CRONOC YAZILIM

E-Bülten

12 Mart– 18 Mart 2022

İçindekiler

Küresel Mahremiyet Asamblesi İcra Komitesi'nin 68. Toplantısı Gerçekleştirildi

Küresel olarak 130'dan fazla veri koruma otoritesinin temsil edilmekte olduğu Küresel Mahremiyet Asamblesi'ni (GPA) yönetmek ve temsil etmekten sorumlu olan GPA İcra Komitesi'ne (Executive Committee) Kurumumuz, 2022 GPA ev sahibi olması dolayısıyla ilk kez 23 Kasım 2021'de katılım sağlamıştı.

Asamble'nin (GPA) 68. İcra Komitesi (ExCo) Toplantısı çevrimiçi ortamda; Meksika, Bermuda, Arjantin, Almanya, Fas ve Avustralya Veri Koruma Otoritelerinin yanı sıra Kurumumuzun da katılımıyla 17 Mart 2022 tarihinde Türkiye saati ile 22.00 – 23.00 saatleri arasında gerçekleştirildi.

Meksika Veri Koruma Otoritesi'nin (INAI) başkanlığında yapılan Toplantı'da; GPA Stratejik Planı'nın mevcut durumu, GPA Sekretaryası'nın geleceği, Referans Panel'in başkanlık seçimi ve GPA'ya üye olmak isteyen otoritelerin akreditasyonu süreçleri görüşüldü.

Diğer yandan 44. GPA Konferansı'nın Kurumumuz ev sahipliğinde Türkiye'de yapılacak olması nedeniyle, Kurum Başkanımız Prof. Dr. Faruk BİLİR tarafından konu ile ilgili bilgilendirme yapıldı. Ayrıca Kurumumuzun GPA Konferansı hazırlıkları sürecinde izleyeceği yol planı bir sunum şeklinde tanıtıldı.

Kaynak:https://www.kvkk.gov.tr/Icerik/7193/Kuresel-Mahremiyet-Asamblesi-Icra-Komitesi-nin-68-Toplantisi-Gerceklestirildi

Kullanıcı Güvenliğine İlişkin Veri Sorumluları Tarafından Alınması Tavsiye Edilen Teknik ve İdari Tedbirlere İlişkin Kamuoyu Duyurusu

Bilindiği üzere, 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasında " veri sorumlusunun;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu" hükme bağlanmıştır.

Mezkûr Kanunun amir hükmü kapsamında Son zamanlarda Kişisel Verileri Koruma Kurumuna intikal eden veri ihlal bildirimleri değerlendirilmiştir. Bu kapsamında; finans, e-ticaret, sosyal medya ve oyun gibi muhtelif sektörlerde faaliyet gösteren veri sorumlularının internet sitelerine giriş için kullanılan kullanıcı hesap bilgilerinin (kullanıcı adı ve parolalar) bazı internet sitelerinde herkese açık şekilde yayınlandığı görülmüştür. Söz konusu kullanıcı hesaplarını elde eden üçüncü kişilerce anılan veri sorumlularının internet sitelerine kullanıcıların haberi olmadan aktif bir şekilde giriş yapıldığı ve ilgili kişilere ait verilerin bu kapsamda görüntülenebildiği tespit edilmiştir.

Ayrıca farklı zamanlarda, veri sorumluları sistemlerinden veya son kullanıcı bilgisayarlarındaki güvenlik açıkları kullanılarak elde edilen kişisel verilerin, hukuka aykırı bir şekilde paylaşıldığı ve ekonomik bir değer karşılığında satışa sunulabildiği görülmektedir. Bununla birlikte ilgili kişilere ait bu veriler elden ele dolaşarak kötü niyetli kişilerce arşivlenerek daha büyük veri setleri halinde yeniden pazarlanabilmektedir.

Veri sorumluları ve veri işleyenler tarafından veri güvenliği kapsamında alınacak teknik ve idari tedbirlerin olası veri ihlal durumlarını ve ilgili kişiler üzerinde oluşturabileceği riskleri minimize edeceği muhakkaktır. Bu kapsamda yaygın olarak yaşanan ve veri ihlallerinin oluşmasına neden olan "aynı kullanıcı adı ve parolanın farklı platformlarda kullanılması, belirli zaman aralıklarında parola değişiminin yapılmaması, iki kademeli kimlik doğrulama vb. giriş yöntemlerinin kullanılmaması" gibi teknik ve idari tedbir eksikliklerinin kişisel veri ihlallerine neden olabildiği görülmektedir.

Yukarıda belirtilen ve yaygın olarak yaşanan veri ihlallerini önlemek veya meydana gelmesi halinde ilgili kişiler üzerinde olumsuz sonuç doğurma olasılığının azaltılmasını teminen, veri sorumluları tarafından bir takım önlemlerin alınmasına ihtiyaç duyulmaktadır.

