GÜZELDERE ◆ BALKAN
HUKUK BÜROSU

Telefon : (212) 244 84 94
Faks : (212) 244 85 95
Adres : İnönü Cad. Dilaram Apt. No: 19/9-11 Taksim 34437 İstanbul
E-Posta : info@guzeldere-law.com
Web : www.guzeldere-law.com

25.01.2021

Sayın İlgili,

İşbu bilgi notu; Kişisel Verileri Koruma Kurumu ("**Kurum**") tarafından yayımlanan Kişisel Verileri Koruma Kurulu'nun (**"Kurul"**) 09.10.2020 tarihli ve 2020/787 sayılı kararı ("**Karar**") ile ilgili olarak sizleri bilgilendirmek amacıyla hazırlanmıştır.

Karar'ın konusu, sağlık sektöründe faaliyet gösteren veri sorumlusu ("**Veri Sorumlusu**") tarafından Kurum'a iletilmiş veri ihlali bildirimine ilişkindir. Veri Sorumlusu tarafından yapılan bildirimde ihlale ilişkin bilgilerin yanı sıra aynı zamanda ihlal öncesi ve sonrası alınmış teknik ve idari tedbirlere de yer verilmiştir. Kurum'a intikal eden ihlal bildiriminde ihlale ilişkin olarak özetle;

- İhlalin 30.09.2020 tarihinde başladığı, 05.10.2020 tarihinde tespit edildiği ve yine aynı tarihte sona erdiği,
- Dünya genelinde yaygın olan ve Veri Sorumlusu tarafından da kullanılan bir uygulamada bulunan açıktan yararlanılarak, Veri Sorumlusu nezdinde söz konusu uygulamanın bulunduğu tek sunucuya zararlı bir yazılımın yüklendiğinin tespit edildiği,
- Veriye erişim/ulaşılabilirlik bakımından ihlalin etkisinin, sunucuda bulunan uygulamanın erişiminin gerektiği "xml" formatındaki bazı dosyalara ulaşılamaması sonucunda fonksiyonlarını yerine getirememesi olduğu,
- İhlalden etkilenen kişisel verilerin kimlik verisi (ad-soyad; ticari unvan, T.C. kimlik numaraları, bağlı olunan vergi dairesi), iletişim verisi (adres, e-posta adresi, telefon numarası), müşteri işlem verisi (e-faturanın düzenlenme tarihi ve belge numarası, malın nevi, miktarı, fiyatı ve tutarı, vergi türü, oranı ve tutarı, satılan malların teslim tarihi ve irsaliye numarası, fatura tipi, fatura kayıt no. ödeme tarihi, ödeme şekli) olduğu,
- İhlalden etkilenen kişi sayısının 200 (1 müşteri ve 199 tedarikçi); kayıt sayısının ise 1187 olduğu,
- Fatura ilişkisi kapsamında hâlihazırda Veri Sorumlusu'nun veri kayıt sisteminde bulunan iletişim bilgileri vasıtasıyla ilgili kişilere bildirimin en geç Kurul'a ihlal bildirimin yapıldığı tarihi takiben 3 (üç) iş günü içinde gerçekleştirileceği

ifadeleri yer almaktadır.

Veri Sorumlusu tarafından ayrıca tevsik edici belgeler ile de desteklenen idari ve teknik tedbirler ise şu şekildedirler:

1) **İhlal ile ilgili olan çalışanların son bir yıl içerisinde aldığı eğitimler hakkında;**

- ISO27001 uyumu ve sertifikası kapsamında bilgi güvenliği eğitimlerinin çalışanlar bakımından zorunlu eğitim statüsünde olduğu ve bu eğitimlerin her yıl güncel içerik ile tekrarlandığı,
- Ayrıca işe yeni giren çalışanlar bakımından da aynı eğitimlerin oryantasyon programları kapsamında verildiği,
- Veri Sorumlusu'nun vermiş olduğu eğitimlerin, sunumların, katılım durumunu tevsik edici belgelerin ve log kayıtlarının münferit ekler olmak üzere veri ihlal bildirim formunun ekinde Kurul'un bilgilerine sunulduğu,

2) **İhlalden önce alınmış bulunan teknik tedbirler hususunda;**

- Ağ güvenliği ve uygulama güvenliği sağlandığı,
- Çalışanlar için yetki matrisi oluşturulduğu,
- Erişim loglarının düzenli olarak tutulduğu,
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin kaldırıldığı,
- Güncel anti-virüs sistemleri kullanıldığı,
- Güvenlik duvarlarının kullanıldığı,
- Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alındığı ve ilgili evrakın gizlilik dereceli belge formatında gönderildiği,
- Kişisel verilerin yedeklendiği ve yedeklenen kişisel verilerin güvenliğinin de sağlandığı,
- Kullanıcı hesap yönetimi ve yetki kontrol sisteminin uygulandığı ve bunların takibinin de yapıldığı,
- Mevcut risk ve tehditlerin belirlendiği,
- Her yıl sızma testi uygulandığı,
- Kullanıcı bilgisayarlarının USB'lerinin kapalı durumda olduğu, sadece özel üretim cihazlarında açık olduğu,
- Veri kaybı önleme yazılımlarının kullanıldığı,
- Saldırı tespit ve önleme sistemlerinin kullanıldığı,

3) İhlalden önce alınmış olan idari tedbirler ile ilgili olarak;

