

Kişisel Verileri Koruma Kurulu'nun Sağlık Sektöründe Faaliyet Gösteren Şirket Tarafından Yapılan Veri İhlali Bildirimine İlişkin Kararı

10 Şubat 2021

Kişisel Verileri Koruma Kurulu ("**Kurul**") veri ihlali sonrasında, gerekli tüm teknik ve idari tedbirleri alan veri sorumlusu hakkında yaptırılan karar almamış ilk kararını yayımladı.

Karara konu veri ihlali 30 Eylül 2020 ve 5 Ekim 2020 tarihleri arasında yaşanan bir veri sorumlusu tarafından dünya genelinde yaygın olan ve veri sorumlusu tarafından da kullanılan bir uygulamada bulunan açığa çıkarılan veriler olarak, veri sorumlusu nezdinde söz konusu uygulamanın bulunduğu tek sunucuya zararlı bir yazılımın yüklendiğinin tespit edilmiştir.

Kurul'un yaptırılan inceleme sonucunda,

1. İhlal ile ilgili olan çalışanlara gerekli eğitimlerin verildiği, veri sorumlusunun verdiği eğitimlerin, katılımlarını durumunu tevsik edici belgelerin ve log kayıtlarının veri ihlali bildirim formunun ekinde Kurul'a sunulduğunu,

2. İhlalden önce aşağıdakiler dahil olmak üzere gerekli teknik tedbirlerin alındığını;

- Ağ güvenliği ve uygulama güvenliği,
- Kişisel verilerin yedeklenmesi ve yedeklenen kişisel verilerin güvenliğinin de sağlanması,
- Her yıl sızma testi uygulanması,
- Veri kaybı önleme yazılımlarının kullanılması,
- Saldırı tespit ve önleme sistemlerinin kullanılması,
- İhlalden önce gerekli idari tedbirlerin alındığını,

3. İhlalden sonra aşağıdakiler dahil teknik tedbirlerin alındığını,

- Zararlı yazılımın bulunduğu sunucunun host edildiği lokasyonun diğer bağlantılara kapatılması,
- Adli bilişim yazılımları ile sistemin denetlenmesi,
- Kullanılan yedekleme sisteminin kontrollü bir lokasyona taşınması,
- İlk tespitlerde rastlanmamış olmasına karşın tekrardan hizmet temin edilen uzman firmadan alınan IOC bilgileri ve olaylara müdahale ekibi tarafından sağlanan kurallar aracılığıyla, sistemlerin ele geçirilmediğinin teyidinde devam edilmesi,
- Ele geçirilen belirlenen uç noktalardan gerekli iz ve kayıtların toplanması,

4. İhlalden sonra gerekli idari tedbirlerin alındığını

tespit etmiştir.

Bu kapsamda Kurul,

- İhlalin veri sorumlusunun tedbir eksikliğinden kaynaklanmayıp yaygın kullanılan bir uygulamadan kaynaklandığı; bu duruma veri sorumlusunun müdahale edemeyeceği,
 - İhlalden etkilenen kişisel verilerin şahs şirketi kaynaklarından ve kamuya açık kaynaklardan rahatlıkla elde edilebileceği,
 - Veri sorumlusunun ihlalden etkilenen kişilere üç iş günü içerisinde bildirim gerçekleştireceğini belirtmesi,
 - İhlalin ilgili kişiler açısından olumsuz sonuçlar doğurma riskinin düşük olması,
 - Veri sorumlusunun makul teknik ve idari tedbirleri almış olması
 - Veri sorumlusunun ihlali kısa zamanda fark etmiş olduğu,

hususları dikkate alarak veri ihlali bildirimi ile ilgili yapılacak başka bir işlem olmadığının karar vermiştir.

22 Ocak 2021 tarihinde Kurul'un resmi internet sitesinde yayımlanan 2020/787sayılı özet karara bu [bağlantı](#)dan ulaşabilirsiniz.

İLGİLİ ÇALIŞMA ALANLARI

- [Gizlilik ve Kişisel Verilerin Korunması](#)

Related Attorneys

- [BURCU TUZCU ERSİN, LL.M.](#)
- [CEYLAN NECİPOĞLU, PH.D, LL.M.](#)