KASIM 2024 Gökçe SAYI: 132

THE FINE PRINT

Teori değil. Cevap.

TÜRÜNÜN İLK ÖRNEĞİ: AB SİBER DAYANIKLILIK YASASI

- 2025 Cumhurbaşkanlığı Yıllık Programı Yayımlandı: Dijital Dönüşüm ve Sağlık Verileri Alanında Yeni Adımlar
- Uzaktan İletişim Araçları Yoluyla Piyasaya Arz Edilen Ürünlerin Piyasa Gözetimi ve Denetimi Yönetmeliği Yayımlandı

GÜNCEL HUKUKİ GELİŞMELER

- Standart Sözleşme Bildirimi Modülü ve Kılavuzu Yayımlandı
- Avrupa Birliği Komisyonu'ndan Meta'ya 798 Milyon Euro'luk Ceza

Türünün İlk Örneği: AB Siber Dayanıklılık Yasası

Avrupa Birliği üye devletleri arasında dijital ürünlerin siber güvenlik gerekliliklerini uyumlaştırarak bu ürünlerin siber güvenlik standartlarına uygunluğunu sağlamayı amaçlayan AB Siber Dayanıklılık Yasası **(CRA),** 20 Kasım 2024'te AB Resmî Gazetesi'nde yayımlandı.

Siber saldırıların bu denle arttığı dünyamızda, **2031 yılına kadar her 2 saniyede bir saldırı gerçekleşeceğini ve bunun yıllık 251 milyar €'dan fazla bir maliyete neden olabileceğini** öngören raporlarla[1] birlikte, bu yasa adından çokça söz ettirecek.

Elbette AB'deki, siber güvenlik odaklı, Siber Güvenlik Yasası, Direktifi Şebeke ve Bilgi Güvenliği Direktifi **(NIS2)** gibi düzenlemeleri de unutmamak gerekir.

Yasa, genel olarak 11 Aralık 2027'den itibaren uygulanmaya başlayacak olsa da bazı maddeler daha erken tarihlerde uygulama alanı bulacak.

AB Siber Dayanıklılık Yasası Tanımı ve Kapsamı

AB çapında bir ilk olan CRA, tüm AB için tek bir kurallar dizisi oluşturmayı amaçlamakta, veri işleme sistemleri ve ayrıca satışa sunulan bileşenler de dahil olmak üzere tüm yazılım ve donanım ürünlerini kapsamakta.

CRA, üreticileri, yazılım geliştiricileri, ithalatçıları, distribütörleri ve satıcıları kapsayarak, dijital bileşenlere sahip ürünlerin yaşam döngüsü boyunca güvenli olmasını hedeflemekte. CRA'nın öncelikli olarak gömülü olmayan yazılımları geliştiren ve pazarlayan şirketlere odaklandığını söylemek yerinde olacak.

Nesnelerin interneti **(IoT)** cihazları, işletim sistemleri ve yüksek riskli yapay zekâ sistemleri gibi doğrudan veya dolaylı olarak ağa bağlanan tüm ürünler yasa kapsamında. Ancak elbette kapsam dışında kalan bazı istisnalar da mevcut:

- Halihazırda diğer AB kurallarının (**NIS2 Direktifi, AI Act** vb.), kapsama alanına giren cihazlar
- Ürünün esas bileşeni olmayan hizmet olarak yazılım (SaaS) araştırma ve inovasyon için kullanılan ve kâr amacı gütmeyen ücretsiz açık kaynaklı yazılımlar (open-source software) gibi bazı ürünler

Ancak, geliştiricilerinin bir tür ticari faaliyet elde ettiği açık kaynaklı yazılımların kapsamda olduğunu vurgulamak gerekir.

