**ÖZEL NİTELİKLİ KİŞİSEL VERİ GÜVENLİĞİ POLİTİKASI**

## **TANIMLAR VE KISALTMALAR**

**Kurum :** VERVO MAKİNA OTOMASYON SİSTEMLERİ SANAYİ VE TİCARET LİMİTED ŞİRKETİ

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

**Politika:** Özel Nitelikli Kişisel Veri Güvenliği Politikası.

**Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.

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

**İlgili Kişi:** Kişisel verisi işlenen gerçek kişi.

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

**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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

**Kişisel Veri İşleme Envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.

## **AMAÇ VE KAPSAM**

Özel Nitelikli Kişisel Veri Güvenliği Politikasının (“Politika”) amacı, Kişisel Verileri Koruma Kurulunun *31/01/2018 tarihli ve 2018/10 sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler* kararından doğan hukuki yükümlülüklerin yerine getirilmesi ile özel nitelikli kişisel verilerin işlenmesinde alınan teknik ve idari tedbirlerin ortaya konulmasıdır.

Politikanın kapsamında özel nitelikli kişisel veri güvenliğine yönelik olarak Kurum tarafından alınan teknik ve idari tedbirler yer almaktadır.

## **SORUMLULUK ve GÖREV DAĞILIMLARI**

Kurumun tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile özel nitelikli kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, hukuka aykırı olarak erişilmesinin önlenmesi ve hukuka uygun saklanmasının sağlanması amacıyla özel nitelikli kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Özel nitelikli kişisel verilerin güvenliğinin sağlanmasında görev alanların ünvanları, birimleri ve görev tanımlarına ait dağılım aşağıdaki gibidir.

|  |  |
| --- | --- |
| **Unvan** | **Görev** |
| Yönetim Kurulu | Politikayı onaylayarak yürürlüğe girmesini sağlar. Üst Yönetimin ve çalışanların Politikaya uygun hareket etmesinden sorumludur. Politikanın uygulanması için gerekli bütçeyi oluşturarak destek ve kaynak sağlar. |
| Üst Yönetim | Politikanın işletilmesi ve yürütülmesi kapsamında yapılan çalışmaların takibinden sorumludur. Politikanın yürütülmesi için gerekli kararları alma ve uygulama faaliyetlerini yürütür. |
| KVKK Sorumlusu | Politikanın oluşturulmasından ve onaylanması sonrasında ilgili ortamlarda yayınlanmasından sorumludur. Politikanın uygulanmasında Üst Yönetimin karar verdiği ve kaynak sunduğu teknik çözümlerin uygulanması faaliyetlerini yürütür. |
| Muhasebe ve FinansKiralama Hizmetleri | Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur. |

##

## **TEKNİK ve İDARİ TEDBİRLER**

Kanunun 6 ncı maddesinin 4 numaralı fıkrasında, “*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*” hükmü yer almaktadır. Bu çerçevede, özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel Verileri Koruma Kurulunun *31/01/2018 tarihli ve 2018/10 sayılı kararı* ile belirlenmiştir.

Kurum, özel nitelikli kişisel verilerin Kanuna ve ilgili mevzuata uygun olarak işlenmesi ile özel nitelikli kişisel verilerin güvenliğinin sağlanması için her türlü teknik ve idari tedbiri alır. Bu kapsamda alınan tedbirler aşağıda sıralanmıştır:

## **Teknik Tedbirler**

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

* Veriler kriptografik yöntemler kullanılarak muhafaza edilir,
* Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulur,
* Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanır,
* Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilir, gerekli güvenlik testleri düzenli olarak yapılır veya yaptırılır, test sonuçları kayıt altına alınır,
* Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmeleri yapılır, bu yazılımların güvenlik testleri düzenli olarak yapılır veya yaptırılır, test sonuçları kayıt altına alınır,
* Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi 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 önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınır,
* Bu ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenir.

Özel nitelikli kişisel veriler aktarılacaksa;

* Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılır,
* Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenir ve kriptografik anahtar farklı ortamda tutulur,
* Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilir,
* Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınır ve evrak “gizlilik dereceli belgeler” formatında gönderilir.

## **İdari Tedbirler**

Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

* Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilir,
* Gizlilik sözleşmeleri yapılır,
* Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamları ve süreleri net olarak tanımlanır,
* Periyodik olarak yetki kontrolleri gerçekleştirilir,
* Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılır. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanter iade alınır.

Kişisel veri işleme envanterinde özel nitelikli kişisel veri işlenen faaliyetler etiketlenir.

Özel nitelikli kişisel veri güvenliğine yönelik risk analizleri gerçekleştirilir.

## **POLİTİKANIN GÖZDEN GEÇİRİLMESİ**

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

## **POLİTİKANIN UYGULAMA SORUMLULUĞU**

Politika, Yönetim Kurulu tarafından onaylanlandığında yürürlüğe girmiş kabul edilir. Politika çalışanlara duyurulur.