Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin işlenmesini ve korunmasını düzenleyen AB'nin veri gizliliği ve güvenliğiyle ilgili temel bir düzenlemesidir. GDPR, 25 Mayıs 2018'de yürürlüğe girmiş ve AB ülkelerinde ve AB dışındaki bazı durumlarda geçerli olan bir düzenlemedir. Tüzük, Mauritius, Şili, Japonya, Brezilya, Güney Kore, Güney Afrika, Arjantin ve Kenya da dahil olmak üzere dünya çapında birçok kanuna model olmuştur. 2021 itibarıyla Birleşik Krallık, artık bir AB üye devleti olmamasına rağmen yasayı aynı biçimde korumaktadır.

1. **Kurumsal Firmalarda Ne Tür Faaliyetler Yapılmaktadır:**
   * Kişisel verilerin toplanması ve işlenmesi (müşteri bilgileri, çalışan bilgileri, tedarikçi bilgileri, vb.).
   * Verilerin güvenli bir şekilde saklanması ve erişiminin kontrol edilmesi.
   * Kişisel verilerin paylaşılması veya aktarılması durumlarında gerekli izinlerin alınması.
   * Veri ihlallerinin izlenmesi ve bildirilmesi.
2. **Ne Tür Önlemler Alınmaktadır:**
   * Kişisel verilerin güvenliğini sağlamak için teknik ve organizasyonel önlemler alınır.
   * Veri koruma politikaları ve prosedürleri oluşturulur.
   * Veri koruma eğitimi verilir.
   * Veri ihlali durumlarında hızlı bir tepki verme mekanizmaları oluşturulur.
3. **Firma Çalışanları ile Yapılan İş Sözleşmesine Nasıl Maddeler Eklenmelidir:**
   * İş sözleşmelerine GDPR ile uyumlu bir dil eklemek önemlidir.
   * Veri güvenliği ve gizliliğine saygı göstermeyi taahhüt eden maddeler eklenmelidir.
   * Çalışanların kişisel verilere erişimini ve kullanımını sınırlayan maddeler eklenmelidir.
   * Veri ihlali durumunda nasıl bir bildirim süreci izleneceği hakkında bilgi içeren maddeler eklenmelidir.
4. **Firmanın Diğer Tedarikçi Firmaları ile Yapılan Sözleşmelere Nasıl Maddeler Eklenmelidir:**
   * Tedarikçi firmalarla veri işleme anlaşmaları (Data Processing Agreements - DPA) yapılmalıdır.
   * DPA'lar, tedarikçinin kişisel verileri güvenli bir şekilde işlemesini ve GDPR'ye uygun olmasını sağlamalıdır.
   * Veri paylaşımının kapsamı, amaçları ve süreçleri net bir şekilde tanımlanmalıdır.
   * Tedarikçi firmaların veri ihlali durumunda nasıl bildirim yapmaları gerektiğini içeren maddeler eklenmelidir.

GDPR uyumluluğu, işletmelerin kişisel verileri koruma yükümlülüklerini yerine getirmelerini sağlar ve müşterilerin, çalışanların ve tedarikçilerin veri gizliliğine saygı gösterilmesini sağlar. Bu nedenle işletmeler, GDPR'yi anlamalı ve gerektiğinde profesyonel danışmanlık alarak uygun önlemleri almalıdır.

GDPR – KVKK

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) kişisel verilerin işlenmesini ve korunmasını düzenleyen iki farklı yasa ve düzenlemedir. GDPR ile KVKK arasındaki ana farklar:

1. **Uygulama Alanı:**
   * GDPR: Avrupa Birliği (AB) üyesi ülkelerde ve AB dışındaki bazı durumlarda kişisel verilerin işlenmesini düzenler.
   * KVKK: Türkiye'de kişisel verilerin işlenmesini ve korunmasını düzenler.
2. **Veri İhlali Bildirimleri:**
   * GDPR, veri ihlali durumlarında yetkililere 72 saat içinde bildirim yapma zorunluluğunu getirir.
   * KVKK'da da veri ihlali bildirimi gereklidir, ancak bildirim süreleri GDPR'e göre daha farklı olabilir.
3. **Veri İşlemeye İzin Alma (Consent):**
   * GDPR, veri sahiplerinin (kişilerin) rızasını almayı ve rıza geri çekme hakkını vurgular.
   * KVKK da rıza önemlidir, ancak GDPR kadar ayrıntılı ve güçlü bir rıza düzenlemesi içermez.
4. **Kişisel Veri Sahiplerinin Hakları:**
   * GDPR, veri sahiplerine geniş haklar tanır, bu haklar arasında bilgiye erişim, düzeltme, silme, veri taşınabilirliği ve itiraz hakkı gibi haklar bulunur.
   * KVKK da benzer hakları tanır ancak bazı farklılıklar olabilir.
5. **Veri İşleyen ve Veri Sorumlusu Kavramları:**
   * GDPR, veri işleyen (data processor) ve veri sorumlusu (data controller) kavramlarını tanımlar ve bunların sorumluluklarını açıkça belirtir.
   * KVKK da bu kavramları tanır ve benzer sorumlulukları düzenler, ancak bazı farklılıklar vardır.
6. **Para Cezaları:**
   * GDPR, ciddi ihlaller için yüksek para cezalarını öngörür (şirketlerin yıllık gelirlerinin yüzde 4'üne kadar veya 20 milyon euro, hangisi daha yüksekse).
   * KVKK da para cezaları öngörür, ancak miktarlar GDPR ile karşılaştırıldığında genellikle daha düşüktür.

GDPR ve KVKK, kişisel verilerin korunması konusundaki temel prensipleri benimser ve işletmelerin bu prensiplere uyum sağlamasını gerektirir. Her iki düzenleme de veri gizliliği ve güvenliği konularında ciddiye alınmalıdır, ve işletmeler bu düzenlemelere uyum sağlamak için gerekli önlemleri almalı ve gerektiğinde profesyonel danışmanlık almalıdır.