CRA, ürünleri önem seviyelerine göre önemli ve kritik olacak şekilde iki ana kategoriye ayırır:

- **Önemli ürünler:** Ürünler, siber güvenlik için kritik işlevler sağlıyor veya manipülasyonla kullanıcı ve ürün güvenliğini olumsuz etkileyebiliyorsa "önemli" sayılır. Dijital unsurları içeren ve kimlik yönetimi, VPN, işletim sistemleri gibi siber güvenlik için kritik işlevler sunan ürünler örnek olarak verilebilir.
- **Kritik ürünler:** Kritik ürünler, güvenlik açıklarının tedarik zincirinde ciddi aksamalara neden olma riskine göre belirlenir. Örnekler arasında güvenlik kutularına sahip donanım cihazları, akıllı sayaç ağ geçitleri ve akıllı kartlar yer alır.

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

CRA'de öne çıkan düzenlemeleri aşağıda sizler için derledik:

Temel Gereklilikler: CRA, dijital ürünlerin siber güvenliğini sağlamak için temel gereklilikleri belirler. Ürünler, riskleri ele alacak şekilde tasarlanmalı, geliştirilmeli ve üretilmelidir. Bu temel gereklilikler arasında güvenlik açıklarının giderilmesi, varsayılan güvenlik yapılandırmalarının sunulması, güvenlik güncellemelerinin zamanında sağlanması ve veri gizliliği, bütünlüğü ile erişilebilirliğinin korunması yer alır.

Üreticilere Getirilen Temel Yükümlülükler: Üreticiler, yetkisiz erişime karşı kontrol mekanizması sağlamalı, veri toplamayı sadece gerekli olanlarla sınırlandırmalı ve olası saldırılara karşı dayanıklılığı sağlamalıdır. Ayrıca, üreticilerin ürün güvenliğini düzenli olarak test etmeleri, güvenlik açıklarını derhal tespit ederek gidermeleri gerekir.

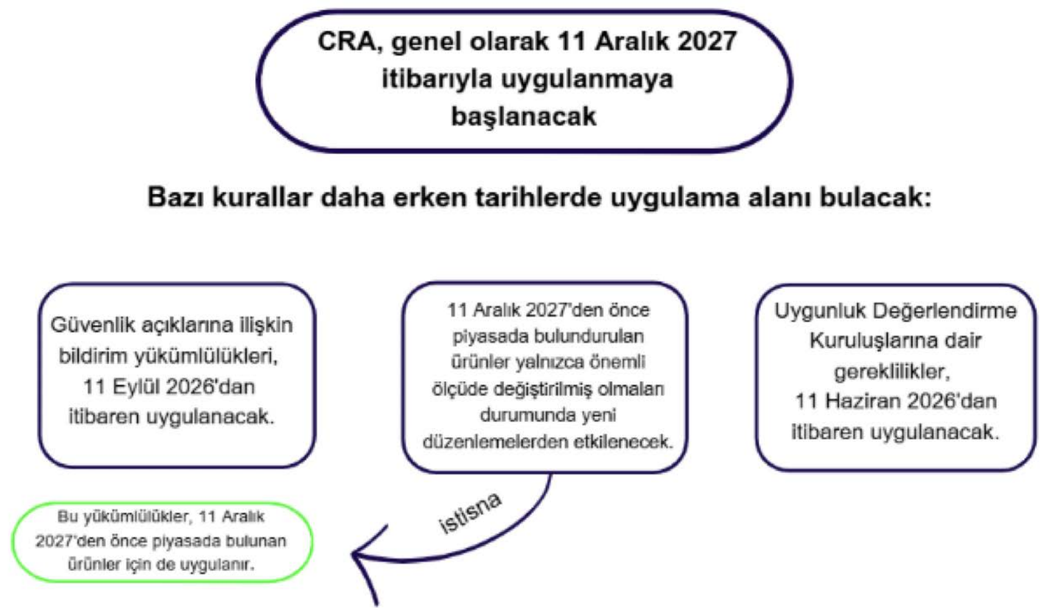
- **Ürün yaşam döngüsü güvenliği:** Üreticiler, ürünün tüm aşamalarında (tasarım, üretim, güncellemeler) siber güvenliği sağlamalı, güvenlik açıklarını gidermeli ve varsayılan güvenlik ayarlarını sunmalıdır.
- **Ürünün uygunluk değerlendirmeleri:** Tüm ürünlerin AB pazarında satılmadan önce güvenlik kontrollerinden geçmesi ve kontrollerden geçen ürünlerin, AB'de satılabilmeleri için gerekli olan CE işareti verilmesi gerekir.
- **Güvenlik açığı bildirimi:** Üreticilerin güvenlik açıklarını bildirmek veya bu tür bildirimleri almak için bir yöntem sağlamaları gerekir. Üreticiler, aktif olarak kötüye kullanılan güvenlik açıklarını 24 saat içinde bildirmeli ve 72 saat sonra daha ayrıntılı bir bildirimde bulunmalı.
- **Üçüncü taraf bileşenlerin entegrasyonu:** Üreticiler, açık kaynaklı bileşenler de dahil olmak üzere başkaları tarafından üretilen bileşenleri veya yazılımları kullanıyorlarsa, bunların güvenliğini sağlamalı, güvenlik açıklarını belgelemeli ve güvenlik açığındaki bileşeni üreten veya bakımını yapan kişi veya kuruluşa durumu bildirmelidir.

