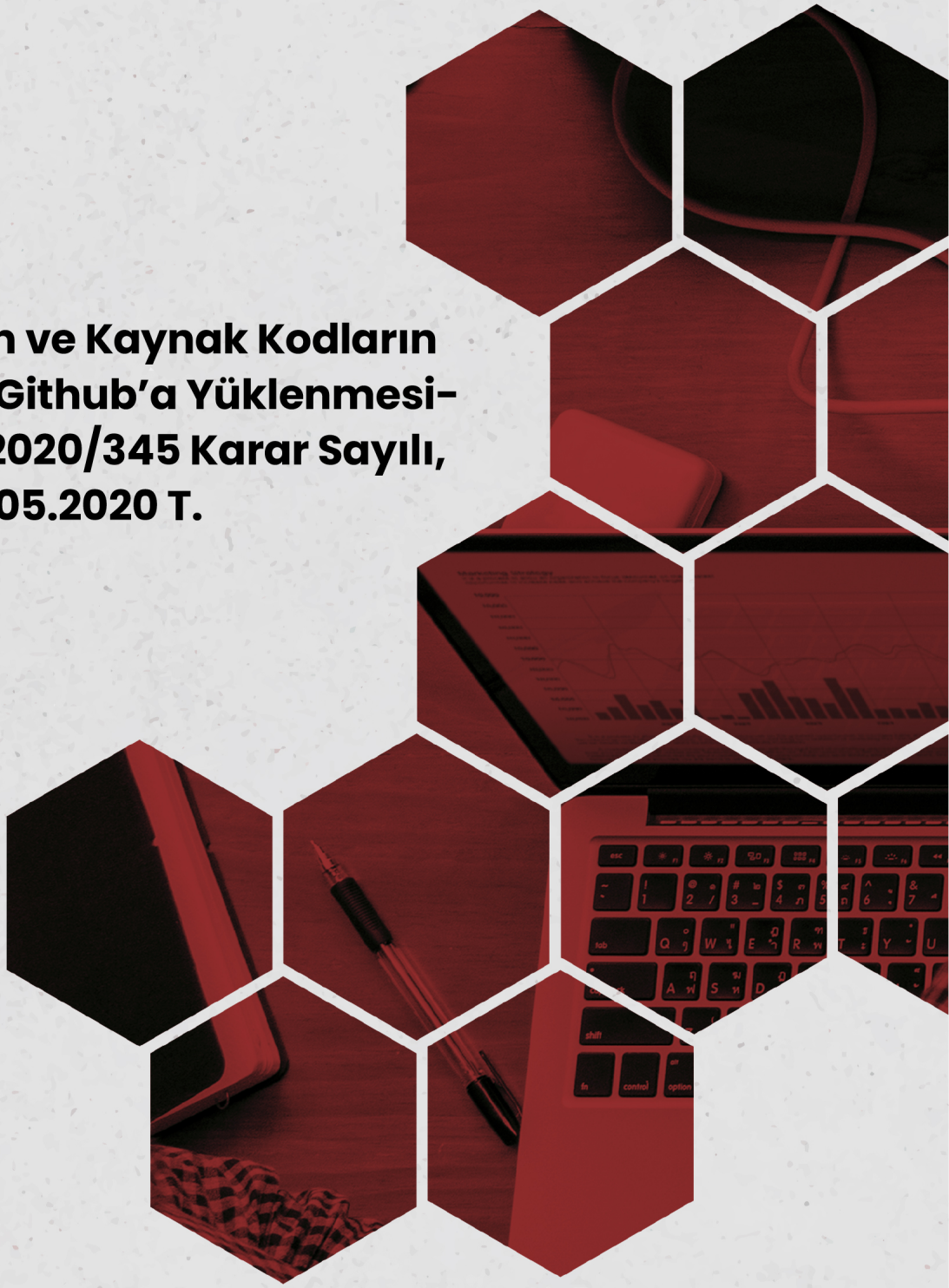
Kişisel Verilerin ve Kaynak Kodların Yetkisiz Olarak Github'a Yüklenmesi- KVKK Kararı - 2020/345 Karar Sayılı, 05.05.2020 T.



aeylegal

A. Ekrem Yılmaz

03

Olay Özeti

04

Çözümü Gereken Hukuki Sorun

05

Mahkemenin Çözümü

07

Görüşümüz

OLAY ÖZETİ

2019 yılında Kuruma intikal eden veri ihlali özetle; 2017 yılında eski veri sorumlusu çalışanı (web geliştiricisi) tarafından içerisinde kaynak kod ve veri dosyalarını içeren klasörün yetkisiz olarak github.com internet sitesine yüklenmesidir. İhlale ilişkin incelemede ilgili klasörde hem sahte (bot) hesaplara hem de Türkiye'de mukim kullanıcılara ait gerçek hesaplara ilişkin verilerin bulunduğu görülmüştür. İhlalden etkilenen kişiler; içlerinde çocukların da bulunduğu kullanıcı, müşteri, potansiyel müşterilere ilişkindir ve ihlalden etkilenen kişi sayısı toplamı 62'dir. İhlale konu kişisel veriler kimlik bilgileri, iletişim bilgileri, lokasyon bilgileri gibi bilgilerdir.

