thinktech
STM Teknolojik Düşünce Merkezi

AB'de Kişisel Veri Güvenliğinde Yeni Düzenleme ve Türkiye'ye Etkileri

Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (General Data Protection Regulation -GDPR) 25 Mayıs 2018'de yürürlüğe girdi. Esasen GDPR, 24 Mayıs 2016 tarihinde kabul edilmiş olmakla birlikte söz konusu metnin uygulamaya başlama tarihi 25 Mayıs 2018 olarak belirlenmişti. Yönetmeliğin yürürlüğe girmesi, internetteki kişisel veriler üzerinden yapılan işlerde köklü değişikliklere yol açacak. Çünkü bu düzenleme Avrupa Birliği vatandaşlarının verilerini işleyen dünyanın herhangi bir ülkesindeki kurumları kendine tabi kılıyor. Çok sayıda kişisel geliştirici ve küçük işletme sahibi, AB üyesi ülkelerde ikamet etmeseler bile sundukları uygulama, hizmet ve internet siteleri GDPR'ye uygun olmak zorunda kalacak. Peki, bu düzenlemenin siber güvenlik açısından önemi nedir ve dijital ekonomi üzerinde nasıl bir etki yaratacak?

Artık Firewall Yeterli Değil

GDPR'nin amacı kişisel verilerin güvenlik altına alınması. Düzenleme, bu amaca ulaşmak için çevrimiçi olarak veri toplayanlar üzerinde baskıları artırıyor. Veri toplama ve saklama işinde olanlardan sadece teknik olarak değil organizasyonel açıdan da önlemler alması bekleniyor. Bu önlemler arasında kaza sonucu kayıplarda verilerin yasadışı ve izinsiz kullanımını engelleyecek önlemler başta geliyor.

Yönetmelikle; veri toplayan ve işleyenler, kişisel verilerin etkin biçimde korunması, olası sızıntıların önlenmesi ve yönetmeliğin hükümlerinin delinmesine karşı önlemleri almakla yükümlü kılınıyor. Bununla, işletmelerden kişisel verileri işlerken ortaya çıkabilecek riskleri öngörmesi bekleniyor. Özel durumlar gözetilerek, kişisel verilerin kriptolanması ve anonimleştirilmesi de beklenenler arasında.

Veri Toplama ve Saklama Kısıtlanıyor

GDPR'nin ikinci önemli amacı, veri gizliliğini sağlamak. Bunun için düzenleme öncelikle kişisel verinin tanımını genişletiyor. İsim, telefon numarası ve e-posta gibi temel bilgilerin yanı sıra, posta kodu, ehliyet, pasaport, kredi kartı, banka hesap numarası, IP adresi, işyeri adresi, üyesi olunan sendika, genetik bilgileri, sosyal statüsü vb. de kişisel veriler kapsamına alınıyor.

İkinci olarak kişisel veriler üzerinden iş yapan şirketlerin, kullanıcıların onayını alma zorunluluğu genişletiliyor. Pagely'nin Teknoloji Grup Müdürü Josh Eichorn'un altını çizdiği gibi, "Web sitesini ziyaret eden herkesi, kişisel verilerini ticari amaçla kullanmaya yetki vermiş gibi kabul etmek artık söz konusu değil."[1]

Bundan böyle kişisel veriler gerekli olduğunda, kullanıcılardan her aşamada onay istenecek, kullanıcıya karşı açık ve net bir dil kullanılacak.

1 https://www.infosecurity-magazine.com/opinions/life-gdpr-cybersecurity/

Bildirim Zorunlu

GDPR, kişisel verilerin korunmasına ilişkin risklerin oluşması halinde yapılması gerekenleri de sıralıyor. Buna göre, kişisel verilere yasadışı erişim söz konusu olduğunda, elinde veri olanlar yetkili kurumları 72 saat içinde uyarmak zorunda. Ancak veri bulunduran kurumlar, herhangi bir güvenlik ihlalinin kişilerin hak ve özgürlüklerine tehdit oluşturmadığını ispatlayabilirse, bu bildirimin yapılması zorunlu olmayabilir. Veriyi elinde bulunduranlar adına veri işlemciliği yapanlar da olası veri sızıntılarını en kısa zamanda sorumlu oldukları kuruluşlara bildirmek durumunda.

