

Siber hukuk

Türkiye | Avrupa Birliğı |
Birleşik Krallık

2025



Shape the future
with confidence

Siber Hukuk I Türkiye

2024'ü bitirirken...

18 Aralık 2024 I Kişisel Verileri Koruma Kurumu, KVKK Bülten'in 6. sayısını "Kişisel Verilerin Korunması ve Siber Güvenlik" başlığıyla yayımladı.

Kişisel Verileri Koruma Kurumu, KVKK Bülten'in 6. sayısını "Kişisel Verilerin Korunması ve Siber Güvenlik" başlığıyla yayımladı.

Bültenin konu başlıkları incelendiğinde, Siber Suçlarla Mücadele Daire Başkanlığı SİBERAY ile Röportaj, Genel Olarak Kişisel Veri Güvenliğine İlişkin Tedbirler ve Avrupa Birliği'nin Siber Güvenlik Stratejisinde Dönüşüm: NIS2 Direktifi gibi konular yer alıyor.

İlgili kararnameye [buradan](#) ulaşabilirsiniz.

2025'in ilk çeyreği...

8 Ocak 2025 I Siber Güvenlik Başkanlığı kuruldu.

8 Ocak 2025 Tarih ve 32776 Sayılı Resmî Gazetede yayımlanan 177 sayılı Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığı'na bağlı, kamu tüzel kişiliğini haiz, özel bütçeli ve merkezi Ankara'da bulunan Siber Güvenlik Başkanlığı kurulmuştur. Siber Güvenlik Başkanlığı; siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planları hazırlamak, mevzuat çalışmalarını yürütmek, ilgili faaliyetlerin koordinasyonunu sağlamak, bunların etkin şekilde uygulanmasını takip etmek, siber güvenlik konusunda eğitim ve farkındalık çalışmalarını yürütmek, acil durum ve kriz yönetimi planları oluşturmak, siber güvenlik ile ilgili tatbikatları yürütmek başta olmak üzere Kararnamenin 4. maddesinde belirtilen yetki ve görevlere haizdir.

İlgili kararnameye [buradan](#) ulaşabilirsiniz.

19 Mart 2025 I Siber Güvenlik Kanunu yürürlüğe girdi. (1/3)

10 Ocak 2025 tarihinde Türkiye Büyük Millet Meclisi (TBMM) Mili Savunma Komisyonu'na sunulan Siber Güvenlik Kanun Teklifi ("Teklif") 12 Mart 2025 tarihinde TBMM Genel Kurulu'nda kabul edilerek yasalaşmış, 19 Mart 2025 tarihinde yürürlüğe girmiştir.

Siber Güvenlik Kanunu, ulusal siber güvenliği güçlendirme amacıyla çeşitli düzenlemeler getirmektedir. Kanun kapsamında kurumsal veri güvenliği, uluslararası iş birliği ve sertifikasyon süreçleri, idari yapılanma ve hukuki yaptırımlara yönelik önemli yenilikler düzenlenmiştir. Kanunun temel amaçları; Türkiye Cumhuriyeti'nin siber uzaydaki gücünü oluşturan unsurlara yönelik iç ve dış tehditleri tespit edip bunları bertaraf etmek, siber saldırıların etkilerini azaltmaya yönelik esaslar belirlemek, kamu kurumları meslek kuruluşları özel sektör ve diğer kuruluşları siber saldırılara karşı koruyacak düzenlemeler yapmak, ulusal siber güvenlik stratejilerini ve politikalarını belirlemek, siber güvenliğe ilişkin idari teşkilatı kurmaktır.

Siber Hukuk I Türkiye

19 Mart 2025 I Siber Güvenlik Kanunu yürürlüğe girdi. (2/3)

Kanun ile bilişim sistemleri, kritik altyapı, kritik kamu hizmeti, siber güvenlik, siber olay, siber tehdit, siber saldırı, siber tehdit istihbaratı, SOME, varlık, zafiyet ve siber uzay gibi önemli kavramlar tanımlanmıştır. Siber Güvenlik Kanunu kapsamında, 8 Ocak 2025 tarihinde Cumhurbaşkanlığı Kararnamesi ile kurulan Siber Güvenlik Başkanlığı'nın görev, yetki ve sorumlulukları düzenlenmiştir.