Çözümü Gereken Hukuki Sorun

Çözümü gereken hukuki sorun; eski çalışanın kaynak kod ve veri dosyalarını github.com'a yüklemiş olmasının bir güvenlik açığı olup olmadığı, veri sorumlusunun gerekli tedbirleri alıp almadığı, bu güvenlik açığının veri sorumlusuna yükletilip yükletilemeyeceği ve veri sorumlusunun "en kısa sürede" bildirimde bulunma yükümlülüğünü yerine getirip getirmediğidir.

Mahkemenin Çözümü

Kurum; eski çalışanın kaynak kodları ve veri dosyalarını github.com internet sitesine yüklenmiş olmasının bir güvenlik açığı olduğu, veri sorumlusu tarafından gerekli teknik ve idari tedbirlerin yeterince alınmamış olduğu, çalışanlarına kişisel verilerin güvenliğinin sağlanması bakımından eğitim ve bilgilendirme çalışması yapması gerekliliği hususuna uygun davranmadığı, ihlalin 19.04.2017 tarihinde gerçekleşmesi ancak ihlalin tespit edilmesi tarihinin 09.01.2019 olduğu değerlendirildiğinden veri sorumlusunun güvenlik kontrollerini düzenli yapmadığı, ihlal tespitinden 1 ay 19 gün sonra bildirim yapılması sebebiyle "en kısa sürede" bildirimde bulunma yükümlülüğünün yerine getirilmediği hususlarını dikkate almış ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 12 nci maddesinin (1) numaralı fıkrası kapsamında veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 100.000 TL, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 30.000 TL olmak üzere toplam 130.000 TL idari para cezası uygulanmasına karar vermiştir.

Görüşümüz

Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde de ifade edildiği gibi, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu nedenle çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları, çalışanlara yönelik farkındalık çalışmaları yapılması ve güvenlik risklerinin belirlenebildiği bir ortam oluşturulması kişisel veri güvenliğinin sağlanması bakımından çok önemlidir.
Veri sorumlusu nezdinde çalışan herkesin hangi konumda çalıştığına bakılmaksızın kişisel veri güvenliğine ilişkin rol ve sorumlulukları, görev tanımlarında belirlenmeli ve çalışanların bu konudaki rol ve sorumluluğunun farkında olması sağlanmalıdır. Ayrıca kişisel veri içeren ortamlara erişim hakkı verilirken veya bu konuda kurum kültürü oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibi değil, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesine dikkat edilmelidir.

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir. Bu durumun önüne geçebilmek için hazırlanan rehberde düzenli kontrol ve denetimin yapılması öngörülmüştür. Bu önlemler; bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi, bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi, tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi), güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması, çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması şeklindedir.

Somut olay bakımından veri sorumlusunun kişisel verilerin güvenliği için gerekli tedbir ve önlemleri almadığı açıkça görülmektedir. Gerekli önlem ve tedbirlerin alınması durumunda ihlalden haberdar olunması için bu denli uzun bir süre geçmesinin mümkün olmadığı da ortadadır. Ayrıca veri sorumlusunun, işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurula bildirme yükümlülüğü vardır. "en kısa sürede" şeklinde belirlenen süreden kasıt en geç 72 saat içinde ilgilisine ve kuruma bildirilmesidir. Söz konusu olayda olduğu gibi 1 ay 19 günlük sürenin "en kısa süre" ifadesine sığdırılamayacağı da açıktır. Dolayısıyla Kurul kararı ve görüşüne katılmaktayız.

Teşekkürler

Abdullah Erkam Yılmaz
Kurucu Avukat

İletişim:
aeylegal.com
erkam@aeylegal.com

Buse Hamurcu
Avukat

İletişim:
aeylegal.com
buse@aeylegal.com

Gizem Bayram
Stajyer

İletişim:
aeylegal.com
gizem@aeylegal.com

Sorularınız ve görüşleriniz için bizimle iletişime geçebilirsiniz.