**YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**ÖZEL NİTELİKLİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**

**ÖZEL NİTELİKLİ KİŞİSEL VERİ YÖNETİMİ POLİTİKASI**

**A. KAPSAM**

1. İşbu Özel Nitelikli Kişisel Veri Yönetimi Politikası ("**Politika**") YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ ("**Şirket**") bünyesinde kişisel verileri işleyen herhangi bir sürece dâhil olan tüm departmanları, çalışanları ve 3. tarafları kapsamaktadır.

2. İşbu Politika; Şirket'in özel nitelikli kişisel verilerin güvenliğine yönelik kuralları tanımlayacak ve bu alandaki yönetimi sağlayacak tüm faaliyetleri kapsayacak olup, bunu sürdürmek adına her adımda uygulanacaktır.

3. İşbu Politika özel nitelikli kişisel veri olmayan veriler hakkında uygulanmayacaktır.

4. Konuyla alakalı yeni mevzuatın belirlenmesi veya ilgili mevzuatın güncellenmesi durumunda, Şirket politikasını ilgili mevzuata uyumlu olacak şekilde güncelleyerek mevzuat gerekliliklerine uyacaktır.

5. İşbu Politika'nın Şirket tarafından uygulanmasında hukuki bir engel olduğuna kanaat getirildiği durumlarda, Şirket uygulayacağı adımları, gerek görmesi durumunda İşbu Politika'yı yeniden belirleyebilecektir.

**B. TANIMLAR**

**Kanun :** 6698 Sayılı Kişisel Verilerin Korunması Kanunu'dur.

**Yönetmelik :** Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik'tir.

**İlgili Karar :** "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31.01.18 tarihli, 2018/10 sayılı kararıdır.

**Kurul :** Kişisel Verileri Koruma Kurulu'dur.

**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 ortama verilen addır.

**Kişisel Veri :** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir ve kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hallerini kapsar.

**Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçlarını, veri kategorisini, aktarılan alıcı grubunu ve veri konusunu kişi grubuyla ilişkilendirerek oluşturan ve detaylandıran envanterdir.

**Özel Nitelikli Kişisel Veri:** Kanun’da belirtilen özel nitelikli kişisel veriler, işlenmeleri halinde sahipleri hakkında ayrımcılık yapılmasına neden olma riski taşıyan verilerdir.

**Sicil :** Başkanlık tarafından tutulan Veri Sorumluları Sicilidir (VERBİS).

**Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

**Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.

**Alıcı Grubu :** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

**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.

Şirket bünyesinde oluşturulmuş Kişisel Verilerin Korunması ve İşlenmesi Politikası ile Kişisel Veri Saklama ve İmha Politikası içerisinde bulunan tanımlar işbu Politika için de geçerlidir.

**C. AMAÇ VE KAPSAM**

İşbu Politika, Kanunun 6. Maddesinde belirtilen "Özel Nitelikli Kişisel Verilerin” işlenmesi şartları kapsamında Şirket ve ile Şirket'in sözleşmesel olarak sorumlu kıldığı üçüncü kişiler tarafından uyulması gereken esasları belirlemektedir.

Kişisel Verileri Koruma Kurulu'nun 07.03.2018 tarihli Resmi Gazete' de yayımlanan, 31.01.2018 tarihli Kararı uyarınca Şirket, Sicile kayıt yükümlülüğü olan bir Veri Sorumlusu olarak, uhdesinde bulunan özel nitelikli kişisel verileri; kişisel veri işleme envanterine uygun bir şekilde saklamaktan, bu verilerin güvenliğine yönelik kuralları tanımlamaktan ve yönetimini sağlayacağı tüm faaliyetleri kapsayarak, bunu sürdürmek adına uygulayacak bir Politika hazırlayarak bu Politika’ya uygun hareket etmekten yükümlüdür.