Bu kapsamda veri sorumlularının;

- 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 yapılması durumunda, giriş bilgilerinin e-posta/sms vb. yöntemlerle ilgili kişilerin iletişim adreslerine iletilmesinin sağlanması,
- Uygulamaların HTTPS (Hypertext Transfer Protocol Secure - Hiper Metin Aktarma Güvenli İletişim Kuralı) ile veya aynı güvenlik seviyesini sağlayacak bir şekilde koruma altına alınması,
- Kullanıcı parolalarının, siber saldırı yöntemlerine karşı korunmasını teminen, güvenli ve güncel karma (hashing) algoritmaların kullanılması,
- IP (Internet Protocol Address) adresinden yapılacak başarısız giriş denemesi sayısının sınırlandırılması,
- İlgili kişilerin en az son 5 adet başarılı 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 olmasının engellenmesi, kullanıcı hesaplarına girişlerde bilgisayar ile insan davranışlarını ayırt edici güvenlik kodu gibi teknolojilerin (CAPTCHA, dört işlem vb.) 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

gibi teknik ve idari tedbirlerden kendi risk değerlendirmelerini yaparak uygun olanlarını almaları tavsiye edilmektedir.

Kaynak:https://www.kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu

➢Şikâyetçinin Yeni Doğan Bebeğine Ait Doğum Belgesinde Yer Alan Kişisel Verilerin Üçüncü Kişiler Tarafından Özel Hastane Olarak Faaliyet Gösteren Veri Sorumlusundan Hukuka Aykırı Olarak Ele Geçirilmesi" Hakkında Kişisel Verileri Koruma Kurulunun 06/07/2021 Tarihli Ve 2021/666 Sayılı Karar Özeti

Kuruma intikal eden şikâyette özetle; şikâyetçinin veri sorumlusu hastanede doğan oğluna ait doğum belgesinin yer aldığı bilgisayar ekran görüntüsünün boşanmış olduğu eski eşi tarafından hastaneden temin edildiği ve Aile Mahkemesinde tarafına açılan yargılamanın iadesi davasına ilişkin dosyada, içeriğinde oğlunun T.C. kimlik numarası, doğum tarihi, anne ve baba adı, hasta numarası vb. kişisel veriler içeren bilgisayar ekran görüntüsünün delil olarak kullanıldığı, konuya ilişkin hastaneye yazılı olarak başvurmasına rağmen başvurusuna, hastane tarafından herhangi bir cevap verilmediği belirtilerek 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) kapsamında gereğinin yapılması talep edilmiştir.

Konuya ilişkin başlatılan inceleme çerçevesinde veri sorumlusundan savunması istenilmiş olup alınan cevabi yazıda özetle;

- Şikayetçi ile hastane arasında şikâyet öncesinde ve sonrasında devam eden bir dava süreci bulunmadığı,
- Hastane bünyesinde sağlık ve destek ekipleri dahil olmak üzere toplam 653 personelin çalıştığı, bu nedenle kuruma çeşitli kanallardan gelen ve kurum tarafından gönderilen evrak ve taleplere ilişkin yoğun bir trafiğin mevcut olduğu, bu nedenle gün içerisinde kuruma gelen ve gönderilen evrak ve talep sayılarının değişkenlik göstermekle birlikte gün içerisinde yaklaşık olarak bu sayının yetmişi bulduğu, evrak trafiğinin yoğunluğu nedeniyle bir hata yaşandığı ve başvurunun ilgili birimlere iletilmesindeki aksaklık nedeniyle başvuru sahibi kişiye dönüş yapılamadığı,
- Cumhuriyet Başsavcılığınca hazırlanan iddianame ve ekinde yer alan görüntünün doğumhane/bebek odasındaki hastaların bilgilerinin takip edildiği ekran görüntüsü olduğunun tespit edildiği,
- Bu ekrana ilgili birimde çalışan yatan hasta misafir hizmetleri çalışanları ve hemşirelerin erişim yetkisinin bulunduğu,
- Mevcut bölümde hizmet veren kişilerin Kişisel Verilerin Korunması Kanunu ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında eğitim aldığı,
- Şikâyetçinin yapmış olduğu suç duyurusu üzerine adı geçen iki kişiden alınan ifadelerden de anlaşılacağı üzere her iki şüphelinin de görevliye fark ettirmeden gizlice ekran görüntüsünü çektikleri ve bu hususun zapt altına alındığı,
- Hastane olarak hasta bilgi gizliliği, hasta mahremiyeti konularındaki prensipleri gereği hasta dosyalarının gizliliği, hasta bilgilerinin paylaşılmaması, hastane dışına çıkarılmaması gerekliliği vb. konularda oldukça detaylı idari ve teknik tedbirler alındığı

belirtilmiştir.

