquiring, obtaining, obtained, provided that personal data is completely or partially automated or part of any data recording system. Any process performed on data such as blocking.
Making Personal Data Anonymous	Personal data, even by matching other data, in any way that the identity can not be associated with a specific or specific real person.
Deletion Of Personal Data	Deletion of personal data; Making personal data cannot be inaccessible and reusable for relevant users.
Destruction Of Personal Data	The process of making personal data cannot be accessed, irreversible and reused in any way by anyone.

Board	Personal Data Protection Board.
Special Data	Biometric and genetic data related to the race, ethnic origin, political thought, philosophical belief, religious, sect or other beliefs, disguise, company, foundation or union membership, health, sexual life, criminal conviction and security measures.
Periodic Destruction	The process of erasing, destroying or making anonymously in the case of all the requirements for the processing of personal data and the policy of storing and destruction of personal data and repetitive intervals.
Policy	Personal Data Protection Policy created by the Company.
Data Processing	Based on the authority given by the data officer, the real or legal person who processes personal data on his behalf
Data Registration System	The recording system in which personal data is processed by structured according to certain criteria.
Data Owner/Related Person	The real person whose personal data is processed.
Data Officer	The real or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data registration system.
Regulation	Regulation on deleting, destruction or anonymous of personal data.
Source:	Law No. 6698 on the Protection of Personal Data - Regulation on Deleting, Destruction or Anonymous of Personal Data - Regulation on the Regulation on Data Officers - Procedures and Principles to be Following the Lighting Obligation - Application and Procedural Principles and Procedural Principles Application Procedures and Application Procedures. Communique on Principles

3. DATA OFFİCER ID

Information on the identity of the data officer for any personal data processing activity covered by this policy is given below.

Data Officer	ZİMED MEDİKAL SANAYİ VE TİCARET LİMİTED ŞİRKETİ
Address	Aydınlar Mahallesi 03070 Cad. No :4 ŞEHİTKAMİL/GAZİANTEP
Telephone	0 342 238 43 44
Fax	0 342 238 44 11
Kep	zimedmedikal@hs01.kep.tr
Web	www.zimed.com.tr

4. PERSONAL DATA PROTECTİON ORGANİZATİONAL STRUCTURE

In terms of personal data processing activities within the scope of this policy, Data Officer is Zimed Medical Industry and Trade Limited Company.

Our company has created an organizational structure in order to ensure the sustainable compliance of personal data protection legislation and implemented a compliance program within this scope. Within this framework, a “personal data protection unit ında was established within the“ Administrative Affairs Department of our Company and the liaison person was assigned.

5. PERSONAL DATA PROTECTİON UNİT

A PDPL unit was established within our company in order to show our determination to ensure sustainable compliance with the protection of personal data and to ensure the effectiveness of our personal data protection system. The Chairman of the PDPL Unit and the members of the PDPL Unit are determined by the Board of Directors.

In the event that the PDPL Unit President is not present in our company depending on the permission and/or other reasons, the person who will replace him shall be temporarily appointed by the President of the PDPL Unit. In this case, the temporary person is responsible for the fulfillment of all duties assigned to the PDPL Unit President within the scope of the policy of protection of personal data.

5.1 Contact Person

The contact person has been determined to follow the effectiveness of the measures taken by our company to adapt to the protection of personal data. The main responsibility of the contact person is to work to fulfill the duties and responsibilities of the Central Policies of the PDPL Unit. The contact person becomes a member of the PDPL Unit and calls for the PDPL Unit to the meeting.

The contact person also acts as a contact person within the scope of the PDPL legislation before the registry of the data officers of our company and the Personal Data Protection Board.

If the contact person is not present in our company depending on the permission and/or other reasons, the person who will be replaced by the PDPL unit shall be temporarily appointed by the PDPL unit. In this case, the temporary person is responsible for the fulfillment of all tasks assigned to the contact person within the scope of the policy of the protection of personal data.

6. THE PURPOSES OF PROCESSİNG YOUR PERSONAL DATA, YOUR PERSONAL DATA, COLLECTİON METHODS, AND LEGAL REASONS

6.1 Purpose Of Processing

Your personal data is observed in the process of processing personal data by complying with the limits envisaged in PDPL; In accordance with the law and the rules of honesty, correct and when necessary, in the framework of current, specific, clear and legitimate purposes, it is carried out in a limited, limited and moderate personal data processing activity, and maintains personal data for the time required by the laws or required for personal data processing.

Our company, including our customers who benefit from their products and services, but not limited to them, our potential customers, employees, trainees, employees, shareholders, authorities, suppliers, consultants, authorities, authorized vendors, our employees, shareholders, authorities, authorities, visitors, visitors, visitors, visitors Our users who visit our site, in short during our activities, personal information of the people who are in contact with our company; Identity, contact information, usage habit of all kinds of products within the framework of activity, financial data, health data, demand and complaint management data, such as data owners, data owners to benefit from zimed medical products and services, marketing, work of the work, instead of contract requirements In order to fulfill the financial and legal obligations of the company, it works based on the following criteria provided that it is necessary to consent to the data holders and to consent in accordance with the law.

Our Company provides personal data limited to the purposes and conditions within the personal data processing conditions specified in Article 5 and Article 6 of Article 5 of Article 5 and Article 6 of the Article 6. These aims and conditions are as follows;

Fulfilling the requirements of contracts,
Research, Development and Production Activities,
Performing invoice arrangement and collection procedures,
Execution of after -sales services,
Customers; Providing various advantages through product, service presentation, information, advertising, campaigns and other benefits, sending commercial electronic messages, survey applications, statistical analysis,
Studies to improve the quality of service and provide better service,
Service purchasing from outsourcing,

Identity confirmation,
Evaluation and response of requests and complaints,
Providing financial agreement with the relevant business partners and other third parties,
Provision of the necessary information in line with the demands and inspections of the official authorities,
Measurement of customer satisfaction,
In terms of employees; The creation of the personal file, determining whether or not to fulfill the requirements of the work, the creation of a health file, taking occupational safety measures,
Execution of application processes in terms of employee candidates and trainees,
Planning of human resources processes,
Execution of information security processes,
Fulfilling legal obligations,
Execution/tracking of reporting and risk management transactions
Execution/follow -up of legal affairs,
Creation and follow -up of visitor records
Execution of storage and archive activities.

6.2 Processing Your Personal Data

Identity Information: Your name, your surname, T.C. Identity number, mother name, father name, birthplace and date, personnel registry number, national information and other information provided to the Company within your consent by you.

Contact Information: Your residence address, your workplace address, your phone number and your e-mail address, if you have to communicate with your side if you have a mobile phone number, fax number, or other contact channels you have obtained with your consent so that you can reach you.

Your Labor and Training Information: Application Form for Application to the Company (Job Application, Participation in Participation in Trainings without Certified/Participation)) Within the scope of the registration document and/or other online or physical online or physical online or other physical Application procedures by using your identity information, information about your business status, contact information with your educational status (such as university graduate, graduate graduate) and past graduation information, course/seminar information you attended, certificate information and national or international exam results.

Your Financial/Financial Information: Obtained for payments such as payment of salary and subsidiary rights, refund of more and out of place; Bank Name and Branch Information, Bank Account No Information, IBAN Number Information.

Visual/Audio Information: In relation to the event in conferences, seminars and similar activities organized by the Company; Introducing the activity, announcement and spreading, the static or flowing images and/or sounds of the place where the event takes place and the participants, and the visual/auditory information provided by the cameras established to ensure security in the company center, branches and representative offices. The visual/auditory information obtained in these activities will not exceed the company activities and will be limited to the purpose of the event on the company's website, social networking platforms used by the company and in the works printed by the company. Or by the permission and control of the Company, it can be sent to the third parties for publication/publication. This usage procedure will not include security camera images, and before the use of the relevant visual/auditory personal data (for example;

Specıal Qualıty Personal Data: In order to fulfill the obligations of the legislation within the company within the company, the personal data regarding the criminal conviction and safety measures regarding the disabled and/or security measures imposed on the disabled and/or safety measures are produced, our company manufactures medical medical products. In order to prevent infectious diseases, a health report is requested and regular health checks are passed.

Although the Company is not the purpose of processing any other personal data directly, the identity certificate you have submitted to the Company, photos or activities within the scope of stable/flowing images within the scope of the data obtained indirectly within the scope of the data obtained within the scope of the religion, disguise, philosophical,

philosophical Faith, political thought and health data (for example, apparently understood from photography, devices and prostheses) and a special quality information you have specified in a document provided by the company.

6.3 Collection Methods Of Your Personal Data

Your personal data, job application form, job application forms filled on the internet, security camera recordings and the official e-mail address of the COMPANY, info@zimed.com.tr , zimeddikal@hs01.kep.tr KEP address or +90 342 238 44 11 In case of sending personal data to the fax address, it is collected through the said communication channels.

Personal data is also collected by physically sending documents, physically filling out a document provided by the company, calling the lines , +90 342 238 43 44 or other internal numbers belonging to the company.

Your personal data is also collected automatically via the cookies used in https://www.zimed.com.tr and its extensions. These cookies are only necessary for the visitor to use the site with full efficiency and are used to remember the visitor's preferences and do not provide any other personal data. You can reach our cookie policy at www.zimed.com.tr.

6.4 Legal Reasons For Personal Data Processing

PDPL lists the processing conditions of personal data in paragraph 2 of Article 5. If the purposes of processing personal data by a data controller can be evaluated within the framework of the personal data processing conditions listed in the PDPL, that data controller can process personal data in accordance with the law. In this context, personal data processing activities are carried out by the Company in cases where the personal data processing purposes pursued by the Company can be evaluated within the scope of the personal data processing conditions regulated in PDPL. The company does not engage in any personal data processing activities that do not fall within the scope of personal data processing conditions.

The personal data processing conditions in PDPL are as follows;

Having the explicit consent of the person concerned,
It is clearly stipulated in the laws,
It is compulsory for the protection of the life or physical integrity of the person or another person, who is unable to express his consent due to actual impossibility or whose consent is not legally recognized,
It is necessary to process the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,
It is mandatory for the data controller to fulfill its legal obligation,
It has been made public by the data owner himself,
Data processing is mandatory for the establishment, exercise or protection of a right,
Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data owner.

The basic processing condition for sensitive personal data is express consent and the Company does not basically aim to process sensitive personal data. However, your personal data of special nature, which we have to process due to our activities or that you have given your consent with your explicit consent, are also processed in a measured manner within the scope of the legislation.

The conditions listed in the PDPL for the processing of special quality personal data are as follows;

Having the explicit consent of the person concerned,
Explicitly stipulated in laws for personal data of special nature other than health and sexual life,
Personal data related to health and sexual life, however,
Protection of public health,
Preventive medicine,
Medical diagnosis,
Execution of treatment and care services,
For the purpose of planning and managing health services and financing,
It can be processed by persons or authorized institutions and organizations under the obligation of secrecy without seeking the explicit consent of the person concerned.

One or more personal data processing conditions that make a personal data processing activity lawful may exist at the same time.

In order to realize our aforesaid purposes, it is necessary to process your data, which we mentioned above. While transferring identity information to our company, data that is not actually within our processing purposes can also be transferred to us. Within the scope of administrative and technical measures, we delete and/or anonymize the data in question at the end of the periods stipulated in the legislation, but it is not possible to ensure this in all circumstances. In this case, it is necessary to apply for your explicit consent in order to process the data in question.

7. TRANSFER OF PERSONAL DATA

Your personal data is shared with authorized public institutions and organizations, judicial authorities, execution authorities, law enforcement units and suppliers from whom contracted products and services are purchased, when necessary and through the means here, for the purposes indicated in this Clarification Text. Our company can transfer the personal data and sensitive personal data of the personal data owner to third parties by taking the necessary security measures in line with the personal processing purposes in accordance with the law. Personal data may be transferred to third parties by our company, provided that legal, technical and administrative measures are taken in accordance with the current legislation and regulations, even without the explicit consent of the data owner, if one or more of the following conditions are present.

The relevant activities regarding the transfer of personal data are clearly stipulated in the laws,
The transfer of personal data by the company is directly related to and necessary for the establishment or performance of a contract,
The transfer of personal data is mandatory for our company to fulfill its legal obligations,
The personal data has been made public by the data owner,
The transfer of personal data by the company is mandatory for the establishment, use or protection of the rights of the company or the data owner or 3rd parties,
It is obligatory to transfer personal data for the legitimate interests of the company, provided that it does not harm the fundamental rights and freedoms of the data owner.
The person who is unable to express his consent due to actual impossibility or whose consent is not given legal validity is compulsory for the protection of himself or someone else's life or physical integrity.