Kişisel verilerin saklanması ve imhasında aşağıdaki ilkeler geçerli olacaktır:

*a) Kanunun 4 üncü maddesindeki genel ilkelere uyulacaktır.*

*b) Şirket, işbu Politikayı hazırlamış olmanın tek başına kişisel verilerin Yönetmelik, Kanun ve ilgili mevzuata uygun olarak silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmeyeceğini kabul etmektedir.*

*c) Şirket, kişisel verileri saklarken yahut silerken, yok ederken veya anonim hale getirirken, Kanunun 12. Maddesinde yer alan güvenlik tedbirlerine, ilgili mevzuatta yer alan hükümlere, Kişisel Verileri Koruma Kurulu'nun alacağı kararlara, Veri Güvenliği Rehberi'nde belirtilen İdari ve Teknik Tedbirlere ve Politikaya uygun hareket edeceğini kabul, beyan ve taahhüt eder.*

*d) Şirket, bünyesinde bulundurduğu kişisel verilerin amacı tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işle nen kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi sırasında; İşbu Politika'ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.*

**D. KAYIT ORTAMLARI**

Şirket, işbu Politika ile kişisel veri içeren ve aşağıda sayılmış olan ortamlar ve bunlara ek olarak ortaya çıkabilecek diğer ortamlardaki kişisel verileri Politikanın kapsamına dahil etmeyi kabul eder.

*a) Şirket adına kullanılan bilgisayarlar / sunucular*

*b) Ağ cihazları,*

*c) Ağ üzerinde veri saklanması için kullanılan paylaşımlı / paylaşımsız disk sürücüleri,*

*d) Mobil telefonlar ve içerisindeki tüm saklama alanları,*

*e) Kağıt,*

*f) Yazıcı, parmak izi okuyucu gibi çevre birimler,*

*i) Optik diskler,*

*j) Flash hafızalar.*

**E. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ**

**1. Özel Nitelikli Kişisel Veri İşlenmesine İlişkin Genel İlkeler**

1. **Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler**

Şirket, kişisel verilerin işlenmesine ilişkin KVK Kanunu’nda belirtilen genel ilkelere uymakla yükümlüdür. Bu kapsamda Şirket, özel nitelikli kişisel veriler işlerken aşağıdaki ilkelere uygun olarak hareket edecektir:

* *Hukuka ve dürüstlük kuralına uygun olarak kişisel verileri işleme,*
* *Kişisel verilerin doğru ve gerektiğinde güncel olmasını sağlama,*
* *Kişisel verileri belirli, açık ve meşru amaçlarla işleme,*
* *Kişisel verileri işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak işleme,*
* *İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza etme.*

1. **Özel Nitelikli Kişisel Verileri İşleme Şartları**

Şirket, yukarıda bahsedilen genel ilkeler ile beraber KVK Kanunu’nun 6. maddesinde belirtilen şartlara uygun olarak özel nitelikli kişisel verileri işlemekle yükümlüdür. Bu kapsamda Şirket, aşağıdaki şartlardan birine dayalı olarak özel nitelikli kişisel verileri işleme faaliyeti yürütebilecektir:

*a) İlgili kişinin açık rızasının olması,*

*b) Kanunlarda açıkça öngörülmesi,*

*c) 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,*

*ç) İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması,*

*d) Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,*

*e) Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması,*

*f) İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması,*

*g) Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması,*

1. **Özel Nitelikli Kişisel Verilerin Aktarılması**

Şirket, özel nitelikli kişisel verileri KVK Kanunu’nun 8. ve 9. maddelerinde belirtilen veri işleme şartlarına uygun olarak üçüncü kişiler ile paylaşabilecektir. Özel nitelikli kişisel verileri üçüncü kişilere aktarması esnasında, Şirket, Kurul Kararı’nda belirtilen güvenlik önlemlerini alacaktır. Bu kapsamda Şirket, özel nitelikli kişisel verileri;

* e-posta ile aktardığı durumlarda, şifreli olarak kurumsal e-posta adresi veya Kayıtlı Elektronik Posta (KEP) hesabı kullanmaktadır,
* farklı fiziksel ortamlardaki sunucular arasında aktardığı durumlarda, sunucular arasında VPN kurarak ya da sFTP yöntemiyle verileri aktarmaktadır,
* kağıt üzerinden aktardığı durumlarda, belgenin çalınması, kaybolması ya da yetkisi kişisel tarafından erişilmesi gibi risklere karşı gerekli önlemleri almakta ve belgeyi “gizlilik dereceli belgeler” formatında göndermektedir.

