DEMİRCAN İNŞAAT

OLASI İHLAL SENARYOLARI

2020

Bayraktar Mah. Vedat Dalokay Cad. Folklor Sok. No:13 D:4,
06670 Çankaya/Ankara

Örnek Olay	KVKK'na Bildirim?	İlgili Kişilerin Bilgilendirilmesi?	Not ve Düşünceler
i. Veri sorumlusu kişisel veri arşivinin bir kopyasını şifrelenmiş bir anahtar şeklindeki USB bellekte muhafaza altına alır. Şirket binasında yapılan soygunda bahse konu bellek çalınır.	Hayır	Hayır	Veriler son teknoloji bir algoritma ile şifrelendiği, verilerin yedekleri mevcut olduğu sürece özgün anahtar bellek tehlikeye atılmaz ve veriler zamanında geri yüklenebilir olduğu için bu rapor edilebilir bir ihlal olmayabilir. Bununla birlikte, daha sonra bellekteki veri tehlikeye girecek olursa bildirim gereklidir.
ii. Veri sorumlusu çevrim içi ortamda hizmet sunmaktadır. Söz konusu hizmete yapılan siber saldırı sonucunda bireylerin çevrim içi ortamdaki kişisel verileri çalınır. Veri sorumlusunun yalnızca Türkiye'de müşterileri vardır.	EVET. İlgili kişiler açısından ihlal sonuçlar doğuracak ise KVKK'na bildirim yapılmalıdır.	Evet, etkilenen kişisel verilerin niteliğine ve bireyler üzerindeki olası sonuçlarının ciddiyetinin yüksek olup olmadığına bağlı olarak(risk analizi sonucuna göre) kişilere bildirimde bulunulması gerekir.	
iii. Veri sorumlusunun çağrı merkezinde birkaç dakika süren kısa bir elektrik kesintisi sonucu müşteriler veri sorumlusunu arayamaz ve kayıtlarına erişemez.	Hayır	Hayır	Bu, bildirilmesi zorunlu bir ihlal değildir, ancak yine de GDPR Madde 33 (5) uyarınca kaydedilmesi gereken bir olaydır. Veri sorumlusu tarafından olaya ilişkin uygun kayıtlar tutulmalıdır.
iv. Veri sorumlusu, tüm verilerin şifrelenmesine neden olan bir fidye yazılımı saldırısına maruz kalır. Verilerin yedeklemesi yoktur ve veriler geri yüklenemez. İnceleme sırasında, fidye yazılımının tek işlevinin verileri şifrelemek olduğu ve sistemde başka kötü amaçlı yazılım olmadığı ortaya çıkar.	Veri erişimi/ulaşılabilirliği kaybı söz konusu olduğu için İlgili kişiler açısından ihlal sonuçlar doğuracak ise KVKK'na bildirim yapılmalıdır.	Evet, etkilenen kişisel verilerin niteliğine ve verilerin kullanılabilir olmamasının olası etkisine ve diğer olası sonuçlara bağlı olarak kişilere bildirimde bulununuz.	İhlale uğrayan verilerin yedeği mevcutsa ve veriler zamanında geri yüklenebiliyorsa, kalıcı olarak kullanılabilirlik veya gizlilik kaybı olmayacağından, bu durumun denetim makamı olan KVKK'na veya kişilere bildirilmesi gerekmez. Bununla birlikte, KVKK olaydan başka yollarla

