CRONOC YAZILIM

E-BÜLTEN (2 TEMMUZ- 9 TEMMUZ)

KVKK VE İYS'YE DAİR GELİŞMELER VE GÜNCEL DUYURULAR

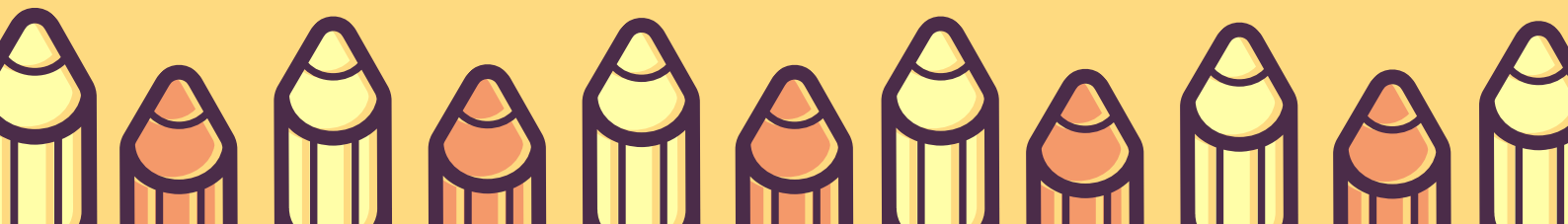
İÇİNDEKİLER

Bir bilişim şirketinin veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- Veri sorumlusu Şirketin sistemlerine siber saldırı gerçekleştirilerek sistemlerinde yer alan verilerin elde edilmeye çalışıldığı,
- Pilot adı verilen uygulamada debugging özelliğinin açık olduğu ve şirket için sistem geliştirmesi yapan geliştiricilerin bu özelliği kullanarak uygulamadaki hataları tespit ettiği ve iyileştirme gerçekleştirdiği,
- İhlale konu siber saldırı ile Pilot uygulamasına internet üzerinden erişim sağlamaya çalışan kişinin(lerin), uygulamaya daha önce giriş yapmış kişilere ait “PHPSESSID” değerini elde ettiği ve Pilot uygulamasına erişim sağladığı,
- Debugging özelliğinin açık olmasının sebebinin sisteme internet üzerinden erişilerek geliştirmelerin yapılmasına olanak sağlamak olduğu, ancak bu durumun internet üzerinden siber saldırılar gerçekleştirilerek sisteme erişilmesine olanak tanıdığı,
- Sistemde saldırganlar tarafından erişilen verilerin neler olduğunun net bir şekilde tespit edilemediği ancak veri sorumlusunun sistemlerinde yer alan verilerin tümü dikkate alındığında sistemde 65.993 kişinin yer aldığı, bu kişilerin sadece teklif almış, üyelik oluşturmuş, herhangi bir şekilde hizmet almış, aktif olan ve olmayan kişileri içerdiği,
- İlgili kişilere ilişkin sistemde yer alan kayıtların 1259 sözleşme, 701 alan adı başvuru dosyası (içerisinde imza sirküleri, vergi levhası ve kişi kimlik fotokopisi kayıtları) olduğu,
- Sistemde ayrıca elli bin kredi kartı bilgisi yer aldığı, ancak bu kredi kartı bilgilerinin büyük çoğunluğunun son kullanma tarihinin geçmiş olduğu ve kullanılamayacağı, sadece sekiz bin kartın aktif olduğunun tespit edildiği,
- İhlalden etkilenen kişi kategorilerinin müşteriler ve potansiyel müşteriler olduğu,
- Saldırganların hangi verilere eriştiklerinin tespit edilemediği, sistemde yer alan verilerin kimlik, iletişim, işlem güvenliği (kullanıcı adı ve parola bilgileri), ödeme Bilgileri (kredi kartı numarası) olduğu,
- Ele geçirilen kredi kartı bilgilerinin 2018 tarihi öncesinde veri sorumlusu Şirkete aktarılan bilgiler olduğu, 2016 tarihi itibari ile ödeme hizmetlerinde iyileştirme çalışmaları kapsamında bir proje başlatıldığı, 2018 yılı itibariyle kredi kartı bilgilerinin yetkilendirilmiş ödeme hizmet sağlayıcıları üzerinden toplanmakta ve onlar tarafından saklanmakta olduğu,
- Veri ihlalinden doğrudan etkilenen özel nitelikli bir veri bulunmadığı, ancak tüzel kişi müşterilerin imza sirkülerinin ekinde yer alan eski kimlik fotokopilerinde kan grubu ve din bilgisi hanelerinin bulunduğu ve bazı imza sirkülerinde kimlik fotokopisinin arka yüzünün de yer alabildiği dikkate alınarak; bazı müşteriler için saldırganların bu verilere de erişme ihtimali olabileceği,
- Sistemde yer alan tüm kayıtların incelendiği ve sayımlarda (imza sirkülerlerinde yer alan kimlik fotokopileri de dahil) 1.784 adet eski kimlik fotokopisinin arkalı önlü yüzünün bulunduğunun tespit edildiği,
- İhlalden etkilenen tüm müşterilere e-posta göndermek suretiyle bildirimde bulunulduğu, bir kısım müşterilere mümkün olduğunca telefonla da bilgilendirme gerçekleştirildiği ifadelerine yer verilmiştir.

