



# KVKK ile uyumlu musunuz?

*Kişisel Verilerin Korunması Kanunu'na hazır olun*

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması ve bu verileri işleyen kişilerin yükümlülüklerinin düzenlenmesi amaçlanmaktadır. Yürürlüğe giriş tarihi olan 07.10.2016'dan itibaren bu kanun, kişisel veri işleyen tüm kuruluşlar için pek çok sorumluluğu da beraberinde getirmektedir.

## KVKK ile neler değişecek?

€ Birçok ağır yaptırım; **5.000 ila 1.000.000 TL arasında değişen** idari para ve hapis cezaları.



Kişisel veri işleyen **tüm kuruluşlar** herhangi bir ayırım gözetilmeksizin bu düzenlemeden etkileniyor.



Veri güvenliğini temin etmek adına **gerekli teknik ve idari tedbirlerin alınması** gerekliliği.



Veriler, kullanım amaçları doğrultusunda **kişilerin açık rızası olmadan işlenemiyor.**



Sistemik olarak veri işleyen kuruluşlar için **"Veri Sorumlusu"** belirleme zorunluluğu.



İşletmeler, veri kullanımıyla ilgili bilgi talep edilmesi durumunda **en geç 15 gün içerisinde** KVK Kurumu'na bilgi vermek zorunda.

## İşletmenizin ne gibi kişisel verileri koruması gerekiyor?

- Çalışanların kişisel bilgileri (kimlik bilgileri, adres, doğum tarihi, vb.).
- Müşterilerin/hastaların/konaklayanların kişisel bilgileri (pazarlama veritabanları sağlık kayıtları, iletişim listeleri).
- İş ortaklarının ve hizmet sağlayıcıların kamuya açık olmayan kişisel verileri.
- Üçüncü şahıslara aktarılıp işlenen kişisel bilgiler (muhasabe kayıtları, kredi sicilleri, doğrudan pazarlama).

# KVKK uyumluluęu için verilerinizi nasıl güvende tutabilirsiniz?

## 1/Veri denetimi

Şirketinizin sahip olduęu tüm verilerin nasıl kullanıldığını bilmek zorundasınız. Hassas içerięe sahip verilerin nereye taşındığını, bu verileri kimlerin, ne amaçla kullandığını görüntülemeniz gereklidir.

## 3/Çalışanların eğitimi

Her çalışan hangi verinin ne şekilde kullanılması gerektiğini bilmelidir. Çalışanları güvenlik politikanız hakkında bilgilendirerek veri kullanım sınırlarını belirleyebilirsiniz.

## 5/Veri sızıntısı önleme (DLP)

Veri sızıntısı önleme, mutlaka etkin bir şekilde uygulanmalı ve tüm iletişim kanallarını kapsamalıdır. E-posta, yazıcılar, USB, DVD gibi çıkarılabilir cihazlar ve diğer iletişim kanalları denetlenerek yalnızca belirli verilerin şirket dışına çıkabilmesi sağlanmalıdır.

## 2/Veri kullanım kuralları

Kişisel verilerle kimlerin, ne şekilde çalışabileceęi konusunda kesin kurallar oluşturmalısınız. Bu kurallar kağıt üzerinde kalmamalı, etkin bir şekilde uygulanmalıdır.

## 4/Şifreleme

Kişisel bilgiler içeren tüm veriler şifrelenmelidir. Şifreleme kullanımını uç noktalar da dahil olmak üzere tüm şirketinize yaymalısınız.

## Safetica – KVKK ile uyumlu kişisel veri koruması

Safetica ile katı yasal yükümlülöklere kolayca uyum sağlayabilirsiniz. Şirketinizde neler olup bittięi hakkında doğru bir fikre sahip olabilir, çalışanların kişisel verileri ne şekilde kullandıklarını görebilir, kişisel verilerin yanlış kullanımını önleyebilir ve herhangi bir güvenlik tehdidi oluşması durumunda gerçek zamanlı bildirimler yoluyla bilgi sahibi olabilirsiniz.



## Dięer ESET çözümleri



ENDPOINT  
ENCRYPTION



SECURE  
AUTHENTICATION



ENTERPRISE  
INSPECTOR



THREAT  
INTELLIGENCE

*ESET'in kapsamlı uç nokta, DLP, şifreleme ve kimlik doğrulama çözümleriyle birlikte, gelişmiş güvenlik servislerini de kullanarak BT altyapınızı KVKK ile uyumlu hale getirebilirsiniz.*