Yaptırımlar Ne Olacak?

CRA kurallarına uyulmaması halinde, aşağıdaki tutarlardan en yükseği para cezası olarak uygulanır:

- **Siber güvenlik ihlalleri:** 15.000.000 € veya yıllık satışların %2,5'ine kadar
- **Diğer ihlaller:** 10.000.000 € veya yıllık satışların %2'sine kadar
- **Yanlış bilgi verilmesi:** 5.000.000 € veya yıllık satışların %1'ine kadar

CRA'nın Uygulanma Tarihine İlişkin Tablo:



CRA'nın tam metnine buradan ulaşabilirsiniz (yalnızca AB dillerinde mevcut).

2025 Cumhurbaşkanlığı Yıllık Programı Yayımlandı: Dijital Dönüşüm ve Sağlık Verileri Alanında Yeni Adımlar

2025 yılı Cumhurbaşkanlığı Yıllık Programı 30 Ekim 2024'te Resmî Gazete'de yayımlandı.

Planda pek çok başlık ön plana çıkıyor. Bu kapsamda, önceki yıllarda da hedefler arasında yer alan GDPR'a uyumluluk hedeflerinin küresel ticarette mal ve hizmet ihracatını desteklemek amacıyla tekrar vurgulanması kritik. Yine, özellikle dijital kamu hizmetlerinin kullanıcı odaklı, bütüncül ve katılımcı bir yaklaşımla yaygınlaştırılması ve kullanımının artırılması amacıyla eklenen pek çok tedbir de oldukça anlamlı. Bu amaçla dijital dönüşümde AB mevzuatı ve uluslararası standartlarla uyumlu şekilde siber güvenliğin güçlendirilmesi ve kritik altyapı sektörlerinin güncellenmesine, siber güvenlik standartlarının oluşturulmasına ve AB Siber Dayanıklılık Yasası ile uyumlu mevzuatın hazırlanmasına vurgu yapılıyor. Özellikle Ulusal Veri Stratejisi ve Eylem Planı'nın uygulamaya konulması ve "açık veri" mevzuatıyla ulusal açık veri portalı kurulması hedefleri de önemli hususlardan birkaçı.

Bunlar yanında öne çıkan bir diğer önemli konu, sağlık verilerinin anonimleştirilerek özellikle Ar-Ge ve ekonomik değer yaratma amacıyla ikincil kullanımına yönelik altyapının oluşturulması hedefi.

Bu plan, esasen AB'deki European Health Data Space **(EHDS)** çalışmalarının bizdeki "başlangıç adımları" olarak adlandırılabilir. Nitekim EHDS ile de sağlık verilerinin AB içerisinde birincil ve ikincil kullanımı amaçlanıyor. İlgili "alan", GDPR, Veri Yönetişimi Yasası, Veri Yasası ve NIS2 Direktifi temel alınarak oluşturuluyor. Henüz tamamlanmış bir geçiş olmasa da AB üyesi ülkelerin 2025'e kadar MyHealth@EU'ya katılımının tamamlanması bekleniyor.

