

Kişisel Verileri Koruma Kurulu, Facebook Nezdinde Gerçekleşen Veri İhlali Sebebiyle İdari Para Cezasına Hükmetti

22 Eki 2019

Kişisel Verileri Koruma Kurulu ("**Kurul**"), veri ihlallerini önlemek için gerekli teknik ve idari tedbirleri almadığı ve ihlali tespit etmesine rağmen bildirmediği gerekçeleriyle Facebook hakkında toplamda 1.600.000 TL idari para cezasına uygulanmasına karar verdi.

Facebook, sisteminin birbirinden farklı üç özelliğinin etkileşimi sonucunda oluşan ve veri ihlaline sebep olan hatayı 25 Eylül 2018 tarihinde tespit etmiş, 14 Ekim 2018'de Facebook yetkilileri Kurul'u e-posta ile durumdan haberdar etmişti. Ancak Facebook, meydana gelen veri ihlaline ilişkin olarak Kurul'a 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda ("**Kanun**") öngörülen usule uygun herhangi bir bildirim yapmamıştı. Bunun üzerine Kurul, Kanun'un 15. maddesinin 1. fıkrasında tanıyan yetkiye dayanarak Facebook hakkında re'sen inceleme başlattı.

Kurul incelemesi neticesinde özetle;

- 14-28 Eylül 2018 tarihleri arasında Facebook sisteminin "Başkasının Gözünden Gör", "Doğum Günü Kutlayıcısı" ve "Video Yükleyicisi" adlı üç özelliğinin etkileşiminden kaynaklı zafiyetten faydalanarak erişim jetonları'nın elde edildiği ve saldırganların erişim jetonları aracılığıyla kullanıcıların kişisel verilerine eriştikleri ve bu ihlalden Facebook'u Türkçe kullanan 280.959 kullanıcı'nın etkilendiği tespit edilmiştir.
- Bu tip hataların test aşamasında tespit edilerek özellikler kullanıma açılmadan önce düzeltilmesi gerektiği dikkate alınarak Facebook'un gerekli idari ve teknik tedbirleri almakta kusurlu olduğuna karar verilmiştir.
- Ek olarak, ilgili zafiyetin 21 Temmuz 2017 ve 27 Eylül 2018 tarihleri arasında yaklaşık 14 ay boyunca devam etmesinin gerekli denetim ve kontrollerin yapılmadığı'nın göstergesi olduğu, ihlalin tespiti sonrasında da gerekli müdahalelerin zamanında yapılmaması sebebiyle Facebook'un yeterli idari ve teknik tedbirleri almadığına karar verilmiştir.
- İhlalden etkilenen ve Facebook'u Türkçe olarak kullanan 280.959 kullanıcı'nın temel profil bilgileri, konum bilgileri, din bilgileri, geçmişi aramaları ve takip ettiği başlıca hesaplar dahil birçok kişisel verisine hukuka aykırı şekilde erişim sağlandığı tespit edilmiştir.
- Ek olarak, ihlalden etkilenen bazı kullanıcıların ait din bilgisi başta olmak üzere özel nitelikli kişisel verilere yetkisiz erişim sağlanması sebebiyle Facebook'un Kurul'un "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili 31 Ocak 2018 tarihli ve 2018/10 sayılı kararının (3) numaralı maddesine aykırı davrandığı tespit edilmiştir.
- Ayrıca, ihlal sonucu erişilen kişisel veriler kullanılarak veri sahipleri hakkında profillemeye yapılabileceği ve bu faaliyetlerin veri sahipleri aleyhine sonuçlar oluşturabileceğine karar verilmiştir.

Tüm bu değerlendirmelerin sonucu olarak Kurul;

- Facebook'un Kanun'un 12. maddesinin 1. fıkrası çerçevesinde gerekli teknik ve idari tedbirleri almadığı gerekçesiyle 1.150.000 TL idari para cezasına ve
- 25 Eylül 2018 tarihinde tespit edilen veri ihlalinin Facebook tarafından Kanun'un 12. maddesinin 5. fıkrası uyarınca en kısa sürede bildirilmediği gerekçesiyle 450.000 TL idari para cezasına

uygulanmasına, Kanun'un 18. maddesinin 1. fıkrasının (b) bendi uyarınca karar vermiştir.

3 Ekim 2019 tarihinde Kurul'un resmi internet sitesinde yayımlanan özet karara bu [linkten](#) ulaşabilirsiniz.

LG ÇALI MA ALANLARI

- Gizlilik ve Kiisel Verilerin Korunmas

Related Attorneys

- BURCU TUZCU ERS N, LL.M.
- BURCU GÜRAY