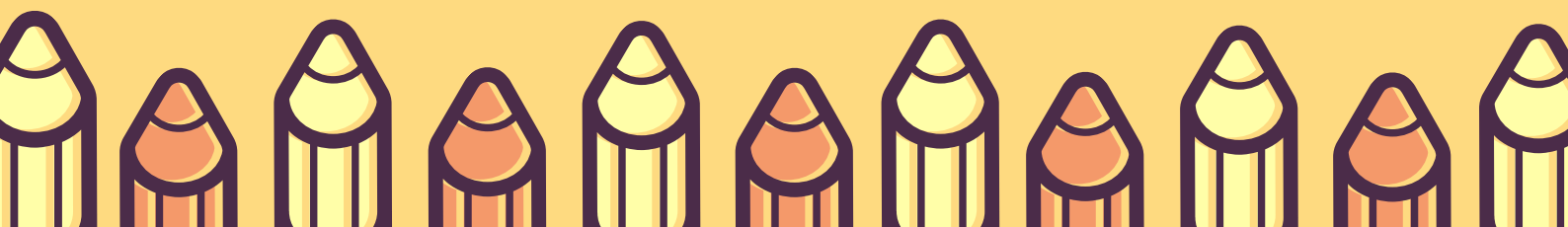
https://kvkk.gov.tr/Icerik/6992/2020-216



Bir otoyol işletmesinin veri ihlal bildirimi hakkında

Veri sorumlusunun Kurumumuza intikal eden veri ihlal bildiriminde;

- İhlalin; çalışanların kendi rıza ve talepleri ile yazılı ve imzalı olarak veri sorumlusuna ilettikleri kişisel e-posta adreslerinin sisteme işlenmesinden sonra bordro programı üzerinden bu hesaplara gönderilen bordrolarda, gönderilen kişilerin kendisine ait olmayan ancak aynı şirket çalışanı olan başka çalışanlara ait bordroyu ve dolayısıyla başkasına ait ad, soyad, TC Kimlik No ve sicil numarası görüntülemesi şeklinde gerçekleştiği, maaş bilgisinin ise herkeste aynı jenerik bilgisinin görüntülendiği,
- İhlalin sistemsel bir hata sebebiyle hatalı e-posta gönderimi neticesinde meydana geldiği ve bu teknik hatanın da bordro sisteminde Türkçe dili için bir cihaz türü tanımlı olmaması nedeni ile programın bordro zarflarını anlık göndermek yerine öncelikle kuyruğa gönderip oradaki kayıtları sonrasında e-posta atmak yöntemini kullanması nedeniyle yaşandığı,
- İhlalden etkilenen kişi ve kayıt sayısının 489 olduğu, ifadelerine yer verilmiştir.
- 31.05.2019 tarihli ve 2019/157 sayılı Kurul Kararında de belirtildiği üzere, kurumsal e-posta hizmetinin sunucularının yurt dışında olan veri sorumlularından/veri işleyenlerden temin edilmesi durumunda saklama hizmetlerinin de 6698 sayılı Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesi gerektiği, veri sorumlusu tarafından Kurumsal e-posta hizmeti alınmadan çalışanların şahsi e-posta hesaplarının çalıştıkları işlerle ilgili e-posta gönderiminde kullanılmasının verilerin farklı ülkelerde saklanması durumunu ortaya çıkarabileceği ve veriler üzerinde kontrol kaybına neden olabileceği
- hususları dikkate alındığında, Kanun'un 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında kabahatin haksızlık içeriği, veri sorumlusunun kusuru ve ekonomik durumu da göz önünde bulundurularak Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 60.000 TL idari para cezası uygulanmasına karar verilmiştir.



Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Cosmolog Kozmetik Sanayi ve Ticaret AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.