EHDS esas olarak; bireylerin elektronik sağlık verilerine dijital erişimini artırmak, elektronik sağlık kayıtları ve ilgili sistemler için tek bir pazar oluşturmak ve sağlık verilerinin araştırma, inovasyon ve politika oluşturma süreçlerinde güvenli kullanımını sağlamak amacıyla kurgulanmıştı.

Kritik olan ikincil kullanım ise plandakine benzer. Bu kapsamda EHDS uyarınca; gereken şartların sağlanması halinde,

- İkincil kullanım için sağlık verilerine siber güvenlik standartlarına uygun, kapalı ve güvenli ortamlarda erişilebilecek ve yalnızca anonimleştirilmiş veya takma adla işlenmiş veriler kullanılabilecek.
- İlgili sağlık verileri araştırma, inovasyon, halk sağlığı ve kişiselleştirilmiş tıp gibi alanlarda kullanılabilecek.
- Bu verilere erişim üye devletlerin katılımı ile "HealthData@EU" dijital altyapısı üzerinden sağlanacak.

Planın mevzuatımıza nasıl yansıyacağı ve özellikle sağlık verilerinin ikincil kullanımı için nasıl bir sistematik kurgulanacağı sektörde merak konusu.

2025 yılı Cumhurbaşkanlığı Yıllık Programı'nın tam haline buradan ulaşabilirsiniz. EHDS'ye ilişkin daha detaylı bilgiye ise buradan ulaşabilirsiniz (Yalnızca İngilizcesi mevcut).

Uzaktan İletişim Araçları Yoluyla Piyasaya Arz Edilen Ürünlerin Piyasa Gözetimi ve Denetimi Yönetmeliği Yayımlandı

Uzaktan İletişim Araçları Yoluyla Piyasaya Arz Edilen Ürünlerin Piyasa Gözetimi ve Denetimi Yönetmeliği **(Yönetmelik)** 30 Ekim 2024'te Resmî Gazete'de yayımlandı. Yönetmelik, internet kanalları başta olmak üzere, uzaktan iletişim araçları yoluyla piyasaya arz edilen ve piyasada bulundurulan ürünlere dair uyulması gereken esasları, güvenlik standartlarını ve piyasa süjelerinin uyması gereken kuralları düzenliyor.

Yönetmelik uyarınca, bir ürünün uzaktan iletişim araçları yoluyla piyasaya arz edilebilmesi veya piyasada bulundurulabilmesi için ilgili teknik düzenlemelere veya Genel Ürün Güvenliği Yönetmeliği'ne uygun olması gerekecek.

Uzaktan iletişim araçlarıyla satış yapan iktisadi işletmelerin ürünleri, Türkiye'deki yerleşik nihai kullanıcıları hedefliyorsa "piyasada bulundurulmuş" kabul edilecek ve bu mevzuata uyumluluk gerekecek. Aşağıdaki durumların varlığı halinde iktisadi işletmecilerin Türkiye'deki nihai kullanıcıları hedeflediği kabul edilebilecek:

- Satış ilanlarında Türkçe dil, uyarı ve güvenlik bilgilerinin bulunması,
- Fiyatın Türk lirası olarak belirtilmesi,
- Türkiye'ye sevkiyat veya adres seçeneği sağlanması,
- Alan adının Türkiye'ye sevkiyat yapılabilen bölgelerde kayıtlı olması.

Bu konu, yurt dışından Türkiye'ye satış yapan pek çok platform için kritik öneme sahip.

İktisadi işletmeci uzaktan iletişim araçları yoluyla piyasaya arz ettiği veya piyasada bulundurduğu ürüne ilişkin gereken bilgileri satış ilanına yansıtacak. Bu bilgiler Yönetmelik ve ürünlerin kendi ilgili mevzuatında detaylıca düzenleniyor.