In addition to the above, personal data may be transferred to foreign countries declared to have adequate protection by the Board in case of any of the above conditions. In the absence of sufficient protection, in line with the data transfer conditions stipulated in the legislation, data controllers in Turkey and in the relevant foreign country may be transferred to foreign countries where they have committed in writing and where the board has permission.

8. TRANSFER OF PERSONAL DATA WİTH SPECİAL QUALİFİED

Sensitive personal data may be transferred by our company in accordance with the principles set forth in this policy, by taking all necessary administrative and technical measures, including the methods to be determined by the board, and in the presence of the following conditions;

Special categories of personal data other than health and sexual life may be processed without the explicit consent of the data owner, provided that it is expressly stipulated in the law. Otherwise, the explicit consent of the data owner will be obtained.
Sensitive personal data regarding health and sexual life may be disclosed by persons or authorized institutions and organizations under the obligation of keeping secrets for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and these services. may be processed without consent. Otherwise, the explicit consent of the data owner will be obtained. In addition to the above, personal data may be transferred to foreign countries with adequate protection in the presence of any of the above conditions. In the absence of sufficient protection, in line with the data transfer conditions stipulated in the legislation, it can be

transferred to foreign countries where the data controllers in Turkey and the relevant foreign country undertake adequate protection in writing and where the data controller is committed to adequate protection.

9. THE RİGHTS OF THE RELATED PERSON

Within the scope of PDPL;

Learning whether your Personal Data is processed or not,
If your Personal Data has been processed, requesting information about it,
To learn the purpose of processing your Personal Data and whether they are used in accordance with its purpose,
Knowing the third parties to whom your Personal Data is transferred, at home or abroad,
Requesting correction of your Personal Data if it is incomplete or incorrectly processed,
Requesting the deletion or destruction of your Personal Data within the framework of the conditions stipulated in the PDPL legislation,
v. and vi. Requesting notification of the transactions made within the scope of the articles to the third parties to whom your Personal Data has been transferred,
Objecting to the emergence of a result against you by analyzing the processed data exclusively through automated systems,
If you suffer damage due to the illegal processing of your Personal Data, you have the right to demand the removal of this damage.

How Can You Exercise Your Rights?

You can fill in the application form, which you can download from our company's website (using the link www.zimed.com.tr), in line with your request/complaint, and send the said form to us via e-mail address (info@zimed.com.tr), or fill the form physically and send it to Aydınlar Mah. 03070 Cad. No.: 4 ŞEHİTKAMİL 27580 GAZİANTEP/TURKEY via cargo/mail.

If you submit your request to us using one of the methods shown above, PDPL art. In accordance with 13/2, your request will be evaluated within 30 days at the latest and you will be informed about the subject. If your request is accepted, the necessary actions will be carried out immediately by the data controller company.

As a rule, requests are met free of charge; As stipulated in article 7 of the Communiqué; "If the application of the person concerned is to be answered in writing, no fee is charged for up to 10 pages. A transaction fee of 1 TL may be charged for each page over 10 pages. If the response to the application is given in a recording medium such as CD or flash memory, the fee that may be requested by the data controller cannot exceed the cost of the recording medium. In accordance with its provisions, a fee may be requested by the COMPANY.

10. LEGAL EXCEPTİONS AND OPEN CONSENT İN THE PROCESSİNG OF PERSONAL AND SPECİAL PERSONAL DATA

The PDPL has stated that the data processing activity can be carried out without the explicit consent of the data controller in the cases listed below.

Considering the processing purposes and conditions specified in this Policy, there is no need to obtain the consent of the data subjects in terms of data processing conditions that fall within the scope of legal exceptions. However, eliminating the conflicts that may arise from the interpretation of the exceptions and processing principles, while some of the data in a document is included in the scope of the exception, the other part is not considered as an exception, the concept of legitimate interest of the data controller is interpreted differently, the case law and high court decisions within the scope of the PDPL and its relevant legislation. few in number; When the legally required data to be processed, stored and transferred are not counted one by one in the regulatory proceedings, the retention periods are not specified and/or they are vague and/or demanded in actual practice and the sanctions are severe, the company adopts the method of applying for the "explicit consent" of the persons concerned as a principle. is desired.

