BİR TURİZM ŞİRKETİ HAKKINDA KİŞİSEL VERİLERİ KORUMA KURULU'NUN 27 AĞUSTOS 2019 TARİH VE 2019/255 SAYILI KARAR ÖZETİ HAKKINDA BİLGİ NOTU

Bir turizm şirketi tarafından Kişisel Verileri Koruma Kurumu ("Kurum")'na iletilen bildirimin incelenmesi neticesinde Kişisel Verileri Koruma Kurulu ("Kurul")'nun 27 Ağustos 2019 tarih ve 2019/255 sayılı kararı ile;

- Şirket yetkilileri ve bilgi işlem uzmanlarının incelemeleri neticesinde Şirketin Local Area Network (LAN-Yerel Alan Ağı) üzerinden, ilgili şifrelerin ele geçirilmesi yoluyla yetkisiz şifre girişi ile siber saldırı yapıldığı ve söz konusu olayın Şirketin genel alanlarda bulunan bir çalışan bilgisayarı üzerinden çalışan ağına sızılarak gerçekleştirilmesi şeklinde olduğu,

- Etkilenen kişisel verilerin; personel verileri (Ad, soyad, TC kimlik numarası, doğum tarihi, medeni durum vb.) ile müşteri verileri (Ülke/eyalet, uyruk, doğum tarihi (DB-Veri tabanı seviyesinde şifreli), e-posta adresi, cinsiyet vb.) olduğu,

- Genel alanlarda bulunan bir çalışan bilgisayarına Şirket çalışanı olmayan yetkisiz 3. kişilerce erişilebilmesinin idari bir tedbirsizlik olduğu,

- Genel alanlarda bulunan, sunuculara erişimi olan çalışan network bağlantılarının ihlal gerçekleştikten sonra kapatıldığı ve bu hususun da sunucu güvenliği noktasında bir aksaklık teşkil ettiği,

- Güvenlik duvarının ihlal gerçekleştikten sonra yenilenmesinin sağlandığı ve güvenlik duvarının güncel durumda bulunmamasının teknik bir eksiklik olduğu,

- Çalışanların ihlal gerçekleştikten sonra güvenlik eğitiminin sağlandığı ve daha önce böyle bir eğitim almadıkları anlaşılmış olup bu durumun da kişisel veri güvenliği sağlanması ve farkındalığı noktasında idari bir eksikliğin göstergesi olduğu,

- Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının Şirket IT sistemleri tarafından fark edilmemesinin teknik bir eksiklik olduğu, sunucu üzerindeki verilerin geri getirilemez şekilde ihlali gerçekleştiren kişi tarafından yok edildiği,

- Söz konusu olayın Bilgi İşlem Birimine Şirketin diğer birimlerinde çalışanlar tarafından bildirilmesinin Şirketin Bilgi İşlem Biriminin ve Bilgi Sistemlerinin düzgün olarak çalışmadığı ve işlemediğinin bir göstergesi olduğu

dikkate alınmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun")'nun 12. maddesinin (1) numaralı fıkrasında yer alan *"..veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır."* hükmü ile, (3) numaralı fıkrasında yer alan "*Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır."* hükmü çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanun'un 18. maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **400.000 TL idari para cezası uygulanmasına,**

Şirket tarafından tespit edilen ihlale ilişkin ilgili kişilere bildirim yapılmadığı ve Kurum'a yapılan bildirimin Kanun'un 12. maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanun'un 18. maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **100.000 TL idari para cezası uygulanmasına**

karar verilmiştir.

Legal Hukuk Bürosu