Aracı hizmet sağlayıcı, nihai kullanıcıların ürün güvenliği konusunda hızlı ve doğrudan iletişim kurabilmesi için bir elektronik temas noktası belirleyecek ve bu sayede tüketiciler temas noktalarından ürünlerin güvenliği ve uygunluğu ile ilgili şikâyet ve bildirim yapabilecek.

Aracı hizmet sağlayıcı, çevrimiçi platformlarındaki ürünlere ilişkin bilgilere kolay erişimi sağlayacak ve yetkili kuruluşlardan gelen içerik kaldırma taleplerini en geç 24 saat içinde yerine getirecek.

Yönetmelik'te ayrıca; yetkili temsilci, ifa hizmet sağlayıcı ve aracı hizmet sağlayıcıların yükümlülükleri ile ürün güvenliği denetim ve gözetiminden sorumlu yetkili kuruluşların görev, yetki ve sorumlulukları ayrıntılı olarak düzenleniyor.

Yönetmelik'e aykırı hareket edenler ise Kanun ve ilgili diğer mevzuat kapsamında idari yaptırımlarla karşılaşacak.

Yönetmelik'in tam haline buradan ulaşabilirsiniz.

Standart Sözleşme Bildirimi Modülü ve Kılavuzu Yayımlandı

Kişisel Verileri Koruma Kurumu **(Kurum)**, web sitesi üzerinden yayınladığı 25 Ekim 2024 tarihli kamuoyu duyurusuyla, standart sözleşme bildirimlerinin Standart Sözleşme Modülü ile de yapılabileceğini açıkladı.

Bilindiği üzere Kişisel Verilerin Korunması Kanunu **(Kanun)** m.9/5'e göre, standart sözleşmelerin imzalanmasından itibaren 5 (beş) iş günü içerisinde Kurum'a bildirilmesi gerekiyor. Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 14. maddesi uyarınca bu bildirimin fiziki veya kayıtlı elektronik posta **(KEP)** adresi veya Kişisel Verileri Koruma Kurulu **(Kurul)** tarafından belirlenecek diğer yöntemlerle gerçekleştirilebileceği de düzenleniyor.

Fiziki iletimin operasyonel zorluğu ve KEP'in de herkesçe kullanılmaması sebebiyle kolaylaştırıcı yöntemlerin açıklanması bir süredir bekleniyordu. Bu duyuruya ek olarak, standart sözleşme bildirimlerinin gerçekleşmesine ilişkin yöntemleri açıklayıcı nitelikteki Standart Sözleşme Bildirimi Kılavuzu **(Kılavuz)** yayımlandı. Kılavuzda özetle, standart sözleşme modülü kullanım süreçleri bakımından izlenmesi gereken adımlar açıklanıyor.

Modülün kullanımı için izlenmesi gereken adımlar kısaca aşağıdaki gibi:

- Veri sorumlusu/veri işleyen olarak sisteme https://standartsozlesme.kvkk.gov.tr adresi üzerinden kaydolma
- Yetkili kişi ekleme
- Yetkili kişilerin sözleşmede yer alacak tarafları eklemesi
- Yetkili kişinin sözleşme eklemesi (Bu adıma dair önemli bir not olarak; yetkili kişi girişi ile oturum açılmış olunması ve veri sorumlusu/veri işleyen seçimi işleminin tamamlamış olması gerekiyor).
- Sözleşme düzenleme sayfasında taraflar bakımından veri aktaran-alıcı seçimlerinin yapılması, taraf rolü, imzaların tamamlandığı tarih ve dosya açıklaması gibi bilgilerin eklenmesi gerekiyor.

Sözleşme ekleme sayfasından aynı zamanda Kurum'a gönderme işlemi de yapılabilmekte. Bunun için de modülün genel mantığında olduğu üzere yetkili kişi hesabı ile giriş yapılmış olması gerekiyor.