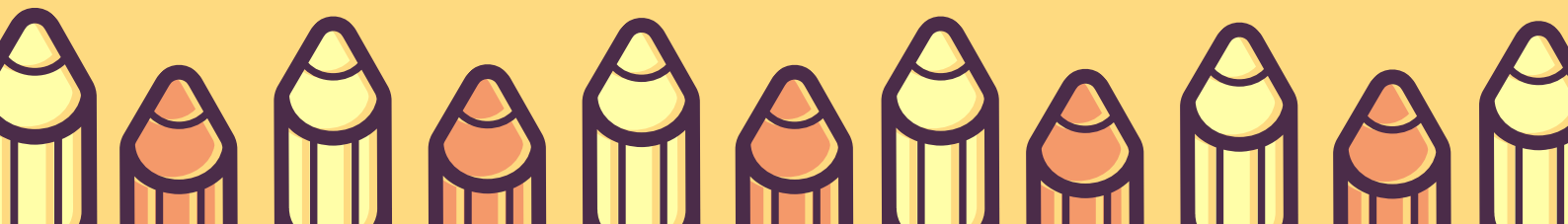
Veri sorumlusu sıfatını haiz olan Cosmolog Kozmetik Sanayi ve Ticaret AŞ tarafından Kurumumuza gönderilen veri ihlali bildiriminde özetle;

- Veri sorumlusu kayıtlarında veri ihlali olduğuna ilişkin iddiaların iki adet internet sitesinde 17-18 Haziran 2021 tarihinde duyurulduğu, 25 Haziran 2021 tarihinde veri sorumlusuna haber verilmesiyle konu hakkında incelemelerin başlatıldığı,
- Yapılan incelemelerde veri sorumlusunun sistemde oluşturduğu raporların, rapor isimlerinin/URL isimlerinin herhangi bir kişi tarafından bilinmesi durumunda söz konusu raporlara erişim yetkisi verilmeyen 3. kişilerce erişilebileceğinin tespit edildiği,
- İhlalin 02.07.2021 tarihinde sona erdiği,
- İhlalinden etkilenen kişi sayısının 36.116 kişi olduğu,
- İhlalden etkilenen ilgili kişi gruplarının müşteriler olduğu,
- İhlalden etkilenen kişisel verilerin kimlik (ad-soyad), iletişim (e-posta ve adres) bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili guvenlik@cosmolog.com.tr e-posta adresinden bilgi alabileceği

ifade edilmiştir.

Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.07.2021 tarih ve 2021/675 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.

Kamuoyuna saygıyla duyurulur.



Kamuoyu Duyurusu (Veri İhlali Bildirimi) – T. Garanti Bankası AŞ

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12 nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir.
Veri sorumlusu sıfatını haiz olan T. Garanti Bankası AŞ tarafından Kuruma gönderilen 2 adet veri ihlali bildiriminde özetle;

- Banka sistemi üzerinden Kredi Kayıt Bürosu (KKB) ekranlarına yönelik yapılan görüntülemelere ilişkin Teftiş Kurulu Başkanlığı tarafından 01.04.2020 - 15.03.2021 dönemi için uzaktan gerçekleştirilen incelemelerde, 2 farklı banka şubesinde görev alan 2 çalışanın gerçekleştirdiği görüntülemelerin dikkat çekici bulunması üzerine incelemelerin genişletildiği,
- Veri sorumlusu tarafından yapılan değerlendirme sonucu çalışanların sorgulamalara istinaden elde etmiş oldukları muhtelif müşterilere ait bilgileri 3. şahıslar ile paylaşmış olabilecekleri konusunda güçlü kanaate varıldığı,
- Bir şube çalışanının, %85’i şube müşterisi olmayan ve % 90’ı farklı müşteri segmentlerinden 3277 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydını görüntülediği, Akyazı şubesinde bir çalışanın ise %90’ının şube müşterisi olmayan ve %70’i farklı bir şehirde ikamet eden müşterilerden 5079 farklı kişiye ait KKB (Kredi Kayıt Bürosu) kaydı görüntülemesi yaptığı,
- İhlalden etkilenen kişisel veri kategorisinin finans bilgileri olduğu,
- İlgili kişilerin veri ihlali ile ilgili www.garantibbva.com.tr, banka şubeleri ile bankanın çağrı merkezinden bilgi alabileceği

ifade edilmiştir. Konuya ilişkin inceleme devam etmekle birlikte, Kişisel Verileri Koruma Kurulunun 06.07.2021 tarih ve 2021/677 sayılı Kararı ile söz konusu veri ihlali bildiriminin Kurumun internet sayfasında ilan edilmesine karar verilmiştir.
Kamuoyuna saygıyla duyurulur.

Kişisel Verilerin İşlenmesinde Genel (Temel) İlkeler Nelerdir?

Kişisel verilerin işlenmesinde her zaman Kanunda ortaya konulan genel ilkelere uygun davranılmalıdır. Kişisel verilerin işlenmesinde genel ilkeler şunlardır: a. Hukuka ve dürüstlük kurallarına uygun olma. b. Doğru ve gerektiğinde güncel olma. c. Belirli, açık ve meşru amaçlar için işlenme. ç. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme. Kişisel verilerin işlenmesine ilişkin ilkeler, tüm kişisel veri işleme faaliyetlerinin özünde bulunmalı ve tüm kişisel veri işleme faaliyetleri bu ilkelere uygun olarak gerçekleştirilmelidir.