GDPR'de kişisel verilere yönelik bazı tehditler, kişisel hak ve özgürlükler açısından yüksek riskli grupta yer alıyor. Kişisel verileri kontrol edenlerin bunlara özel önem atfetmesi kendi yararlarına olacak. Hassas ve (çocuklar ve yaşlılar gibi) savunmasız kişilere ait verilerin işlenmesi bu tür yüksek riskler arasında sayılıyor. Hukuki sonuçlar doğurabilecek, otomatik kararlara ulaşan veri işlemleri de bu sınıfta yer alıyor. Yönetmeliğe göre, işlemlere geçmeden önce yetkili denetim kurumlarına danışılması ve zorunlu veri koruma etki değerlendirme raporu hazırlanması gerekiyor[2].

Teknoloji Standardı Yok

GDPR, kişisel verileri ellerinde bulunduran şirketlere bunları koruyabilmeleri için bir asgari teknik ve organizasyonel güvenlik standardı belirlemiyor. Ayrıca yönetmelik, bazı belirli alanlarda kişisel verilerin korunmasına ilişkin tam bir uyum gösteremiyor. Çokuluslu şirketlerin birimleri arasındaki veri paylaşımı, düzenleme dışı bırakılmış. Akademik, sanatsal veya edebi ifade amaçlı veri paylaşımına ilişkin düzenlemeler yönetmelikte bulunmuyor. Ayrıca elektronik telekom şirketlerinin işlediği verilere ilişkin hükümler de yönetmelikte yer almıyor[3].

Geliştiriciler Ne Yapacak?

GDPR'nin amacı, Avrupalılara kişisel verilerine kimlerin sahip olduğu konusunda açık fikir vermek ve bu bilgiler üzerinde kontrolü sağlamalarına yardımcı olmak. Developers Alliance adında kâr amacı gütmeyen sivil toplum örgütünün AB Politikaları Direktörü Michela Palladino, "Bu verileri kolaylıkla üretmeniz, silmeniz ve takip edebilmeniz gerekir" diyor[4].

Geliştiriciler, sahip oldukları verilerin haritalarını çıkararak işe başlayabilirler. GDPR, "kişisel veri"yi bir kişiyi tanımlayan, doğrudan veya dolaylı her türlü şey olarak ele alıyor. Buna fotoğraf, hesap adresleri, banka verileri, gönderiler ve tıbbi veriler dahil ediliyor. Buna ilaveten, ırk ve etkin köken, siyasi görüş, dini, felsefi inançlar, sendika üyeliği vb. kategoriler de "Özel veri kategorileri" olarak sıralanıyor.

Geliştiriciler açısından ikinci adım, GDPR ile uyumlu hale gelmek için neleri değiştirmek zorunda olduklarını anlamaları. Bunun basit yolu olası sorunlar ve risklerden kaçınmak için ihtiyaç duyulmayan verilerin toplanmasına son verilmesi ve bunların arşivlerden silinmesidir.

Geliştiriciler ihtiyaç duyulan verilerin nasıl kullanılacağını belirlemeli ve her kullanım öncesi kullanıcının onayını almalıdır. Örneğin iki aşamalı kimlik tespiti için cep telefonu isteniyorsa, bu numaralar başka amaç için kullanılmamalıdır.

Öte yandan bazı verilerin toplanması "meşru çıkarlar" adındaki esnek kategoride yer almaktadır. Örneğin bazı internet sitelerinin yorum kutularında, yorumun yanı sıra aynı yöndeki yorumlardan haberdar edilmesi için

2 https://www.scmagazineuk.com/gdpr-and-cyber-security-an-opportunity-that-cannot-be-ignored/article/739688/

3 https://www.financierworldwide.com/europes-general-data-protection-regulation-from-a-cyber-security-perspective/#.Wvq9lIjRCyI

4 https://spectrum.ieee.org/at-work/tech-careers/what-developers-need-to-know-about-europes-data-privacy-rules

e-posta adresi istenmektedir. Ancak bu e-posta adresinin başka bir siteye otomatik kayıt edilmesi gibi amaçlar için kullanılması onay gerektirmektedir.

