



GDPR ile uyumlu musunuz?

Genel veri koruma yönetmeliğine hazır olun

GDPR (Genel Veri Koruma Yönetmeliği), 25 Mayıs 2018 tarihinde yürürlüğe girecek olan Avrupa Birliği merkezli veri koruma düzenlemesidir. AB vatandaşlarının kişisel verilerini işleyen tüm kuruluşları kapsamaktadır. Bu, AB ülkeleri dışında faaliyet gösteren şirketlerin de etkileneceği anlamına gelmektedir. GDPR, şu ana dek hazırlanmış en katı ve kapsamlı veri koruma düzenlemesidir.

GDPR kapsamındaki en kritik değişiklikler neler?



Yıllık cironun %4'ü kadar, 20 milyon Euro'ya varan yüksek para cezaları.



AB ülkelerine ürün veya hizmet sunan farklı ülkelerdeki kuruluşlar da düzenleme kapsamında.



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



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



Sistematically olarak veri işleyen kuruluşlar için "**Veri Koruma Yetkilisi**" belirleme zorunluluğu.



İşletmeler, veri kullanımıyla ilgili bilgi talep edilmesi durumunda **en geç 72 saat içerisinde** 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).

GDPR 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 dięer iletişim kanalları denetlenerek yalnızca belirli verilerin şirket dışına çıkabilmesi sağlanmalıdır.

2/Veri kullanım kuralları

Kişisel verilerle kimlerin, ne şekilde çalışabileceęi konusunda kesin kurallar oluşturmalsınız. 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 – GDPR 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 tehditi 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.