1. **Özel Nitelikli Kişisel Verilerin Muhafazası**

Şirket, yukarıda detaylıca bahsi geçen genel ilke ve işleme şartlarına uygun bir şekilde özel nitelikli kişisel verileri muhafaza etmektedir. Özel nitelikli kişisel verilerin muhafaza edildiği ve/veya erişildiği ortamlara ilişkin, Şirket, Kurul Kararı’nda belirtilen güvenlik önlemlerini alacaktır. Bu kapsamda Şirket,

* Özel nitelikli kişisel verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip etmekte, gerekli güvenlik testlerinin düzenli olarak yaptırmakta ve test sonuçlarını kayıt altına almaktadır,
* Özel nitelikli kişisel verilere bir yazılım aracılığı ile erişildiği hallerde bu yazılıma ait kullanıcı yetkilendirmeleri yapılmaktadır,
* Özel nitelikli kişisel verilerinin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise, elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı önlemleri almaktadır. Bu ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışları engellenmektedir.

**2. Şirket Tarafından İşlenen Özel Nitelikli Kişisel Veriler**

Şirket bünyesinde işlenen özel nitelikli kişisel veriler aşağıdaki gibidir.

|  |  |
| --- | --- |
| **Veri Kategorisi** | **Özel Nitelikli Kişisel Veri** |
| - Sağlık | (Kan Grubu, Akciğer Grafisi, Sağlık Raporları, Engellilik Durumu, Hastalık Bilgileri, Tıbbi Anamnez Bilgileri, Fiziki Muayene Sonuçları, Laboratuvar Bulguları, İşe Göre Çalışabilir / Uygun Raporu, Ateş Ölçümü, Teşhis-Tedavi Bilgileri, İşitme Raporu, İş Kazası Bilgileri, Soygeçmiş Bilgileri vs.) |

Bu veriler Kişisel Veri İşleme Envanteri içerisinde de belirtilmiş olup veri konusu kişi grubu Şirket Çalışanıdır.

**3. Özel Nitelikli Kişisel Verilerin İşlenme Amaçları**

Şirket tarafından işlenen özel nitelikli kişisel verilerin işleme amaçları ve hukuki sebepleri aşağıdaki gibidir.

|  |  |  |
| --- | --- | --- |
| **Veri Kategorisi** | **İşleme Amacı** | **Hukuki Sebep** |
| - Sağlık | 1. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi, 2. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi 3. İş Faaliyetlerinin Yürütülmesi / Denetimi, 4. Hukuk İşlerinin Takibi Ve Yürütülmesi 5. Faaliyetlerin Mevzuata Uygun Yürütülmesi, 6. İnsan Kaynakları Süreçlerinin Planlanması | 1. Kanun madde 6/3(b): Kanunlarda açıkça öngörülmesi, 2. Kanun madde 6/3(f): İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması, Kanun madde 6/3(b): Kanunlarda açıkça öngörülmesi, 3. Kanun madde 6/3(a) İlgili kişinin açık rızasının olması, 4. Kanun madde 6/3(d): Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması, 5. Kanun madde 6/3(b): Kanunlarda açıkça öngörülmesi, Kanun madde 6/3(f): İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması, |

**4. Özel Nitelikli Kişisel Verilerin Aktarılması**

Şirket, işbu Politikanın "Özel Nitelikli Kişisel Verilerin İşlenme Amaçları' bölümünde belirtilen amaçlar çerçevesinde ve KVKK'nin 8 ve 9'uncu maddelerine uygun olacak şekilde Yetkili Kamu Kurum ve Kuruluşları (Bakanlıklar, Adli Makamlar vs.), Sağlık Kuruluşları ve hizmet alınan kurum ve kuruluşlara ( Hukuk bürosu vs.) her türlü idari ve teknik tedbirler alınarak paylaşılmaktadır. Bu hususlar aynı zamanda Şirket’in kişisel Veri İşleme Envanteri’nde detaylı olarak belirtilmiştir.

- Özel nitelikli kişisel verilerin e-posta yoluyla aktarılması gerekiyorsa, şifreli olarak kurumsal e-posta adresi ile veya kayıtlı elektronik posta (KEP) hesabı kullanılarak aktarılır.

- Farklı fiziksel ortamlardaki sunucular arasında, aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemi ile veri aktarımının gerçekleştirilir.

- Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa, evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın gizlilik dereceli belgeler formatında gönderilir.

