

Kişisel Verileri Koruma Kurulu, Veri Sorumluları Tarafından Kullanıcı Güvenliğine İlişkin Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu Yayınlandı

15 Nis 2022

Kişisel Verileri Koruma Kurulu ("**Kurul**") teknik tedbirlere ilişkin yayınlamış olduğu rehberden sonra veri sorumluları tarafından hangi teknik tedbirlerin alınması gerektiği ve gerekçelerine ilişkin bir de kamuoyu duyurusu yayınladı.

15 Nisan 2022 tarihli duyurunun önemli hususları aşağıdaki gibidir:

- Kurul'a son zamanlarda intikal eden veri ihlal bildirimleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesi uyarınca veri sorumlularının uygun veri güvenliği düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri alma yükümlülüğü kapsamında değerlendirilmiştir.
- Özellikle finans, e-ticaret, sosyal medya ve oyun gibi sektörlerde faaliyet gösteren veri sorumlularına ait internet sitelerine girişte kullanılan kullanıcı hesap bilgileri (kullanıcı adı ve parola) bazı internet sitelerinde herkese açık şekilde yayınlanmaktadır.
- Kullanıcı hesap bilgilerinin üçüncü kişilerce elde edilmesi sonucu;
 - Kullanıcıların haberi olmaksızın, veri sorumlularının internet sitelerine aktif giriş yapıldığı,
 - Veri sorumlularının sistemsel ve güvenlik açıkları kullanılarak son kullanıcıların bilgisayarlarına rızalar dışında erişim sağlandığı ve elde edilen kişisel verilerin ekonomik bir değer karşılığında satışa sunulduğu,
 - Kötü niyetli üçüncü kişilerce bu verilerin arşivlenerek veri setleri halinde yeniden pazarlandığı

tespit edilmiştir.

- Kurul, veri sorumlularının ve veri işleyenlerin veri sorumluluğu kapsamında alacakları teknik ve idari tedbirler ile olası veri ihlallerini engelleyerek ilgili kişiler üzerinde oluşan riskin asgari düzeye indirgenebileceği belirtmiştir.
- Yaygın olarak yaşanan veri ihlallerinin önlenmesi ve veri ihlalinin gerçekleşmesi halinde ilgili kişinin zarar görme olasılığının azaltılması için veri sorumlularının risk değerlendirmelerini yaparak gerekli teknik ve idari önlemleri almaları Kurul tarafından tavsiye edilmiştir.

Kurul tarafından önerilen önlemler aşağıdaki gibidir:

- Çift kademeli kimlik doğrulama (two-factor authentication) sistemlerini kurmaları ve kullanıcılarına üyelik başvurusu aşamasından itibaren alternatif güvenlik önlemi olarak sunmaları,

- Kullanıcıların hesaplarına sık erişim sağlayan cihazlar haricinde farklı cihazlar üzerinden giriş yapılıp durumunda, giriş bilgilerinin e-posta, SMS ve benzeri yöntemlerle ilgili kişilerin iletilemesi adreslerine iletilmesinin sağlanması,
- Uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletileme Kuralı) ile veya aynı güvenlik seviyesini sağlayacak şekilde koruma altına alınması,
- Kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunması teminen, güvenli ve güncel karma (hashing) algoritmaların kullanılması,
- IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısı sınırlandırılması,
- İlgili kişilerin en az son beş adet başarı ve başarısız giriş denemeleri ile ilgili bilgilerini görüntüleyebilmelerinin sağlanması,
- İlgili kişilere aynı parolanın birden fazla platformda kullanılmaması gerektiğinin hatırlatılması,
- Veri sorumluları tarafından parola politikasının oluşturulması ve kullanıcılara ait parolaların belirli aralıklarla değiştirilmesinin sağlanması veya bu hususun ilgili kişilere hatırlatılması,
- Yeni oluşturulan parolaların, eski parolalarla (en az son üç parolayla) aynı olması engellenmesi, kullanıcı hesaplarına girişlerde bilgisayar ile insan davranışları ayırt edici güvenlik kodu gibi teknolojilerin (CAPTCHA, dört işlem gibi) kullanılması, erişime izin verilen IP adreslerinin sınırlandırılması,
- Veri sorumlularının sistemlerine giriş yapılan parolaların uzunluğunun asgari 10 karakter olması, büyük-küçük harf, rakam ve özel karakterlerin bir arada kullanılmasına yönelik güçlü parola oluşturulmasının sağlanması,
- Veri sorumlularının sistemlerine giriş için üçüncü parti yazılımlar veya servisler kullanılıyorsa bu yazılımların ve servislerin güvenlik güncelleştirmelerinin düzenli olarak gerçekleştirilmesi ve gerekli kontrollerin yapılması.

Duyurunu tamam metnine bu [başlıktan](#) ulaşabilirsiniz.

İLGİLİ ÇALIŞMA ALANLARI

- [Gizlilik ve Kişisel Verilerin Korunması](#)

Related Attorneys

- [BURCU TUZCU ERSİN, LL.M.](#)
- [CEYLAN NECİPOĞLU, PH.D, LL.M.](#)