Siber Güvenlik Kanunu kapsamında cezai hüküm ve idari para cezası öngörülen eylemler aşağıda yer almaktadır:

- **Bilgi ve belge vermeme veya engelleme:** Kamu kurum ve kuruluşları hariç olmak üzere Kanunla yetkilendirilmiş mercilerden bilgi, belge veya donanım talebine uymayanlara bir yıldan üç yıla kadar hapis ve beş yüz günden bin beş yüz güne kadar adli para cezası uygulanacağı öngörülmüştür.
- **İzinsiz faaliyet gösterme:** Kanun uyarınca alınması gerekli onay, yetki veya izin almadan faaliyet gösterenlere iki yıldan dört yıla kadar hapis ve bin günden iki bin güne kadar adli para cezası verileceği öngörülmüştür.
- **Sır saklama yükümlülüğü:** Sır saklama yükümlülüğünü yerine getirmeyenlere, dört yıldan sekiz yıla kadar hapis cezası verileceği öngörülmüştür.
- **Veri sızıntısı ve yetkisiz paylaşım:** Siber uzayda veri sızıntısı sonucu kişisel veya kritik kamu hizmeti verilerini izinsiz şekilde erişime açan, paylaşan ya da satışa çıkaranlara üç ile beş yıl arasında hapis cezası verileceği öngörülmüştür.
- **Gerçek dışı içerik yayma:** Siber uzayda veri sızıntısı olmadığını bildiği halde, halk arasında endişe, korku ve panik yaratmak amacıyla ya da kurumları hedef göstermek için gerçek dışı içerik oluşturan ve yayanlara, iki yıldan beş yıla kadar hapis cezası verileceği öngörülmüştür.
- **Siber saldırılar ve veri elde etme:** Türkiye Cumhuriyeti'nin siber uzaydaki milli gücüne yönelik siber saldırılar gerçekleştirenler ve bu saldırılar sonucunda elde ettikleri veriyi siber uzayda bulunduranlar için fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde sekiz yıldan on iki yıla kadar; bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda yayan, başka bir yere gönderen veya satışa çıkaranlara on yıldan on beş yıla kadar hapis cezası verileceği öngörülmüştür.
- **Siber güvenlik tedbirleri ve yükümlülükler:** Siber güvenliğe yönelik olarak milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almayan, hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlık'a bildirmeyenler ve kamu kurumları ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanları ve şirketlerden tedarik etmek yönündeki görev ve sorumluluklarını yerine getirmeyenlere bir milyon Türk lirasından on milyon Türk lirasına kadar idari para cezası verileceği öngörülmüştür.
- **Siber güvenlik ürünlerinin yurt dışına satışı:** Kamu kurumları ve kritik altyapıların bilişim sistemlerinde kullanılacak siber güvenlik ürünlerinin yurt dışına satışı ya da bu ürünleri üreten şirketlerin satış, birleşme veya bölünme işlemlerinin onayına ilişkin yükümlülükleri yerine getirmeyenlere on milyon TL'den yüz milyon TL'ye kadar idari para cezası verileceği öngörülmüştür.

Siber Hukuk I Türkiye

19 Mart 2025 I Siber Güvenlik Kanunu yürürlüğe girdi. (3/3)

- **Denetim yükümlölükleri ve ceza uygulamaları:** Denetim altındaki kişilerin cihaz, sistem, yazılım ve donanımları denetim için açık tutmaması, gerekli altyapıyı sağlamaması veya çalışır durumda tutmaması durumunda yüz bin TL'den bir milyon TL'ye kadar para cezası uygulanacaktır. Ticari şirketlerin bu yükümlölükleri yerine getirmemesi durumunda ise ceza, yüz bin Türk Lirasından az olmamak üzere bağımsız denetimden geçmiş yıllık finansal tablolarında yer alan brüt satış hasılatının %1'i ile vergi öncesi kârının %20'sinden yüksek olanına kadar idari para cezası verileceği öngörölmüştür.

İlgili kanun metnine [buradan](#) ulaşabilirsiniz.

Siber Hukuk I Avrupa Birliđi I Birleşik Krallık

2024'ü bitirirken...

10 Aralık 2024 I Siber Direnç Yasası (Cyber Resilience Act) yürürlüğe girdi.

Siber Direnç Yasası (Cyber Resilience Act), dijital bileşen içeren ürünlerin siber güvenlik standartlarını artırmak için üreticiler ve perakendecilerden ürünlerinin yaşam döngüsü boyunca güvenliğini sağlamalarını zorunlu kılmaktadır. Bu yasa, tüketicilerin ve işletmelerin hangi ürünlerin güvenli olduğunu anlamasını kolaylaştırmayı hedeflemektedir.

Yasa, dijital bileşeni olan tüm ürünleri kapsamakta ve üreticilerin siber güvenlik gereksinimlerini her aşamada yerine getirmelerini zorunlu kılmaktadır. Ayrıca, bazı kritik ürünler AB pazarında satılmadan önce üçüncü taraf bir denetimden geçmek zorundadır. CE işareti, ürünlerin bu gerekliliklere uygun olduğunu gösterir.

Yasa, 2020 AB Siber Güvenlik Stratejisi ve NIS2 Direktifi ile uyumlu olup, Avrupa'nın dijital güvenlik altyapısını güçlendirmeyi amaçlamaktadır. Ayrıca yasa 10 Aralık 2024'te yürürlüğe girmiştir, temel yükümlülükler ise 11 Aralık 2027'de uygulanmaya başlayacaktır.

İlgili içeriğe [buradan](#) ulaşabilirsiniz.

2025'in ilk çeyređi...

15 Ocak 2025 I Avrupa Komisyonu, özellikle hastaneler başta olmak üzere sağlık sektörünün siber güvenliğini güçlendirmek için bir AB eylem planı başlattı.

Avrupa Komisyonu, sağlık sektörünün siber güvenliğini güçlendirmek amacıyla 15 Ocak 2025'te bir AB Eylem Planı'nı başlatmıştır. Bu plan, özellikle hastanelerin dijital altyapılarını korumayı hedeflemektedir. Bu girişim, AB genelinde artan siber tehditlere yanıt olarak geliştirilmiş olup, 2023'te sağlık sektöründe raporlanan 309 önemli olayın ardından önceliklendirilmiştir. Plan, Avrupa Birliđi Siber Güvenlik Ajansı (ENISA) bünyesinde bir Siber Güvenlik Destek Merkezi'nin kurulmasını içermektedir. Bu merkez, 2026'ya kadar erken uyarı hizmetleri sunarak hastaneleri gerçek zamanlı tehditlere karşı koruyacaktır. Ayrıca, Siber Dayanışma Yasası'ndan faydalanarak hızlı olay yanıtı hizmetleri sağlanması ve ulusal düzeyde siber güvenlik tatbikatları düzenlenmesi öngörülmüştür.

Eylem Planı, siber tehdit aktörlerini caydırmaya yönelik stratejileri de kapsamaktadır. Fidyeye yazılım saldırılarına karşı üye devletlerin fidye ödemelerini bildirme zorunluluğunu teşvik etmekte ve "Siber Diplomasi Araç Kutusu" ile zararlı faaliyetlere diplomatik yanıtlar verilmesini desteklemektedir. Bu girişimler, dijital sağlık hizmetlerinin güvenliğini artırmayı ve Avrupa Sağlık Veri Alanı'nın etkin uygulanmasına katkıda bulunmayı amaçlamaktadır. Planın uygulanması, 2025 ve 2026 yıllarında paydaşlarla iş birliđi içinde aşamalı olarak gerçekleştirilecektir.

İlgili içeriğe [buradan](#) ulaşabilirsiniz.

Siber Hukuk I Avrupa Birliđi I Birleşik Krallık

31 Ocak 2025 I Birleşik Krallık hükümeti, yapay zekâ sistemlerine yönelik siber güvenlik risklerini ele almak amacıyla hazırlanan AI Siber Güvenlik Uygulama Tüzüğü ve kılavuzu yayımladı.

Birleşik Krallık hükümeti, 31 Ocak 2025'te yayımlanan "Code of Practice for the Cyber Security of AI (Yapay Zekâ Siber Güvenliği Uygulama Kodu) " belgesiyle yapay zekâ (YZ) sistemlerinin siber güvenliğini sağlamak amacıyla bir rehber sunmuştur. Bu belge, YZ sistemlerinin tüm yaşam döngüsü aşamalarında güvenliğı sağlamak için gönüllü bir kılavuz niteliğindedir. YZ, geleneksel yazılımdan farklı olarak veri zehirlenmesi, model gizliliğı ihlali ve komut enjeksiyonu gibi özel riskler taşıdığı için güvenlik yaklaşımları da buna uygun olarak şekillendirilmiştir.

Belgedeki 13 temel ilke, YZ sistemlerinin güvenliğini sağlamak için beş ana aşamaya bölünmüştür:

- **Güvenli tasarım:** YZ sistemlerinin baştan güvenlik odaklı tasarlanmasını sağlar. Geliştiricilerin YZ'ye özgü güvenlik tehditleri hakkında farkındalık sahibi olması, sistemlerin insan denetimi ve hesap verebilirliğini desteklemesi, risk değerlendirmelerinin yaşam döngüsü boyunca yapılması gerektiğı vurgulanmaktadır.
- **Güvenli geliştirme:** Altyapı ve veri güvenliğini ön planda tutar. YZ sistemlerinin güvenli bir şekilde geliştirilmesi, verilerin uygun erişim kontrolleri ile korunması ve altyapının güvenliğinin sağlanması gerektiğı belirtilir.
- **Güvenli dağıtım:** YZ sistemlerinin güvenli bir şekilde kullanıcılara sunulmasını kapsar. Son kullanıcıların bilgilendirilmesi, güvenli dağıtım süreçlerinin belgelenmesi ve modellerin gizliliğinin korunması gereklidir.
- **Güvenli bakım:** YZ sistemlerinin kullanım süresince güvenli kalmasını sağlamak amacıyla, sistemlerin güvenlik güncellemeleri ile korunması, anormal durumların izlenmesi ve bilgi paylaşımının etkin olması gerektiğı vurgulanır.
- **Güvenli kullanım sonu:** YZ sistemlerinin kullanım dışı bırakıldığında, verilerin güvenli bir şekilde imha edilmesi ve sistemlerin doğru şekilde devre dışı bırakılması gerektiğı belirtilir.

Bu rehber, **tedarik zincirindeki paydaşların rollerini** tanımlar. Geliştiriciler, güvenli kodlama ve testlerden sorumluyken; sistem operatörleri, sistemleri çalıştırmaktan ve kullanıcılarla iletişimi yönetmekten sorumludur. Kullanıcılar, verilerinin nasıl kullanıldığını bilmelidir.

Ayrıca, özel durumlar (açık kaynak YZ modelleri gibi) için uyarlamalar önerilmekte ve **GDPR gibi veri koruma yasalarına** uyum vurgulanmaktadır. Tüm bu önlemler, YZ'ye özgü riskleri ele alırken hem ekonomik büyümeyi hem de kamu güvenliğini desteklemeyi amaçlamaktadır.

İlgili içeriğe [buradan](#) ulaşabilirsiniz.

Siber Hukuk I Avrupa Birliđi I Birleşik Krallık

4 Şubat 2025 I AB genelinde siber güvenlik olaylarına karşı hazırlık, tespit ve müdahaleyi iyileştirmek için kabul edilen AB Siber Dayanışma Yasası (The EU Cyber Solidarity Act) yürürlüğe girdi.

Avrupa Birliđi (AB), siber güvenlik alanında dayanışmayı ve kapasiteyi güçlendirmek amacıyla, 4 Şubat 2025 tarihinde **AB Siber Dayanışma Yasası'nı (The EU Cyber Solidarity Act)** yürürlüğe koymuştur.

Bu düzenleme, AB genelinde siber tehditlere karşı hazırlık, tespit ve müdahale süreçlerini geliştirmeyi hedefleyen kapsamlı bir yasal çerçeve sunmaktadır. Yasa, üye devletler arasında iş birliğini teşvik ederek, büyük ölçekli siber saldırılara karşı ortak bir savunma mekanizması tesis etmeyi amaçlamaktadır. Avrupa Siber Kalkanı, Siber Acil Durum Mekanizması ve Siber Olay İnceleme Mekanizması olmak üzere üç temel unsurdan oluşan yasa, AB'nin dijital altyapısını, ekonomisini ve demokratik yapısını koruma altına almayı hedefleyen stratejik bir girişim olarak değerlendirilmektedir.

AB Siber Dayanışma Yasası, Avrupa Siber Kalkanı kapsamında, üye devletlerin ulusal ve sınır ötesi Güvenlik Operasyon Merkezlerini (SOC) birleştiren bir altyapı oluşturmaktadır. Bu altyapı, yapay zekâ ve gelişmiş veri analitiđi teknolojilerinden yararlanarak siber tehditlerin gerçek zamanlı tespitini ve üye devletler arasında hızlı bilgi paylaşımını sağlamayı öngörmektedir. Siber Acil Durum Mekanizması, kritik sektörlerde (örneğin, sağlık, enerji ve ulaşım) hazırlık testlerinin yürütülmesini, AB Siber Güvenlik Rezervinin kurulmasını ve üye devletler arasında teknik yardımın koordinasyonunu içermektedir. Söz konusu rezerv, özel sektörden güvenilir hizmet sağlayıcılarla iş birliđi içinde, ciddi siber olaylara hızlı müdahale kapasitesi sunmak üzere yapılandırılmıştır.

Siber Olay İnceleme Mekanizması, büyük çaplı siber olayların ardından analiz ve değerlendirme süreçlerini yöneterek, gelecekteki müdahale kapasitesini artırmayı amaçlamaktadır. Bu kapsamda, Avrupa Birliđi Siber Güvenlik Ajansı (ENISA), olayların incelenmesi ve raporlanması görevini üstlenmiştir; hazırlanan raporlar, siber güvenlik politikalarının geliştirilmesine yönelik öneriler içerecektir.

İlgili düzenlemeye [buradan](#) ulaşabilirsiniz.

Ekibimiz



Av. Tuğçe Gültekin
EY Türkiye Hukuk Bölümü Şirket Ortağı
tugce.gultekin@tr.ey.com



Av. Seda İlik Obut
EY Türkiye Hukuk Bölümü Müdürü
seda.ilik@tr.ey.com

EY | Daha iyi bir çalışma dünyası oluşturuyoruz

EY olarak, müşterilerimiz, çalışanlarımız, toplum ve dünyamız için değer yaratırken sermaye piyasalarında güveni inşa ediyor ve bu şekilde daha iyi bir çalışma dünyası oluşturuyoruz.

Veri, yapay zekâ ve ileri teknolojiden yararlanarak müşterilerimizin geleceği güvenle şekillendirmesine, günümüzde ve gelecekte karşılaşılabilecekleri sorunlara çözüm üretmelerine yardımcı oluyoruz.

EY ekipleri olarak bağımsız denetim, danışmanlık, güvence, hukuk, kurumsal finansman, strateji ve vergi hizmetleri sunuyoruz. Dünya çapında 150'den fazla ülkede, küresel ağıımız, kapsamlı iş birliklerimiz ve güçlü sektörel deneyimizle müşterilerimize hizmet veriyoruz.

Hep birlikte geleceği güvenle şekillendiriyoruz.

EY adı küresel organizasyonu temsil eder ve Ernst & Young Global Limited'in her biri ayrı birer tüzel kişiliğe sahip olan, bir veya daha çok, üye firmasını temsil edebilir. Sınırlı sorumlu bir Birleşik Krallık şirketi olan Ernst & Young Global Limited müşteri hizmeti sunmamaktadır. Kişisel Verileri Koruma Kanunu (KVKK) kapsamında; EY'nin kişisel verileri nasıl topladığı, kullandığı ve bireylerin sahip olduğu haklara dair bilgilere ey.com/tr_tr/privacy-statement adresinden ulaşabilirsiniz. EY üye şirketleri yerel kanunların yasakladığı bölgelerde hukuk hizmeti sunmaz. Daha fazla bilgi için lütfen ey.com adresini ziyaret edin.

© 2025 EY Türkiye.
Tüm Hakları Saklıdır.

Sadece genel bilgi verme amacıyla sunulan bu yayın muhasebe, vergi, hukuk veya diğer profesyonel hizmetler alanında geçerli bir kaynak olarak kullanılması amacıyla hazırlanmamıştır. Belirli bir konuya ilişkin olarak ilgili danışmana başvurulmalıdır.

ey.com/tr

linkedin.com/ernstandyoung
instagram.com/eyturkiye
x.com/EY_Turkiye
facebook.com/ErnstYoungTurkiye