However, this situation should not be interpreted as that the company will not benefit from the exception provisions and/or will choose the path of obtaining explicit consent in any case. The company will be able to benefit from the processing activities within the scope of the legal exception without obtaining explicit consent.

10.1 Processing Of Personal Data Without Clear Consent

In the presence of one of the following conditions, it is possible to process personal data without seeking the explicit consent of the data subject:

Explicitly stipulated by law.

It is compulsory for the protection of life or physical integrity of the person or another person, who is unable to express his consent due to actual impossibility or whose consent is not legally recognized.

It is necessary to process the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract.

It is mandatory for the data controller to fulfill its legal obligation.

The person concerned has been made public by himself.

Data processing is mandatory for the establishment, exercise or protection of a right.

Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

10.2 Processing Of Special Data Without Clear Consent

Data on people's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, disguise and clothing, membership of companies, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data are privately owned. qualified personal data.

Personal data other than the above-mentioned health and sexual life may be processed without seeking the explicit consent of the person concerned, in cases stipulated by the laws.

Personal data related to health and sexual life are only subject to the explicit consent of the person concerned by persons under the obligation of keeping confidentiality or authorized institutions and organizations for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing. can be processed without calling.

Adequate measures determined by the Board must also be taken in the processing of special categories of personal data.

10.3 The Full Exception Of The PDPL Law Will Not Be Applied

Processing of personal data by real and legal persons within the scope of activities related to themselves or their family members living in the same residence, provided that they are not given to third parties and that the obligations regarding data security are complied with.

Processing personal data for purposes such as research, planning and statistics by making them anonymous with official statistics.

Processing of personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime.

Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public safety, public order or economic security.

Processing of personal data by judicial authorities or execution authorities in relation to investigation, prosecution, trial or execution proceedings.

10.4. Part Of Exceptional States

In accordance with the purpose and basic principles of the PDPL, Articles 10, which regulates the obligation of disclosure of the data controller, 11, which regulates the rights of the data subject, except for the right to demand the compensation of the damage, and 16, which regulates the obligation to register in the Data Controllers Registry, are not applied in the following cases:

The processing of personal data is necessary for the prevention of crime or for criminal investigation.

Processing of personal data made public by the person concerned.

The processing of personal data is necessary for the execution of supervisory or regulatory duties and for disciplinary investigation or prosecution by the authorized and authorized public institutions and organizations and professional organizations in the nature of public institution, based on the authority given by the law.

The processing of personal data is necessary for the protection of the economic and financial interests of the State with regard to budgetary, tax and financial matters.

11. GENERAL INFORMATİON ON THE PROCESSİNG OF PERSONAL DATA

11.1 Channels İn Which Personal Data Are Obtained

The channels for obtaining personal data within the company's activities are listed below:

Meeting Minutes of the Board of Directors and other Administrative Units
Executive Board, Departments and Working Groups Activity Documents, Meeting Minutes and Working Documents
Personnel File Documents of the Employees
Financial Data for Execution of Operations and Contractual Transactions
Business cards
CCTV (Closed Circuit Camera Recordings),
SMS/E-Mail, Phone
Website, Applications, Cookies a nd Similar Tracking Technologies (ERP),
Fax,
Postal, Cargo or Courier Services,
Other Physical and Electronic Media.

Depending on the technological developments, new additions to the above personal data acquisition channels may be made by the company or the use of some of the existing channels may be waived. In such cases, in order to maintain transparency and accountability, the channels used will be accurately expressed by updating the Policy.

12. STORİNG AND DİSPOSAL OF PERSONAL DATA

The Company stores the personal data of the data subjects whose personal data it processes, in electronic and physical environments, by taking the necessary technical and administrative security measures.

The company's personal data storage period is calculated by taking into account the periods determined in the relevant legislation. However, it is important for the Company to be in contact with individuals in order to carry out the Company's activities in order to realize the purpose in the Company's legislation. For this reason, apart from the periods stipulated in the relevant legislation, the Company wishes to keep the "name/surname/duty/contact" information by always updating it by obtaining the "explicit consent" of the individuals.