**5. Özel Nitelikli Kişisel Verilerin Saklanması ve İmhası**

Çalışanlar, özel nitelikli kişisel verileri uygun ve sadece yetkili kişilerin erişebileceği ortamlarda saklar. Özel nitelikli kişisel verilerin işlenme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez.

Şirket, özel nitelikli kişisel verilerin işleme şartları ortadan kalktığı durumlarda söz konusu özel nitelikli kişisel verileri İşbu Politika ve Kişisel Verilerin Saklanması ve İmhası Politikası’na uygun bir şekilde ortadan kaldırmakla yükümlüdür.

Şirket aşağıda örnek olarak listelenen ve Yönetmelik içinde de belirtilen ilgili durumlarda özel nitelikli kişisel veri işlenme şartlarının ortadan kalktığını kabul eder:

a) Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,

b) Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,

c) Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması.

Bu kapsamda Şirket tarafından Kişisel Veri Saklama ve İmha Politikası içerisinde tanımlı olan tedbirler, uygulama esas usulleri ve bu çerçevede alınacak olan aksiyonlar geçerlidir.

**6. Özel Nitelikli Kişisel Verilerin Güvenliği**

Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. Kişisel Verileri Koruma Kurulu'nun 07.03.2018 tarihli Resmi Gazete' de yayımlanan, 31.01.2018 tarihli Kararı uyarınca aşağıdaki şekilde belirlenmiştir.

Şirket tarafından;

*• Söz konusu çalışanlar ile Veri Sorumlusu arasında gizlilik sözleşmeleri yapılır,*

*• Verilere erişim yetkisine sahip kullanıcıların yetki kapsamları ve süreleri net olarak tanımlanır.*

*• Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılır, bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanter ya da veri içeren materyaller iade alınır.*

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;

*• Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının denetim izleri tutulur ve söz konusu denetim izlerinin güvenliği sağlanır,*

*• Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli olarak takip edilir, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması ve tespitlere ilişkin aksiyon planlarının oluşturulması sağlanır,*

*• Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait uygun kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak gerçekleştirilmesi/yaptırılması, test sonuçlarının kayıt altına alınması ve tespitlere ilişkin aksiyon planlarının oluşturulması sağlanır,*

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise

*• Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunur,*

*• Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışlar engellenir.*

**F. POLİTİKA YÜRÜRLÜK VE GÜNCELLEMELER**

İşbu Politika Şirket Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girecektir. Politika da yapılacak değişiklikler ve bu değişikliklerin yürürlüğe konulması konusunda gereken çalışmalar Hukuk, Denetim ve KVKK Çalışma Grubu tarafından yapılacak ve değişiklikler Şirket Yönetim Kurulu onayından sonra yürürlüğe girecektir. Ancak mevzuat değişiklikleri, atıf yapılan bir teknik standarttaki değişme, Kişisel Verileri Koruma Kurulu'nun işlemleri ve/veya vereceği kararlar ile mahkeme kararları doğrultusunda Şirket bu Politikayı gözden geçirme ve gerekli durumlarda Politikayı güncelleme, değiştirme veya ortadan kaldırıp yeni bir Politika oluşturma hakkını saklı tutar. Şirket, Politika üzerinde yaptığı değişiklikler incelenebilecek olacak şekilde güncellenen Politika' yı e-posta yolu ile çalışanlarıyla paylaşacak ve kurumsal intranet üzerinden çalışanlarının erişimine sunacaktır. Politika, olağan olarak yılda bir defa gözden geçirilerek güncellenir. Politikanın yürürlükten kaldırılmasına ilişkin olarak karar verme yetkisi Şirket Yönetim Kurulu'na aittir.

**G. POLİTİKA’NIN YÜRÜRLÜK TARİHİ**

İşbu Politika 10/10/2024 tarihinde yürürlüğe girmiştir. Protokolde yapılacak değişiklik ve revizeler yazılı olarak yapılır ve revizyon tarihi, değişikliklerle birlikte işbu Politika’ da belirtilir.

**YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**SPECIAL CATEGORIES OF PERSONAL DATA STORAGE AND DESTRUCTION POLICY**

**SENSITIVE PERSONAL DATA MANAGEMENT POLICY**

1. **SCOPE**
2. This Sensitive Personal Data Management Policy ("Policy") applies to all departments, employees, and third parties involved in any process that handles personal data within YARN DAY TEKSTİL SANAYİ VE TİCARET ANONİM ŞİRKETİ ("Company").
3. This Policy encompasses all activities related to ensuring the security of sensitive personal data, outlining the rules for safeguarding such data, and will be implemented at every step to maintain this security.
4. This Policy does not apply to data that is not classified as sensitive personal data.
5. In the event of new legislation or updates to relevant legislation, the Company will revise its policy accordingly to comply with the legal requirements.
6. If it is determined that legal obstacles hinder the application of this Policy by the Company, the Company reserves the right to revise or redefine the Policy as necessary.
7. **DEFINITIONS**

Law: Refers to Law No. 6698 on the Protection of Personal Data.

Regulation: Refers to the Regulation on the Deletion, Destruction, or Anonymization of Personal Data.

Relevant Decision: Refers to the Personal Data Protection Board's decision No. 2018/10, dated 31.01.2018, regarding "Adequate Measures to Be Taken by Data Controllers in Processing Special Categories of Personal Data."

Board: Refers to the Personal Data Protection Board.

Record Environment: Refers to any environment where personal data is processed either wholly or partially by automatic means, or by non-automatic means as part of a data recording system.

Personal Data: Any information related to an identified or identifiable natural person, and it includes any physical, economic, cultural, social, or psychological identifiers, or any data that links an individual to a specific record such as a name or tax number.

Personal Data Processing Inventory: An inventory created and detailed by data controllers concerning their personal data processing activities, including the purposes for processing, data categories, recipient groups, and the groups of individuals whose data is processed.

Sensitive Personal Data: Special categories of personal data defined by law, the processing of which carries the risk of discrimination against the data subject.

Registry: Refers to the Registry of Data Controllers (VERBİS), maintained by the Authority.

Data Recording System: A system where personal data is processed in a structured manner according to specific criteria.

Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system.

Recipient Group: Refers to the category of natural or legal persons to whom personal data is transferred by the data controller.

Relevant User: Refers to individuals who process personal data within the data controller's organization or upon the authorization and instruction of the data controller, excluding those responsible for the technical storage, protection, and backup of data.

The definitions within the Company’s Personal Data Protection and Processing Policy and Personal Data Retention and Disposal Policy are also applicable to this Policy.

1. **PURPOSE AND SCOPE**

This Policy sets forth the principles that must be adhered to by the Company and any third parties contractually responsible for the Company, within the scope of the conditions for processing "Sensitive Personal Data" as specified in Article 6 of the Law.

Pursuant to the Personal Data Protection Board's Decision dated 31.01.2018, published in the Official Gazette on 07.03.2018, the Company, as a Data Controller subject to registry requirements, is obliged to store sensitive personal data in accordance with the personal data processing inventory. Furthermore, the Company is responsible for defining the rules regarding the security of such data, implementing management practices to protect it, and adhering to the policy accordingly.

The following principles shall apply to the storage and disposal of personal data:

a) The general principles outlined in Article 4 of the Law shall be followed.

b) The Company acknowledges that the mere existence of this Policy does not imply that personal data has been deleted, destroyed, or anonymized in accordance with the Law, the Regulation, and relevant legislation.

c) The Company commits to complying with the security measures outlined in Article 12 of the Law, as well as the provisions in the relevant legislation, the decisions of the Personal Data Protection Board, the Administrative and Technical Measures outlined in the Data Security Guide, and this Policy, when storing, deleting, destroying, or anonymizing personal data.

d) The Company undertakes to comply with the tools, programs, and processes specified in this Policy when deleting, destroying, or anonymizing personal data, whether processed by automated or non-automated means as part of a data recording system.

1. **RECORD ENVIRONMENTS**

The Company agrees to include in the scope of this Policy the following environments, as well as any other environments that may emerge, where personal data is stored:

a) Computers / servers used on behalf of the Company

b) Network devices

c) Shared / non-shared disk drives used for data storage on the network

d) Mobile phones and all storage areas within them

e) Paper

f) Peripheral devices such as printers and fingerprint readers

g) Optical disks h) Flash drives

1. **PROCESSING OF SENSITIVE PERSONAL DATA**
2. **General Principles for Processing Sensitive Personal Data**

a) General Principles for Processing Sensitive Personal Data  
The Company is obligated to comply with the general principles outlined in the Personal Data Protection Law (KVK Law) when processing personal data. Accordingly, the Company shall act in accordance with the following principles while processing sensitive personal data:

* Processing personal data in compliance with the law and the principle of good faith
* Ensuring that personal data is accurate and, where necessary, kept up to date
* Processing personal data for specific, clear, and legitimate purposes
* Ensuring that personal data is processed in a way that is relevant, limited, and proportionate to the purposes for which it is processed
* Retaining personal data for as long as stipulated by relevant legislation or as necessary for the purposes for which it is processed.

b) Conditions for Processing Sensitive Personal Data

The Company is obligated to process sensitive personal data in accordance with the general principles mentioned above and the conditions set forth in Article 6 of the KVK Law. Accordingly, the Company may process sensitive personal data based on one of the following conditions:

a) The explicit consent of the data subject,  
b) Where explicitly stipulated by law,  
c) Where it is necessary to protect the life or physical integrity of a person who is incapable of giving consent due to physical impossibility, or whose consent is not legally valid,  
d) Where the data subject has made the data public, in line with their intention to do so,  
e) Where the processing of data is necessary for the establishment, exercise, or protection of a right,  
f) Where it is necessary for public health, preventive medicine, medical diagnosis, treatment, and care services, or the planning, management, and financing of healthcare services, by persons or authorized institutions who are bound by an obligation of confidentiality,  
g) Where processing is necessary for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance,  
h) Where sensitive personal data is processed by non-profit organizations or entities for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the law and restricted to their members, former members, or individuals who have regular contact with such organizations, and that it is not disclosed to third parties.

c) Transfer of Sensitive Personal Data

The Company may share sensitive personal data with third parties in accordance with the conditions for data processing outlined in Articles 8 and 9 of the KVK Law. When transferring sensitive personal data to third parties, the Company shall take the necessary security measures specified in the Board’s Decision. Accordingly, the Company:

* Uses encrypted corporate email addresses or a Registered Electronic Mail (KEP) account when transferring data via email,
* Establishes a VPN or uses the sFTP method when transferring data between servers located in different physical environments,
* Takes precautions to prevent the theft, loss, or unauthorized access to physical documents and ensures the document is sent in a "classified document" format when transferring data on paper.

d) Retention of Sensitive Personal Data

The Company retains sensitive personal data in accordance with the general principles and processing conditions mentioned above. In terms of the environments where sensitive personal data is stored and/or accessed, the Company shall implement the security measures specified in the Board’s Decision. Accordingly, the Company:

* Continuously monitors security updates related to the environments where sensitive personal data is stored, regularly conducts the necessary security tests, and logs the results of these tests,
* Performs user authorization for software that accesses sensitive personal data,
* Ensures the physical security of environments where sensitive personal data is processed, stored, and/or accessed to prevent incidents such as electric leakage, fire, flooding, or theft. Physical security measures are implemented to prevent unauthorized access.

1. **Sensitive Personal Data Processed by the Company**

The sensitive personal data processed by the Company is as follows:

|  |  |
| --- | --- |
| **Data Category** | **Special Category of Personal Data** |
| - Health | (Blood Type, Lung Radiography, Health Reports, Disability Status, Medical History Information, Medical Examination Results, Laboratory Findings, Fit-for-Job/Workability Report, Temperature Measurement, Diagnosis and Treatment Information, Hearing Report, Occupational Accident Information, Family Medical History, etc.) |

These data are also specified in the Personal Data Processing Inventory, and the data subject group is Company Employees.

1. **Purposes of Processing Special Category Personal Data**

The purposes and legal grounds for processing special category personal data by the Company are as follows:

|  |  |  |
| --- | --- | --- |
| **Data Category** | **Purpose of Business** | **Legal Ground** |
| - Health | 1. Fulfillment of Employment Contract and Statutory Obligations for Employees, 2. Execution of Occupational Health and Safety Activities, 3. Conducting and Auditing Business Operations, 4. Legal Process Follow-up and Management, 5. Ensuring Compliance with Legal Requirements in Business Activities, 6. Planning Human Resources Processes | 1. **Law Article 6/3(b)**: Explicitly stipulated by the law, 2. **Law Article 6/3(f)**: Necessity for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance; **Law Article 6/3(b)**: Explicitly stipulated by the law, 3. **Law Article 6/3(a)**: Obtaining the explicit consent of the data subject, 4. **Law Article 6/3(d)**: Necessity for the establishment, exercise, or protection of a right, 5. **Law Article 6/3(b)**: Explicitly stipulated by the law; **Law Article 6/3(f)**: Necessity for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance. |