İlgili Kurum duyurusuna buradan, standart sözleşme modülüne buradan, Kılavuza ise buradan erişebilirsiniz.

Avrupa Birliği Komisyonu'ndan Meta'ya 798 Milyon Euro'luk Ceza

Avrupa Birliği Komisyonu **(Komisyon)** Meta'ya, Facebook Marketplace'e fayda sağlayan kötüye kullanım uygulamaları nedeniyle yaklaşık 798 milyon Euro değerinde para cezası kesti. İlgili para cezasına ilişkin Komisyon kararı, 14 Kasım 2024 tarihli basın bülteninde yayımlandı.

Komisyonun kararının dayandırdığı temel, AB antitröst kuralları olup; Meta'nın çevrimiçi seri ilan hizmeti Facebook Marketplace'i, kişisel sosyal ağı Facebook'a bağlaması ve diğer çevrimiçi seri ilan hizmeti sağlayıcılarına adil olmayan ticaret koşulları dayatması.

Para cezasına ilişkin basın açıklamasında, Meta'nın hâkim durumunu kötüye kullanarak Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın iç pazarda veya iç pazarın önemli bir kısmında hâkim durumun kötüye kullanılmasını yasaklayan 102. maddesini ihlal ettiği belirtildi. Komisyon, Meta'nın ihlalinin iki ana konudan kaynaklandığını ifade etti:

- **Meta'nın çevrimiçi seri ilan hizmeti Facebook Marketplace'i kişisel sosyal ağı Facebook'a bağlaması:** Bu durumun, tüm Facebook kullanıcılarının istemleri dışında da Facebook Marketplace'e maruz kalmasına sebebiyet vermesinin ve olayın rekabet boyutu bakımından rakiplerine engel olabileceğinin altı çizilmiş. Komisyon; bu şekilde bir bağlantı ile, Facebook Marketplace'in rakiplerinin elde edemeyeceği tipte, dağıtım anlamında bir avantaj sağlamasını, rekabeti engelleyici nitelikte değerlendirmiş.
- **Meta'nın platformlarında, reklam veren diğer çevrimiçi seri ilan hizmeti sağlayıcılarına tek taraflı olarak haksız ticari koşullar dayatması:** Bu durum bakımından Komisyonun tespiti, özellikle Meta'nın diğer reklam verenlerin reklamlarına ilişkin verileri, yalnızca kendi platformu olan Facebook Marketplace lehine kullanılacağı çerçevesinde olup; yine rekabetin kısıtlanacağına dikkat çekmekte.

Komisyon'un para cezalarına ilişkin 2006 kılavuz ilkeleri temelinde belirlenen para cezası ile birlikte Meta'nın rekabeti engelleyici bu faaliyetlerini durdurması gerektiği hususu, Rekabet Politikasından Sorumlu İcra Kurulu Başkan Yardımcısı Margrethe Vestager tarafından da ayrıca vurgulanmış durumda.

Karara ilişkin ilgili basın bülteninin İngilizce metnine buradan ulaşabilirsiniz.

Editörler

Görkem Gökçe
gorkem.gokce@gokce.av.tr

Doç. Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

Hakkımızda

Gökçe Avukatlık Ortaklığı birleşme ve devralma, iş ortaklığı, özel sermaye ve ortak girişim işlemleri, bankacılık ve finans, sermaye piyasaları, sigortacılık, teknoloji, medya, telekom ve internet, e-ticaret, veri koruma, fikri mülkiyet, regülasyon, ticari alacak takipleri, gayrimenkul ve ticari dava alanlarını içeren geniş bir yelpazede hukuki hizmetler sunan İstanbul'da bulunan bir hukuk bürosudur. Hukuki personel ve uzmanlığımız hakkında daha fazla bilgi için www.gokce.av.tr adresinden web sitemizi ziyaret edebilirsiniz.

Lütfen bizimle iletişime geçin
info@gokce.av.tr
0 212 352 88 33