In the event that the personal data processing purposes that will eliminate the existence of the personal data processing conditions in the PDPL are terminated, the personal data will be destroyed by the Company. The destruction processes in question are carried out in 6-month periods in accordance with the provisions of the relevant legislation or are finalized if the requests from the data owners require it. Pursuant to Article 12 of the Regulation, the Company shall fulfill the request for deletion and/or destruction of the person concerned within 30 days at the latest, unless another period is stipulated in the legislation, and inform the person concerned.

The minutes regarding the destruction of Personal Data will be kept for 3 years unless another period is determined by the Company in accordance with the legislation.

The destruction of personal data by the company is carried out by using deletion, anonymization or destruction techniques according to the environments in which the personal data is located. Detailed information about the aforementioned techniques is included in the Guide for Deletion, Destruction or Anonymization of Personal Data published by the Board.

The process of making personal data inaccessible and unusable for the relevant users is called deletion of personal data. Relevant User is the person who processes personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data. In this case, the "Deletion" procedure will be applied primarily within the scope of the processing purposes of the data within the scope of the Company's destruction system.

7/5 of the Regulation on the Deletion, Destruction or Anonymization of Personal Data. In the event that the reasons for data processing disappear and/or upon the request of the person concerned (if it is not within the scope of the legal exception within the scope of Article 28 of the PDPL) Personal data will be deleted by the "PDPL Unit" in a way that makes it inaccessible and unusable for the relevant users in any way.

Although the main method of destruction for the COMPANY is "deletion", if all conditions are met and found appropriate as a result of the evaluation, "destruction" or "anonymization" destruction procedures can also be applied by the COMPANY.

13. SHARİNG PERSONAL DATA WİTH THİRD PARTİES

Due to the requirements of the Company's activities, the Company may share personal data with persons/institutions in the country or abroad. In order to realize the aforementioned shares, the Company pays great attention to the requirements of PDPL and the existence of purposes that meet the data processing conditions. In addition, necessary technical and administrative measures are taken in order to ensure the level of security measures in accordance with the requirements of the legislation during data sharing.

In order to track personal data sharing by the company, the people shared are divided into the following categories:

Domestic transfer: As it is known, in accordance with Article 8/2.a and b of the PDPL, it is possible to transfer the personal data domestically without obtaining explicit consent, if the personal data is processed within the scope of Articles 5/2 and 6/3 of the PDPL. The Company transfers to third parties by observing the relevant provisions, and if the said provisions are not covered, the explicit consent of the relevant persons is sought.

International transfer: As a rule, international transfers are not made. However, it may be possible to keep the data and documents processed by the Company on computers located outside the Company, to send e-mails and to access the records from the said computers, and to have the databases of the systems and/or e-mail providers located abroad, where this data is kept and transferred. In addition, it may be necessary to transfer personal data abroad, especially in international organization, event arrangements, hotel accommodation, obtaining visas, purchasing airline tickets, and conducting and planning international events. In this case, the 9th article of the PDPL. The transfer will be made in accordance with the provisions of the article.

14. LİGHTİNG OBLİGATİON

Pursuant to Article 10 of the PDPL, the Company; will fulfill the obligation of disclosure mentioned in PDPL by presenting the following information to the relevant data owners during the acquisition of personal data:

Identity of the data controller and its representative, if any,
For what purpose personal data will be processed,
To whom and for what purpose the processed personal data can be transferred,
Method and legal reason for collecting personal data,
Other rights listed in Article 11.

In order to fulfill its obligation of disclosure, the Company prepares appropriate disclosure texts to be used at the points of contact with data owners during the Company's activities and presents them to the data owners. In addition, this policy also serves the purpose of fulfilling the obligation to inform.

15. DATA OWNER'S RİGHTS

The rights granted to data owners within the scope of Article 11 of PDPL are listed below:

Learning whether personal data is processed or not,
If personal data has been processed, requesting information about it,
To learn the purpose of processing personal data and whether they are used in accordance with the purpose,
Knowing the third parties to whom personal data is transferred in the country or abroad,
Requesting correction of personal data in case of incomplete or incorrect processing,
Requesting the deletion or destruction of personal data, in case the reasons requiring the processing of personal data processed in accordance with the provisions of the PDPL and other relevant laws disappear, and requesting the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,
Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,
Requesting the compensation of the damage in case of loss due to unlawful processing of personal data.