- Kanunun “Kişisel Verilerin İşlenme Şartları” başlıklı 5 inci maddesinin (1) numaralı fıkrasında kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği, (2) numaralı fıkrasında ise kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarından birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olduğu hükümlerinin yer aldığı,

- 6698 sayılı Kanunun “Özel Nitelikli Kişisel Verilerin İşlenme Şartları” başlıklı 6 ncı maddesinin (2) numaralı fıkrasında özel nitelikli kişisel verilerin ilgilinin açık rızası olmaksızın işlenmesinin yasak olduğu, (3) numaralı fıkrasında birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceği, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceğinin hükme bağlandığı,

- Somut olayda, veri sorumlusu bünyesinde kayıt altına alınan kişisel verilerin yer aldığı ve doğumhane/bebek odasındaki hastaların bilgilerinin takip edildiği sisteme Kanuna aykırı olarak üçüncü kişiler tarafından erişim sağlandığı ve şikâyete konu olan ekran görüntüsünün çekildiği,

- Her ne kadar veri sorumlusu tarafından hasta bilgi gizliliği, hasta mahremiyeti, hasta dosyalarının gizliliği, hasta bilgilerinin paylaşılmaması, hastane dışına çıkarılmaması gerekliliği vb. konularda çalışanlara sürekli eğitimler verildiği ve sürece ilişkin yazılı kurumsal dokümanlar oluşturulduğu ifade edilse de söz konusu olayın meydana geldiği ve kişisel veri ihlaline neden olunduğu,

- Veri sorumlusu hastane tarafından kişisel verilere hukuka aykırı erişimi önlemek adına alınan idari ve teknik tedbirlerin yetersiz kaldığı ve sonuç olarak şikâyetçinin velisi bulunduğu ilgili kişiye ait kişisel verilerin üçüncü kişilerce erişimine neden olunduğu

  değerlendirmelerinden hareketle;

- Şikâyete konu olan ekran görüntüsünün hastanenin veri kayıt sistemine ait ekrandan temin edildiği dikkate alındığında, bu konuda veri sorumlusu Hastanenin gerekli teknik ve idari tedbirleri almadığı; bu minvalde veri güvenliğine ilişkin yükümlülüklerin düzenlendiği Kanunun 12 inci maddesinin (1) numaralı fıkrasına aykırı hareket ettiği değerlendirildiğinden, veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına,

- Veri sorumlusu hastaneye çeşitli kanallardan birçok evrak geldiği ve evrak trafik yoğunluğu nedeniyle bir hata yaşandığı bu nedenle ilgili kişiye cevap verilemediği yönünde savunmada bulunulduğu görüldüğünden veri sorumlusunun Kanun kapsamında kendisine yapılan başvurularda Kanunun 13 üncü maddesi ve Tebliğin 6 ncı maddesine uygun olarak hareket etmesi yönünde uyarıda bulunulmasına, bu minvalde ilgili kişinin başvurusunda talep ettiği hususlara ilişkin olarak cevap verilmesi ve ilgili kişiye verilen cevaba dair Kurula bilgi verilmesi hususlarında veri sorumlusunun talimatlandırılmasına

  Karar verilmiştir.

  Kaynak:https://www.kvkk.gov.tr/Icerik/7133/2021-666

Kurul Kararlarında Yer Alan “Ana Faaliyeti Özel Nitelikli Kişisel Veri İşleme” İfadesiyle Ne Anlaşılmalıdır?

Ana faaliyetin özel nitelikli kişisel veri işleme olup olmadığının tespitinde, veri sorumlularının en çok katma değer ürettiği faaliyetleri veya yürüttükleri temel iş ve görevleri gereği özel nitelikli kişisel veri işlenmesi durumu olup olmadığı dikkate alınmalıdır. Diğer bir deyişle burada değerlendirilmesi gereken; veri sorumlularının herhangi bir faaliyeti içerisinde özel nitelikli kişisel veri işlenmesi değil, temel olarak yürütmekte oldukları işlerinin kapsamının özel nitelikli kişisel veri işlenmesi durumudur.

Ayrıca 5429 sayılı Türkiye İstatistik Kanununun 11 inci maddesine istinaden 2012 yılından itibaren ülkemizde tüm kamu kurum ve kuruluşlarında Türkiye İstatistik Kurumu koordinasyonunda oluşturulan NACE Rev.2 ekonomik faaliyet sınıflaması kullanılmakta olup Kurumumuzca da veri sorumlularının faaliyet konularının tespitinde söz konusu NACE faaliyet kodlarından faydalanılmaktadır. Bu kapsamda, veri sorumlularının ticaret sicil kaydında veya vergi levhasında yer alan faaliyet kodları göz önünde bulundurulmaktadır.