KİŞİSEL VERİLERİ KORUMA KURULU'NUN FACEBOOK'A KARŞI HÜKMETTİĞİ 1.600.000 TL İDARİ PARA CEZASI HAKKINDA BİLGİ NOTU

Facebook temsilcisi tarafından 14 Ekim 2018 tarihinde, Facebook'un birbirinden farklı üç özelliği olan "başkasının gözünden gör", "doğum günü kutlayıcı" ve "video yükleyicinin" etkileşimi sonucunda oluşan bir hatadan kaynaklanan veri ihlali hususunda Kişisel Verileri Koruma Kurumu ("Kurum")'na e-posta göndermek suretiyle bilgi verilmiştir.

Söz konusu e-postada;

- Facebook Inc. nezdinde 14-28 Eylül 2018 tarihleri arasında access token (erişim jetonları) kullanılmak suretiyle Facebook platformları üzerinden çeşitli Facebook hesabı bilgilerinin ele geçirildiği,
- Saldırganların 25 Eylül 2018 tarihinde Facebook platformları üzerinden çeşitli bilgilerin elde edilebilmesi için dijital bir anahtar niteliğindeki bu jetonları sistemleri üzerindeki üç hata arasındaki kompleks etkileşimden doğan bir zafiyetten faydalanmak suretiyle elde ederek ve 14-28 Eylül 2018 tarihleri arasında erişim jetonları kullanılarak Facebook platformları üzerinden çeşitli Facebook hesabı bilgilerinin ele geçirildiği,
- İlgili zafiyetin 21 Temmuz 2017 tarihinde meydana geldiğinin tespit edildiği, ancak erişim jetonlarına yetkisiz olarak erişilmesine sebep olan bu saldırının 14 Eylül 2018 tarihinde başladığı kanaatini taşıdıkları, zira 25 Eylül 2018 tarihinde gerçekleştirilen incelemeler kapsamında beklentinin üzerinde bir "Başkasının Gözünden Gör" trafiği artışının bu tarihte başladığının tespit edildiği, ancak 28 Eylül 2018 tarihinde kod üzerindeki zafiyetin düzeltilerek saldırının durdurulduğu, bununla birlikte ihlal hakkındaki incelemelerin devam ettiği,

ifadelerine yer verilmiştir.

Durumun **"veri gizliliğine/mahremiyetine"** aykırı bir husus olması sebebiyle bir veri ihlali niteliği taşıdığı ve söz konusu ihlalin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun")'nun 12. maddesinin (5) numaralı fıkrasında yer alan "*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede durumun ilgilisine ve Kurula bildirir…*" hükmü uyarınca Facebook tarafından Kişisel Verileri Koruma Kurulu ("Kurul")'na bildirilmesi gerektiği, Facebook temsilcisi tarafından gönderilen e-postada bilgilendirmenin, e-postanın gönderim tarihini takip eden hafta içinde yazılı olarak Kurul'a arz edileceğinin ifade edilmesine rağmen herhangi bir bildirimin yapılmadığı tespit edilmiştir. Bunun üzerine, Kanun'un 15. maddesinin (1) numaralı fıkrasında yer alan "*Kurul, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.*" hükmü kapsamında resen inceleme yapma kararı alınmıştır.

Yapılan inceleme neticesinde;

Veri ihlalinin, 21 Temmuz 2017 tarihinden 27 Eylül 2018 tarihine kadar yaklaşık 14 ay boyunca, Facebook sisteminin birbirinden farklı üç özelliğinin etkileşimi sonucunda karşı tarafın profil bilgilerini elde etmek üzere kullanılabilen bir erişim jetonu üretilmesi sonucunu doğuran bir hatadan kaynaklandığı ve bu tip hataların test aşamasında tespit edilerek değişiklik yayına alınmadan evvel düzeltilmesi gerektiği dikkate alınarak Şirketin bahse konu veri ihlali kapsamında Kanun'un 12 inci maddesinin (1) numaralı fıkrasında belirtilen teknik ve idari tedbirleri almakta kusurlu olduğu,

İlgili zafiyetin 21 Temmuz 2017 tarihinden 27 Eylül 2018 tarihine kadar yaklaşık 14 ay boyunca devam etmesi gerekli denetim ve kontrollerin yapılmadığının göstergesi olduğu, bu durumun ise Kanun'un 12 inci maddesinin (1) ve (3) numaralı fıkralarında belirtilen tedbirlerin alınması hususunda Facebook'un kusurlu olduğunu gösterdiği,

İlgili zafiyetten kaynaklı olarak ihlalin 13 gün boyunca gerçekleştiği Şirket tarafından belirtilmiş olup, güvenlik açığına yönelik yama geliştirildiği ancak Facebook tarafından ihlalin tespit edilmesine rağmen 2 gün boyunca ihlalin devam ettiği, geçici olarak bir özelliğin bütünüyle devre dışı bırakıldığı ancak bahse konu devre dışı bırakma işleminin tespitten itibaren 3 gün sonra yapılmış olduğu, potansiyel olarak etkilendikleri belirlenen yaklaşık 90 milyon hesaba ait erişim jetonlarının 27 Eylül 2018 tarihinden başlayarak 29 Eylül 2018 tarihine kadar devre dışı bırakıldığı, başlamış olan olağandışı bir aktivite sonrası ihlalin tespit edilmiş olduğu, olağandışı aktivitenin olmadığı tarihleri arasında da veri ihlalinin gerçekleşmiş olabileceği göz önüne alındığında, ihlale zamanında müdahale edilmediği ve bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesi olduğu, bu durumun ise veri sorumlusunun Kanun'un 12 inci maddesinin (1) numaralı fıkrasında belirtilen teknik ve idari tedbirleri almakta kusurlu olduğunu gösterdiği,

İhlalinden etkilenen 280.959 kullanıcıdan; 133.510 kullanıcının isim, telefon numarası veya eposta gibi temel profil bilgilerine, 143.974 kullanıcının temel profil bilgilerine ek olarak, doğum günü, cinsiyet, ilişki durumu, din bilgisi, memleket, eğitim ve iş geçmişi, kullanıcı tarafından Facebook'a erişmek için kullanılan cihazlar –alanlar işletim sistemi ve donanım bilgileri, kimlik doğrulama, Facebook'ta son zamanlarda yapılan aramalar, kullanıcının takip ettiği 500'e kadar başlıca hesaplar gibi bilgilerine ulaşılırken 3.475 kullanıcının da ilk iki grubun erişilen veri türlerine ilave olarak profil sayfalarındaki verilerinin de riske maruz kaldığı göz önünde bulundurulduğunda, Facebook kullanıcılarına ait kişisel verileri ile özel nitelikli kişisel verilerine bu zafiyeti kullanan kişiler tarafından erişilebildiği, bu durumun "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarihli ve 2018/10 sayılı Kararının (3) numaralı maddesine ve Kanun'un 12 inci maddesinin (1) numaralı fıkrasına aykırılık teşkil ettiği,

İhlalden etkilenen kişilere ait çok sayıda kişisel verilerin elde edildiği dikkate alındığında, bu verilere yetkisiz bir şekilde erişenler tarafından ilgili kişiler hakkında profilleme yapılabileceği ve bu faaliyetlerin bu kişilerin aleyhine bir sonuç oluşturabileceği,

Veri ihlali hakkında Facebook tarafından Kurum'a bildirim yapılmadığı, tespit edilmiş olup,

Bu kapsamda yukarıda gerekçeleriyle ortaya konulan durumun bir veri ihlali olduğu ve Şirketin bahse konu veri ihlalin kapsamında Kanun'un 12. maddesinin (1) numaralı fıkrasında belirtilen teknik ve idari tedbirlerde kusurunun bulunması çerçevesinde gerekli teknik ve idari tedbirleri almadığı anlaşılan Facebook hakkında Kanun'un 18. maddesinin (1) numaralı fıkrasının (b)bendi uyarınca Şirket hakkında **1.150.000 TL**,

Söz konusu veri ihlalinin 25 Eylül 2018 tarihinde tespit edilmesine rağmen Kurum'a bildirimin yapılmadığının ve 14 - 27 Eylül 2018 tarihleri arasında gerçekleşen veri ihlalinin ilgili kişilere 14 Ekim 2018 tarihinde bildirilmeye başlandığının tespit edildiği, bu çerçevede Kanun'un 12. maddesinin (5) numaralı fıkrasında yer alan en kısa sürede bildirim yapılması gerektiği hükmüne aykırı hareket eden Şirket hakkında Kanun'un 18. maddesinin (1) numaralı fıkrasının (b) bendi uyarınca **450.000 TL idari para cezası** uygulanmasına karar verilmiştir.

Legal Hukuk Bürosu