The Company takes the necessary administrative and technical measures in accordance with the requirements of the legislation so that each data owner can comfortably exercise the rights granted to data owners by the PDPL. Data

owners can convey their above-mentioned rights to our Company by filling out the application form published on www.zimed.com.tr or obtaining from the Company's headquarters, using the following methods.

The Company will finalize the requests of personal data owners regarding the rights listed above, in writing or by other methods to be determined by the Board, as soon as possible and within thirty days at the latest after the date of transmission. Applications of data owners may be charged within the framework of the tariffs published by the Board. Pursuant to Article 7 of the relevant Communiqué, if the application of the relevant person is to be answered in writing, no fee is charged for up to ten pages. A processing fee of 1 Turkish Lira may be charged for each page over ten pages. If the response to the application is given in a recording medium such as CD or flash memory, the fee that may be requested by the data controller cannot exceed the cost of the recording medium.

In order to respond to the applications made by the data owners, additional information and documents may be requested by the Company in order to verify the identity of the applicant, to prevent unlawful transmission of another person's personal data to unrelated persons, and to clarify the applicant's request. If the said information and documents are not shared, the application of the data owner may not be answered.

Confirmation that the application has been made by the “identity holder” and/or the authorized person is of serious importance. Likewise, while the purpose is to protect personal data, giving personal data to third parties due to the inability to verify identity and taking action within the rights set forth in Article 11 of the PDPL will harm the interests of the person concerned. For this reason, we hope that you will understand our sensitivity in terms of identity verification processes and that you will help our Company.

The company concludes requests as soon as possible and within 30 days at the latest. The result of the evaluation is notified to the person concerned in writing or electronically, and if the request is accepted, necessary action is taken in accordance with the PDPL.

In the event that the applications of the Personal Data Owners are rejected, the response is found insufficient or the application is not answered in due time, the person concerned may file a complaint with the Personal Data Protection Board in accordance with Article 14 of the PDPL, within 30 days from the date of learning the answer.

16. MEASURES RELATED TO THE SECURİTY OF PERSONAL DATA

The Company provides all reasonable care and attention to ensure the confidentiality and security of the personal data it processes, with the awareness of its responsibility as a government company. In addition to the requirements of the relevant legislation, the Company takes the necessary technical and administrative measures at a reasonable level to ensure data privacy and security within the framework of Article 12 of the PDPL. Along with the said administrative and technical security measures, it is aimed to prevent the unlawful processing of personal data, to prevent illegal access to personal data, and to preserve personal data at an appropriate level of security.

In the event that personal data is processed by another natural or legal person (data processor) on its behalf, the Company will take the necessary measures to ensure that the above-mentioned measures are also taken by the relevant data processors.

In the event that personal data is unlawfully obtained by third parties, it will notify the data owners, the Board and other relevant public institutions and organizations in accordance with the provisions of the relevant legislation.

The Personal Data Security Guide (Technical and Administrative Measures) published by the Board is taken into consideration when taking measures regarding the security of personal data.

Administrative Measures

Establishment and operation of the information security management system within the company,
Signing undertakings and confidentiality agreements with company personnel and related parties,
Performing risk analyzes on business processes,
Creation of personal data inventories,
Operation of information security policies and procedures,
Organizing and evaluating trainings on information security and personal data processing activities,
Working computer etc. In order to prevent unauthorized access to the equipment, only authorized persons should use the said tools and equipment,
Reviewing activities with internal or independent audits,
Creating records that will produce objective evidence for the transactions,

Teknik Tedbirler

Risks, threats, vulnerabilities and vulnerabilities, if any, regarding the Company's information systems are revealed through penetration tests, and necessary precautions are taken.

Risks and threats that will affect the continuity of information systems are constantly monitored as a result of real-time analyzes with information security incident management.
Access to information systems and authorization of users are made through security policies through access and authorization matrix and corporate active directory.
When software changes and/or updates are to be made on the systems, tests are made in the test environment, security vulnerabilities are detected, necessary measures are taken, and the final version of the changes to be made is given after these processes.
Necessary measures are taken for the physical security of the company's information systems equipment, software and data.
In order to ensure the security of information systems against environmental threats, hardware (access control system that allows only authorized personnel to enter the system room, physical security of the edge switches that make up the area network, fire extinguishing system, air conditioning system, etc.) and software (firewalls, attack prevention systems) , network access control, systems that prevent malicious software, etc.) measures are taken.
Risks to prevent unlawful processing of personal data are determined, appropriate technical measures are taken for these risks, and technical controls are carried out regarding the measures taken.
By establishing access procedures within the company, reporting and analysis studies are carried out regarding access to personal data.
The Company takes the necessary measures to make the deleted personal data inaccessible and reusable for the relevant users.
In case personal data is obtained unlawfully by others, the Company has made appropriate preparations to notify the relevant person and the Board.
Security vulnerabilities are followed and appropriate security patches are installed and information systems are kept up-to-date.
Strong passwords are used in electronic environments where personal data is processed.
Secure record keeping (logging) systems are used in electronic environments where personal data is processed.
Data backup programs are used to keep personal data safe.
Access to personal data stored in electronic or non-electronic media is limited according to access principles.
It is encrypted with SHA 256 Bit RSA algorithm using secure protocol (HTTPS) for accessing the company website.
A separate policy has been determined for the security of sensitive personal data.
Trainings on special quality personal data security were given to employees involved in special quality personal data processing, confidentiality agreements were made, and the authorizations of users who have access to data were defined.
Electronic environments in which sensitive personal data are processed, stored and/or accessed are preserved using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of environments are constantly monitored, necessary security tests are regularly performed/have the test results, to be registered,
Adequate security measures are taken for the physical environments where sensitive personal data is processed, stored and/or accessed, and unauthorized entries and exits are prevented by ensuring physical security.
If sensitive personal data needs to be transferred via e-mail, they are transferred in encrypted form with a corporate e-mail address or by using a KEP account. If it needs to be transferred via media such as portable memory, CD, DVD, it is encrypted with cryptographic methods and the cryptographic key is kept in a different environment.
If transferring is carried out between servers in different physical environments, data transfer is carried out by establishing a VPN between servers or using the sFTP method.
If it is required to be transferred via paper media, necessary precautions are taken against the risks such as theft, loss or viewing of the document by unauthorized persons, and the document is sent in a “confidential” format.

17. REVİEW AND AUDİT

The PDPL Committee within our company monitors the legal, technological and organizational changes and developments that may occur within the scope of personal data protection, and ensures that the necessary actions are taken in order for our company to comply with these developments.

ENG

TR

The KVK Committee examines personal data processing activities and all matters related to these activities, ex officio or upon complaint, and the issues that are found to be inconsistent with the rules and/or legislation determined in the KVK Policies as a result of the examination and the improvement suggestions regarding these are reported to the management by the KVK Committee. In this context, the contact person monitors the execution of the necessary work.

The KVK Committee conducts an examination at least (1) time a year to ensure the compliance of our Company with the legislation on the protection of personal data. The said review is carried out by the KVK Committee itself.

The said inspection activities are at least as follows;

Effective and correct implementation of KVK Policies, duties and responsibilities assigned by the management, undertaken and fulfilled by the employees,

The level of education and awareness of the employees is sufficient,

Personal data processing inventory, disclosure statements and other documents are correct, complete and up-to-date,

Effective and sufficient administr ative and technical measures taken for personal data security,

Keeping PDPL Policies up-to-date in response to legal, technological and organizational developments.

The improvement points determined following the review are reported to the management by the PDPL committee and the necessary work is followed up by the contact person. Within the framework of these determinations, the PDPL committee ensures that the necessary improvements are made with the approval of the management.

18. PROCESSİNG OF PERSONAL DATA COLLECTED THROUGH COOKİES

Our company; It uses cookies to improve the functioning and use of our internet pages and tries to make the time you spend on our digital platforms more productive and enjoyable.

In addition, our websites make use of some cookies to remember the preferences you have made, thus providing you with an improved and personalized experience for your preferences. Your personal data is processed and transferred through cookies on our digital platforms.

Necessary technical and administrative measures are taken by our company to ensure the security of personal data collected through cookies, in accordance with Article 12 of the PDPL.

Detailed information You can access our cookie policy by using the link www.zimed.com.tr.

19. OTHER PROVİSİONS

In the event that this Policy does not comply with other Company policies, the Company will comply between both policies by taking into account the PDPL or related secondary regulations. In case of inconsistency between the policy and the legislation, the relevant legislation will be applied first.

This policy is effective on the date of publication. The policy may be updated over time within the scope of changing situations and needs.