1. **Transfer of Special Category Personal Data**

The Company, within the scope of the purposes specified in the "Purposes of Processing Special Category Personal Data" section of this Policy and in compliance with Articles 8 and 9 of the Personal Data Protection Law (KVKK), shares special category personal data with Authorized Public Institutions and Organizations (e.g., Ministries, Judicial Authorities), Health Institutions, and institutions and organizations from which services are received (e.g., law firms) by taking all necessary administrative and technical measures. These matters are also detailed in the Company's Personal Data Processing Inventory.

* If it is necessary to transfer special category personal data via e-mail, the transfer is carried out either through the corporate e-mail address in an encrypted format or by using a registered electronic mail (KEP) account.
* If the transfer is conducted between servers located in different physical environments, the transfer is carried out by establishing a VPN connection between the servers or by using the SFTP method.
* If it is necessary to transfer the data in a paper environment, appropriate measures are taken to prevent the document from being stolen, lost, or seen by unauthorized persons, and the document is sent in a format for classified documents.

1. **Storage and Disposal of Special Category Personal Data**

Employees store special category personal data in appropriate environments accessible only to authorized personnel. If the conditions for processing special category personal data no longer exist, data processing cannot continue.

In cases where the conditions for processing special category personal data no longer exist, the Company is obliged to eliminate these special category personal data in accordance with this Policy and the Personal Data Retention and Disposal Policy.

The Company acknowledges that the conditions for processing special category personal data are no longer valid in the following situations, which are listed as examples and specified in the Regulation:

a) The purpose that requires the processing of personal data no longer exists, b) Processing of personal data is against the law or the principle of good faith, c) In cases where data processing is based solely on explicit consent, the withdrawal of the consent by the data subject.

Within this scope, the measures defined in the Company's Personal Data Retention and Disposal Policy, the implementation procedures, and the actions to be taken in this framework will apply.

1. **Security of Special Category Personal Data**

When processing special category personal data, it is also mandatory to take adequate measures as determined by the Board. According to the decision of the Personal Data Protection Board dated 31.01.2018 and published in the Official Gazette on 07.03.2018, the following measures are determined:

By the Company:

* Confidentiality agreements are made between the relevant employees and the Data Controller,
* The scope and duration of the authorities of users with access to data are clearly defined,
* The authorities of employees who have had a change of position or who have left the job are immediately revoked, and in this context, any inventory or data-containing materials provided to them by the Data Controller are retrieved.

If the environments in which special category personal data are processed, stored, and/or accessed are electronic environments:

* All activities performed on the data are logged with audit trails, and the security of these audit trails is ensured,
* Security updates related to the environments where the data is stored are constantly monitored, regular security tests are carried out/commissioned, test results are recorded, and action plans are created based on the findings,
* If access to data is provided through a software, appropriate user authorizations are carried out for this software, regular security tests of this software are carried out/commissioned, test results are recorded, and action plans are created based on the findings.

If the environments in which special category personal data are processed, stored, and/or accessed are physical environments:

* Adequate security measures (e.g., against electrical leakage, fire, flood, theft, etc.) are taken based on the nature of the environment in which special category personal data is stored,
* Physical security of these environments is ensured to prevent unauthorized access.

1. **POLICY ENFORCEMENT AND UPDATES**

This Policy will come into effect on the date it is approved by the Company's Board of Directors. The necessary updates and enforcement of changes to the Policy will be carried out by the Legal, Audit, and KVKK Working Group, and the changes will come into effect after the approval of the Company's Board of Directors. However, in accordance with regulatory changes, amendments to referenced technical standards, decisions of the Personal Data Protection Board, and/or court decisions, the Company reserves the right to review, update, amend, or abolish this Policy and create a new Policy if necessary. The Company will share the updated Policy via e-mail so that employees can review the changes made to the Policy, and it will be accessible to employees through the corporate intranet. The Policy will be reviewed and updated on an annual basis. The authority to repeal the Policy lies with the Company's Board of Directors.

**G. EFFECTIVE DATE OF THE POLICY**

This Policy is effective as of 10/10/2024. Changes and revisions to the protocol are made in writing and the revision date, along with the changes, are specified in this Policy.