v. Bir kişi, bir veri ihlalini bildirmek için bir bankanın çağrı merkezini arar. Zira bahse konu kişiye bir başkası adına düzenlenen aylık ekstre gönderilmiştir.Veri sorumlusu, kısa bir araştırma yürütür (24 saat içinde tamamlanmalıdır) ve bir kişisel veri ihlalinin meydana geldiğini ve diğer kişilerin etkileneceği veya etkilenebileceği anlamına gelebilecek sistemik bir kusur olup olmadığını makul bir güven duyulacak seviyede belirler.	Evet	Yüksek risk varsa ve başkalarının etkilenmediği açıksa, yalnızca etkilenen kişiler bilgilendirilir.	haberdar olursa, 32.Maddenin daha geniş güvenlik gerekliliklerine uygunluğu değerlendirmek için bir soruşturma yapmayı düşünebilir. Yapılan daha ayrıntılı araştırma sonucunda, daha fazla kişinin ihlalde etkilendiği tespit edilirse, KVKK'na ihlale ilişkin bir güncelleme yapılmalıdır ve veri sorumlusu, kendileri için yüksek risk söz konusuysa, diğer etkilenen kişilere de bildirimde bulunmak için ek bir adımları atar.
vi. Veri sorumlusu, çevrimiçi satış yapabildiği bir platform işletmektedir ve birden çok ülkede müşterileri vardır. Kullandığı platform bir siber saldırıya uğrar ve kullanıcı adları, şifreler ve satın alma geçmişi saldırgan tarafından çevrimiçi olarak yayınlanır.	Evet, ihlal sınır ötesi işlemleri de içeriyorsa ilgili ülke denetim makamına bildirim yapılmalıdır.	EVET, yüksek risk söz konusu olduğu için gecikmeden bildirimde bulunulmalıdır.	Etkilenen hesapların parolalarının sıfırlamasını ve ilgili kişiler için doğacak risklerin azaltılması için veri sorumlusunun derhal harekete geçmesi gerekir. Ayrıca 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği başkaca bildirimler yapılması gerekebilir.
vii. Veri işleyen olarak hareket eden bir web sitesi barındırma şirketi, kullanıcı yetkilendirmesini kontrol eden kodda bir hata tanımlar. Hata sonucu olarak, herhangi bir kullanıcı diğer kullanıcıların hesap ayrıntılarına erişebilecektir.	Veri işleyen sıfatıyla hareket eden, web sitesi barındırma şirketi, etkilenen müşterilerini (veri sorumluları) gereksiz gecikmeye yer vermeksizin bilgilendirmelidir. Web sitesi barındırma şirketinin kendi araştırmasını yürüttüğünü varsayarsak, ihlalden etkilenen veri	İlgili kişiler açısından yüksek bir risk söz konusu değilse bilgilendirilmelerine gerek yoktur.	Veri işleyen sıfatıyla hareket eden, web sitesi barındırma şirketi, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gereği yapması gerekecek bildirimleri göz önünde

	sorumlularının, bir ihlale uğrayıp uğramadığına makul bir kesinlikte bileceği ve veri işleyen tarafından kendisine bilgi verildikten sonra Veri ihlalinden haberdar olduğu var sayılacaktır. Haberdar olduktan sonra veri sorumlusunun KVKK'na en geç 72 saat içerisinde bildirim yapması gerekir		bulundurmalıdır. Kontrolörlerinden herhangi biri tarafından bu güvenlik açığından yararlanıldığına dair bir kanıt yoksa, bildirimde bulunulabilir bir ihlal meydana gelmemiş olabilir, Ancak durum kaydedilebilir veya GDPR Madde 32'den kaynaklı yükümlülüklere aykırılık söz konusu olabilir. Zira bahse konu maddeye göre veri sorumlusu ve işleyen, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, aşağıdakiler de dahil olmak üzere uygun teknik ve düzenlemeye ilişkin tedbirler uygular:
viii. Bir siber saldırı sonucu hastanenin sağlık verilerine 30 gün süreyle erişilememektedir.	EVET. Veri Sorumlusu ilgili hastaların sağlık ve veri güvenliği bakımından yüksek risk söz konusu olduğu için bildirimde bulunmalıdır.	EVET. Saldırıdan etkilenen veri sahibi ilgili kişiler bilgilendirilmelidir.	
ix. Çok sayıdaki öğrencinin kişisel verisi 1000den fazla alıcısı bulunan bir posta listesine yanlışlıkla gönderilir. .	EVET. Derhal KVKK'na bildirimde bulunulmalıdır.	EVET. Etkilenen kişisel veri kategorileri ve oluşacak olası riskler değerlendirerek veri sahiplerine bildirim yapılması gerekir.	
x.. Bir doğrudan pazarlama e-mail'i	Evet, çok sayıda kişi ihlalden etkilenirse,	EVET. Etkilenen kişisel veri	

alıcılara “to-kime” ve “cc-karbon kopya” satırları görünecek şekilde gönderilir. Bu nedenle alıcılar e-mailin gönderildiği diğer alıcı adreslerini görebilirler.	özel nitelikli veriler ifşa edilmişse (örneğin bir psikoterapistin posta listesi) veya diğer faktörler ilgili kişiler açısından yüksek riskler içeriyorsa (örneğin, posta ilk şifreleri içeriyorsa) KVKK’na bildirimde bulunmak zorunlu olabilir.	kategorileri ve oluşacak olası riskler değerlendirerek veri sahiplerine bildirim yapılması gerekir.	Özel nitelikli veriler ifşa edilmez ve yalnızca az sayıda e-posta adresi üçüncü kişilere ifşa edilmişse bildirim gerekli olmayabilir.