Geliştiricilerin ve web sitesi sahiplerinin, IP adreslerinin kayıtlarının tutulması gibi temel süreçler konusunda paniğe kapılmalarına gerek yoktur. Basit erişim kayıtları sık sık değiştiği ve bir kişinin kimliğini belirlemek için tek başına yeterli olmadıkları için sorun teşkil etmemektedir. Buna karşılık IP adresleri davranışlarla korelasyon sağlamak için tutuluyorsa onay alınmalıdır. Ne var ki bunu yapanların küçük işletme sahibi olmayacakları aşikârdır.

Kullanıcı sayısı 1000'i bulmayan küçük web sitesi sahipleri, kanun koyucuların anlık takibine takılmayabilir ancak GDPR haklarını savunan kişilerle yüz yüze kalmayacakları anlamına gelmez. Bu kişiler yetkililere şikâyette bulunabilir. Yetkililer GDPR ile uyumu denetlemeye geçebilir ve ayrıntılı kayıtları takibe alabilir. Bu nedenle küçük web site sahiplerinin ellerindeki verileri küçümsememeleri gerekir.

GDPR'nin, veri kullanımı ve işletilmesi üzerine kurulu dijital sektörlere önemli bir etkisinin olacağını tahmin etmek mümkündür. Kullanıcının rızasının alınması faktörü her türlü kişisel veriye dayalı iş faaliyetlerinin temeli haline gelecektir. Bu açıdan GDPR'de öngörülen cezalar AB vatandaşlarının kişisel verileri üzerinden iş yapmak isteyenleri, yönetmelik kuralları çerçevesinde hareket etmeye zorlayacak gibi görünüyor[5].

Türkiye'de Veri Güvenliği Düzenlemeleri

Türkiye'de kişisel verilerin korunmasına ilişkin yasal düzenleme çalışmaları 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı "Kişisel Verilerin Korunması Kanunu"[6] ile önemli bir aşama kaydetmiştir. 6698 sayılı Kanun, AB Veri Koruma Reformu kapsamında hazırlanan GDPR metninin Avrupa Parlamentosu'nda 2016'da kabulünden kısa bir süre önce yürürlüğe girmiştir. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü'nün Haziran 2017'de yayınladığı, Ayşe Nur Akıncı tarafından hazırlanan "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi" başlıklı raporda[7] 6698 sayılı Kanun'un GDPR'nin Getirdiği Yenilikler Bağlamında değerlendirilmesi de şu şekilde yapılıyor: "Yeni AB Veri Koruma Tüzüğü ile AB üyesi ülkeler arasında veri koruma hukuku bakımından üst seviyede bir uyumun sağlandığı ve Birlik üyelerinin iç hukuk düzenlemelerinden kaynaklanan farklılıkların giderildiği görülmektedir. Söz konusu düzenleme sayesinde Birlik ülkeleri bakımından sadeleştirilmiş, sorunsuz ve verimli bir AB sayısal pazarı hedefi bağlamında küresel rekabet avantajı sağlanacağı değerlendirilmektedir. Başta veri işleyen tarafların artırılmış sorumluluk rejimi, unutulma hakkının kanunla tanımlanması, idari para cezalarına ilişkin yaptırımların artırılması yoluyla caydırıcılığın güçlendirilmesi olmak üzere veri taşınabilirliği ve etki değerlendirmesi ile tasarımdan itibaren güvenlik gibi yenilikçi yaklaşımların 6698 sayılı Kanun'a ve uygulamaya yansıtılmasının faydalı olacağı değerlendirilmektedir. Bu hukuki yaklaşımların bir kısmıyla ilgili uyumlaştırmalar yasal düzenleme gerektirmekle birlikte bir kısmı içinse Kişisel Verileri Koruma Kurumunun yapacağı ikincil düzenlemeler ve uygulama pratikleri yoluyla uyum sağlanabileceği değerlendirilmektedir. Bu çerçevede, 6698 sayılı Kanun tarafından ikincil düzenlemelere bırakılan hususların ele alınmasında Kişisel Verilerin Korunması Kurumu tarafından GDPR hükümlerinin öncelikle dikkate alınmasının faydalı olacağı değerlendirilmektedir."

5 https://www.financierworldwide.com/europes-general-data-protection-regulation-from-a-cyber-security-perspective/#.WvqO4ojRCyI

6 ttp://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

7 http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf