Avrupa Birliği Dijital Dönüşüm

Siber Güvenlik Mevzuatları

Prof. Dr. Muhammed Ali AYDIN & Dr. Ebu Yusuf GÜVEN

Biz Kimiz
ISTEC
Siber Güvenlik

Amacı:

- IoT cihazlarının siber güvenlik seviyesini test etmek, değerlendirmek ve üreticilere uyumluluk danışmanlığı sağlamak.

Faaliyet Alanları:

- CE & CRA öncesi güvenlik testleri
- Siber Güvenlik Regülasyonları uygunluk değerlendirmesi
- Güvenlik açığı analizi ve raporlama
- Üretim öncesi ve sonrası siber test süreçleri
- Hem laboratuvar ortamında hem sahada test imkanları

Vizyon:

- Türkiye'nin Siber Güvenlik Regülasyonlarına hazırlık sürecinde IoT üreticilerine teknik liderlik ve rehberlik sağlamak.

ISTEC cyber security

Siber Güvenliğin Temel Amaçları

- **Gizlilik (Confidentiality):** Verilere yalnızca yetkili kişilerin erişmesini sağlamak.
- **Bütünlük (Integrity):** Verilerin doğruluğunu ve eksiksizliğini korumak.
- **Erişilebilirlik (Availability):** Verilerin ve sistemlerin ihtiyaç duyulduğunda erişilebilir olmasını sağlamak

ISTEC cyber security

Siber Güvenlik Kavramları

Kavram	Tanım	Kapsam	Hedef
Bilgi Güvenliği	Verilerin gizlilik, bütünlük ve erişilebilirliğini korur.	Fiziksel ve dijital bilgi.	Verilerin güvenliğini sağlamak.
Siber Güvenlik	Dijital sistemleri ve ağları siber tehditlere karşı korur.	Teknolojik altyapı, ağlar, cihazlar.	Dijital tehditlerden korunmak.
Siber Dayanıklılık	Saldırılara karşı direnç ve toparlanma yeteneği.	Proaktif ve reaktif güvenlik yöntemleri.	İş sürekliliğini ve hızlı toparlanmayı sağlamak.
Zero Trust	Hiçbir şeye varsayılan güven duyulmaz; sürekli doğrulama yapılır.	Mikro segmentasyon, IAM, sürekli izleme.	İç ve dış tehditlere karşı sürekli kontrol.

ISTEC
cyber security

Siber Güvenlik ve Regülasyonlara Uyum Neden Önemlidir?

🔐 **Güven ve İtibar:** Yasalara uygunluk, müşteriler ve paydaşlar nezdinde kuruma olan güveni artırır.

💶 **Cezalardan Kaçınma:** Uyumsuzluk durumunda yüksek para cezaları, dava süreçleri ve lisans iptali gibi ciddi riskler doğar.

📈 **Rekabet Avantajı:** Regülasyonlara uyumlu firmalar, yeni pazarlara daha kolay girer ve kamu ihalelerine katılımda avantaj sağlar.

🛡️ **Veri ve Sistem Güvenliği:** Özellikle KVKK, GDPR, NIS2 gibi düzenlemeler; siber güvenliği artırarak kurumsal varlıkları korur.

🔄 **Operasyonel Sürdürülebilirlik:** Standartlara uygun süreçler, kriz anlarında hızlı ve etkili tepki yeteneği sağlar.

ISTEC cyber security

Türkiye 7545 Sayılı Siber Güvenlik Kanunu

- Yürürlük: 19 Mart 2025'te yürürlüğe girdi.
- **Siber Güvenlik Başkanlığı**, Türkiye'nin kamu ve özel sektörü dijital altyapılarını siber tehditlere karşı korumak, ulusal siber güvenlik politikalarını belirlemek ve koordinasyonu sağlamakla görevlidir.
  - Kritik altyapılar belirlenecek, siber risk analizleri ve zafiyet tarama testleri zorunlu,
  - Kamu Kurumları ve özel sektör düzenli olarak siber güvenlik **denetimi yetkisi**,
  - **Siber güvenlik** ürün geliştirilmesi ve hizmetleri Başkanlık kontrolünde yürütülecek.
- Zafiyet veya siber olaylar derhal Başkanlığa bildirilmeli.
- Siber olaylarda başkanlıkça talep edilen bilgi, belge ve destek zamanında sunulmalı.
- Bildirim yükümlülüğünü yerine getirmeyenlere veya Standartlara (?) uyulmaması halinde **para cezası**,
  - Yıllık finansal tablolarında yer alan **brüt satış hasılatının % 5**

ISTEC cyber security

Avrupa Birliği Dijital Pazarı Regülasyonları

- Ürünleriniz CE Belgesine sahip olmalı
  - Kablosuz Ağ özelliği varsa RED
- Firmanız NIS2 Direktifine uygun siber güvenlikli olmalı
- Kişisel verileri GDPR a uygun işlemelisiniz
- Ürünleriniz CRA ya göre siber dayanıklı
- Data Act göre verileri paylaşabilmeli
- AI Act e göre etik, şeffaf ve insan haklarına saygılı

CE Belgesi Nedir?

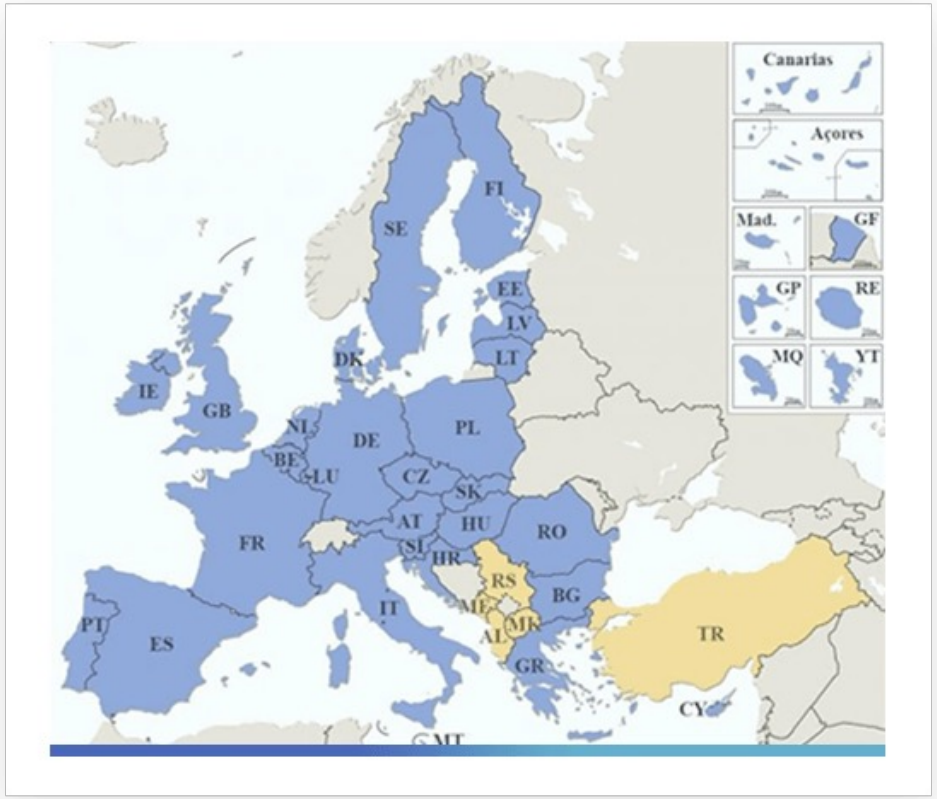
CE Belgesi, bir ürünün **AB mevzuatına uygun olduğunu** ve **sağlık, güvenlik, çevre ve tüketici koruması** şartlarını karşıladığını gösterir. Bu belge ile ürün **AB pazarında serbestçe dolaşabilir.**

Kapsam

- Elektrikli/elektronik cihazlar
- Tıbbi cihazlar, makineler
- İnşaat malzemeleri, basit basınçlı kaplar vb.

Yapılan Başlıca Testler

- EMC (Elektromanyetik Uyumluluk)
- LVD (Düşük Gerilim Direktifi)
- RED (RF, EMC, SAR, **Siber Güvenlik**)
- RoHS (Zararlı Madde Sınırlaması)
- Mekanik ve çevresel güvenlik testleri



Telsiz Ekipmanları Yönetmeliği
Radio Equipment Directive (RED)

- Kablosuz iletişim özellikli cihazların CE işareti alabilmesi için güvenlik, elektromanyetik uyumluluk ve spektrum kullanımı açısından belirli gereklilikleri karşılamasını zorunlu kılan bir regülasyondur.
- RED Delegated Act ile 3 yeni başlık eklendi.
  - (d): Kişisel verilerin korunması,
  - (e): Kötüye kullanım yoluyla ağlara zarar verilmesinin önlenmesi,
  - (f): Şebeke ve hizmetlere erişimin korunması
- RED uyumlaştırılmış (harmonize) standartlar
  - CEN-CENELEC: EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024
  - **1 Ağustos 2025** tüm kablosuz/radyo cihazları CE Belgesi almak için zorunlu.

ISTEC cyber security

General Data Protection Regulation (GDPR)

Yürürlük Tarihi: 25 Mayıs 2018

AB içinde veya dışında faaliyet gösteren ve AB vatandaşlarının kişisel verilerini işleyen tüm kuruluşları kapsar.

- **Veri Sorumluluğu:** Kurumunuzun işlediği her kişisel veri için yasal bir dayanağa sahip olması gerekir.
- **Açık Rıza & Bilgilendirme:** Veri sahibinin açık rızası alınmalı, ne için toplandığı net şekilde açıklanmalıdır.
- **Haklar:** Bireyler, verilerine erişme, düzeltme, silme (“unutulma hakkı”) ve taşınabilirlik haklarına sahiptir.
- **İhlal Bildirimi:** Veri ihlali durumunda 72 saat içinde yetkili otoriteye bildirim zorunludur.
- **Para Cezaları:** Uyulmaması durumunda yıllık cironun %4’üne kadar idari para cezası verilebilir.

ISTEC cyber security

NIS 2 - Ağ ve Bilgi Sistemlerinin Güvenliği

- **Yürürlüğe Giriş Tarihi:** 16 Ocak 2023

- Enerji, ulaşım, sağlık, dijital altyapı gibi kritik sektörlerde faaliyet gösteren şirketlerin siber güvenliğini artırmak için getirilmiş bağlayıcı kurallar ve yükümlülükler setidir.

- AB'de hizmet sunan veya faaliyet gösteren **AB dışı şirketler de** NIS2 kapsamındadır.

- **Büyüklük**: Orta ve büyük ölçekli işletmeler. Genellikle 50'den fazla çalışanı olan ve yıllık cirosu 10 milyon Euro'nun üzerinde olan şirketler.
  - Siber Güvenlik Risk Yönetimi
  - Olay Bildirimi Yükümlülüğü 24 Saat / 72 Saat / 1 Ay
  - Yönetim Seviyesinde Sorumluluk
  - Uyumluluk ve Denetim
  - AB Dışında Yer Alan Şirketler İçin Ek Sorumluluk

ISTEC cyber security

Cyber Resilience Act (CRA) Nedir?

Siber Dayanıklılık Yasası, AB'de piyasaya sürülen tüm "dijital öğe içeren ürünler" için **zorunlu siber güvenlik gereklilikleri** getiren bir regülasyondur.

Amaç:

- Ürünün **yaşam döngüsü** boyunca siber güvenliğini sağlamak,
- Açıkları takip, azaltmak ve kullanıcıları korumak,
- AB içinde güvenli dijital ürün ekosistemi oluşturmak.

Kapsam:

- Başka bir regülasyon kapsamında olmayan yazılım ve donanım içeren tüm ürünler,
  - Örn. IoT cihazları, işletim sistemleri veya güvenlik yazılımları...

ISTEC cyber security

CRA Kapsamı

Doğrudan ya da dolaylı olarak diğer cihazlara veya ağlara bağlanabilen dijital bileşenlere sahip tüm donanım ve yazılım ürünleri bu düzenlemenin kapsamındadır.

Kapsam:

- Ağ bağlantılı cihazlar (router, switch, akıllı ev cihazları, vb.)
- Yazılımlar (OS, VPN, Parola yöneticileri)
- Açık kaynak yazılım (Ticari amaçlı kullanılıyorsa)
- Class I, Class II ve Critical Products 11 Aralık 2025'te Teknik açıklamalar & sınıf tanımlamaları

Kapsam Dışı:

- Sadece ulusal güvenlik amacıyla kullanılan ürünler
- Kendine özgü AB regülasyonuna tabi olan ürünler
- Örn. tıbbi cihazlar, havacılık ve otomotiv ekipmanları
- Geliştirme/test amacıyla piyasaya sürülmeyen yazılımlar

ISTEC cyber security

CRA Gereklilikler & Zorluklar

Gereklilikler:

- Uçtan-uca siber güvenlik gereklilikleri
- Güvenlik açığı bildirim ve yönetimi zorunluluğu
- Class I için uygunluk beyanı Class II ürünler için 3. taraf onaylı test
- Üreticiler AB uygunluk beyanı düzenler, **10 yıl boyunca** veya **destek süresi**
- Eylül 2026 Güvenlik açıkları ve olayları bildirim yükümlülüğü,

Zorluklar:

- Ek test yükleri ve maliyetler
- Yazılım destek süresi belirleme zorunluluğu
- Uyumsuzluk halinde **15 milyon €** veya **ciro %2,5** ceza

ISTEC cyber security

Data Act

Yürürlük Tarihi: 11 Ocak 2024 Uygulama Başlangıç Tarihi: 12 Eylül 2025

Avrupa Birliği tarafından kabul edilen ve dijital ürün ve hizmetlerden üretilen verilerin kullanıcıya ait olduğunu kabul ederek, kimlerle paylaşılabileceği ve nasıl erişileceği konularını düzenleyen bir yasadır.

Kimleri İlgilendiriyor?

- IoT cihaz üreticileri (örneğin akıllı ev cihazları, araçlar)
- Yazılım ve dijital hizmet sağlayıcıları

Temel Hak ve Zorunluluklar

- Kullanıcı, verisine erişebilir ve bu veriyi başkalarıyla paylaşabilir.
- Üretici ya da veri sahibi, **bu veriyi kullanıcıya sunmakla yükümlü.**
- API, SDK gibi teknik yollarla bu paylaşım **pratik ve güvenli** hale getirilmeli.

ISTEC cyber security

AI Act

- Yürürlük Tarihi: 11 Ocak 2024 Uygulama Başlangıç Tarihi: 12 Eylül 2025

- Avrupa Birliği'nin yapay zekâ sistemlerinin geliştirilmesi, pazarlanması ve kullanımı için oluşturduğu ilk yatay regülasyondur. Bu tüzük, risk temelli bir yaklaşım benimseyerek yapay zekâ sistemlerini sınıflandırmakta ve bu sistemlerin taşıdığı riske göre farklı düzeyde yükümlülükler getirmektedir.
  - Kabul Edilemez Risk (Unacceptable Risk):Temel haklara aykırı sistemler yasaktır.
  - Yüksek Risk (High Risk):Sağlık, ulaşım, eğitim, adalet gibi alanlarda kullanılan sistemleri.
  - Sınırlı Risk (Limited Risk): Kullanıcının AI ile etkileşimde olduğunu bildiği, şeffaflık gerektiren uygulamalar.
  - Minimal Risk (Minimal Risk):Genel amaçlı, gündelik kullanımda olan yapay zekâ uygulamaları.

ISTEC cyber security

AI Act Yönetim, Uygulama ve Yaptırımlar

European Artificial Intelligence Office (AI Office)	Avrupa Komisyonu bünyesinde kurulan bu birim, AI Act'in genel uygulanmasından sorumludur. GPAI (General-Purpose AI) sağlayıcılarını denetler, teknik standartların ve rehberlerin geliştirilmesini koordine eder.
European Artificial Intelligence Board (EAIB)	Üye devletlerin ulusal denetim otoritelerinden oluşur. AI Act'in AB genelinde tutarlı şekilde uygulanmasını sağlar, görüş ve tavsiyeler sunar.
Advisory Forum	Sanayi temsilcileri, KOBİ'ler, sivil toplum, akademi ve teknik uzmanlardan oluşur. AI Office'e teknik ve sektörel geri bildirim sağlar.
Scientific Panel of Independent Experts	Akademik ve teknik uzmanlardan oluşur. Genel amaçlı AI sistemlerin risklerini değerlendirme, yeni teknolojilere dair bilimsel görüş sunma görevindedir.

İdari Para Cezaları: Yıllık cironun %6'sına kadar çıkabilir.
Pazardan Men: Uyumsuz AI sistemleri AB pazarından men edilebilir.
Yükümlülükler: Uygunluk değerlendirmesi, CE işareti, teknik dokümantasyon ve risk yönetimi gibi yükümlülükler getirilmiştir.

ISTEC cyber security

ISTEC
cyber security

Teşekkürler

istec.com.tr