- Çalışanlar için veri güvenliği hükümleri içeren disiplin hükümlerinin mevcut olduğu,
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar ve kişisel veri prosedürleri hazırlandığı ve uygulandığı,
- Gizlilik taahhütnameleri yapıldığı,
- Kişisel veri güvenliğinin takip edildiği ve sorunların hızlı bir şekilde raporlandığı,
- Kişisel verilerin mümkün olduğunca azaltıldığı,
- Kurum içi periyodik ve/veya rastgele denetimler yapıldığı ve yaptırıldığı,

4) İhlalden sonra alınmış teknik tedbirler hakkında;

- Zararlı yazılımın bulunduğu sunucunun host edildiği lokasyonun dış bağlantılara kapatıldığı,
- Adli bilişim yazılımları ile sistemin denetlendiği,
- Şirket dış bağlantıları kesilerek kontrollü olarak aktive edildiği,
- Sunucular üzerinde zararlı yazılımlar için forensic çalışması yapıldığı,
- Siber istihbarat verilerinin analiz edildiği,
- Gerçek zamanlı proses ve dosya hareketleri izlemeleri başlatıldığı,
- Kullanılan yedekleme sisteminin kontrollü bir lokasyona taşındığı,
- Veri Sorumlusu bünyesinde daha önceden gerçekleşen ve kayıtları bulunan zararlı aktivitelerin detaylarının elde edilmesi sürecinin devam ettiği,
- Uç noktalarda (istemci ve sunucu) tehdit ve güvenlik zafiyeti avcılığına yönelik çalışmaların devam ettiği,
- Tehdit avcılığına yönelik kural tanımlarının yapılması işlemlerine devam edildiği,
- Uç nokta tespit ve müdahale aracının kurulması işlemlerinin devam ettiği,
- Uç nokta tespit ve müdahale aracına ait sensörlerin tüm uç noktalara dağıtılması işlemlerinin sürdüğü,
- Uç noktalardan verilerin sorunsuz gelmesi için gerekli konfigürasyonların düzenlemelerinin devam ettiği,

- İlk tespitlerde rastlanmamış olmasına karşın tekrardan hizmet temin edilen uzman firmadan alınan IOC bilgileri ve olaylara müdahale ekibi tarafından sağlanan kurallar aracılığıyla, sistemlerin ele geçirilmediğinin teyidine devam edildiği,
- Ele geçtiği belirlenen uç noktalardan gerekli iz ve kayıtların toplanması sürecinin devam ettiği,
- Zararlı IP ve domainlerin belirlenmesi, sistem üzerindeki kalıcılık mekanizmalarının belirlenmesi, arka kapıların tespit edilmesi ve zararlı proseslerin tespit edilmesi işlemlerinin devam ettiği,

5) İhlalden sonra alınmış idari tedbirler hususunda;

- Veri İhlali Müdahale Planı prosedürünün derhal olay özelinde uygulamaya alındığı,
- Yetkisiz erişim denemelerinin Veri Sorumlusu'nun bilgi teknolojileri birimi tarafından tespit edildiği an üst yönetime ve Şirket Kişisel Verilerin Korunması Komitesi'ne ("**Komite**") raporlandığı,
- Komite ve üst yönetim tarafından derhal veri güvenliği ekibi kurulduğu,
- Siber güvenlik alanında uzman bir firma tarafından yetkilendirilen Siber Olaylara Müdahale Ekibinin, Veri Güvenliği Ekibine dâhil edildiği,
- Veri Sorumluları Sicili kaydına göre revize edilen politika, prosedür ve gizlilik taahhütlerinin güncel versiyonlarının çalışanlara iletildiği,
- Veri Sorumluları Sicili kaydına göre revize edilen politikaların güncel versiyonlarının internet sitesinde yayımlandığı

belirtilmiştir.

Yukarıda yer verilen ihlale ilişkin bilgiler ve Veri Sorumlusu tarafından alınan tedbirler çerçevesinde yapılan değerlendirme sonucunda ;

- **İhlalin Veri Sorumlusu'nun tedbir eksikliğinden kaynaklanmayıp yaygın kullanılan bir uygulamadan kaynaklandığı; bu duruma Veri Sorumlusu'nun müdahale edemeyeceği,**
- **Veri Sorumlusu'nun ihlali kısa zamanda fark etmiş olduğu,**
- **İhlalden etkilenen kişisel verilerin şahıs şirketi kaşelerinden ve kamuya açık kaynaklardan rahatlıkla elde edilebileceği,**
- **Veri Sorumlusu'nun ihlalden etkilenen kişilere üç iş günü içerisinde bildirim gerçekleştireceğini belirttiği,**

- **İhlalin ilgili kişiler açısından olumsuz sonuçlar doğurma riskinin düşük olduğu,**
- **Veri Sorumlusu'nun makul teknik ve idari tedbirleri almış olduğu**

hususları dikkate alınmış ve söz konusu ihlale ilişkin ilgili kişilere bildirim yapıldığını tevsik edici belgelerin Kurum'a gönderilmesi suretiyle karara konu veri ihlali bildirimi ile ilgili olarak **Kanun'un 12. maddesi kapsamında yapılacak ilave bir işlem bulunmadığına karar verilmiştir.**

Saygılarımızla,

Güzeldere | Balkan Hukuk Bürosu