

#13 DIGITAL OMNIBUS E AI ACT OBBLIGHI PER LE IMPRESE **CYBER RESILIENCE ACT**



LA COMMISSIONE UE SEMPLIFICA L'ATTUAZIONE. NUOVE LINEE GUIDA PER PREPARARSI ALLE REGOLE.

La Commissione europea ha pubblicato le linee guida ufficiali per aiutare produttori, sviluppatori e imprese di ogni dimensione a comprendere e applicare gli obblighi previsti dal Cyber Resilience Act (CRA, Regolamento UE 2024/2847), che introduce requisiti obbligatori di cyber security per i prodotti con elementi digitali immessi sul mercato dell'UE.



OBIETTIVO

Rendere più semplice e concreta la conformità al CRA, offrendo alle imprese indicazioni chiare su come leggere le nuove regole e prepararsi per tempo attraverso interpretazioni ufficiali della Commissione.



CAMPO DI APPLICAZIONE

Chiarire quali prodotti rientrano nel CRA: viene ad esempio precisato che un'app installata localmente è un prodotto con elementi digitali, mentre una web app fruibile solo via browser non lo è, salvo che supporti funzionalità essenziali di un altro prodotto digitale. Vengono inoltre trattati i criteri per alcune soluzioni di trattamento dati da remoto e per il software open source, distinguendo tra contributori, manutentori e soggetti che effettivamente immettono il prodotto sul mercato.



MODIFICHE DEI PRODOTTI

Definire quando una modifica può essere considerata "sostanziale", facendo scattare specifici obblighi di rivalutazione della conformità.



CICLO DI VITA

Fornire indicazioni sulla durata dei periodi di supporto e sulle responsabilità dei produttori lungo l'intero ciclo di vita del prodotto, dalla progettazione alla gestione delle vulnerabilità.



OBBLIGHI DI SICUREZZA

Chiarire come affrontare la segnalazione degli incidenti e delle vulnerabilità attivamente sfruttate (art. 14 del CRA) e come condurre la valutazione dei rischi.



PARTICOLARE ATTENZIONE ALLE PMI

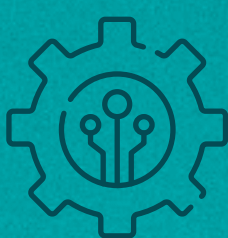
La Commissione dedica un'attenzione specifica a microimprese e PMI, mettendo a disposizione 67 esempi pratici, casi d'uso, diagrammi di flusso e grafici. L'obiettivo è facilitare la conformità evitando, per quanto possibile, oneri amministrativi non necessari.



LE DATE DA TENERE A MENTE

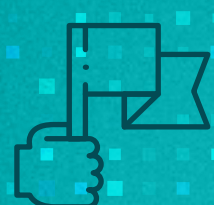
- 11 GIUGNO 2026** → Sono già applicabili le disposizioni sulle autorità di vigilanza del mercato
- 11 SETTEMBRE 2026** → Entrano in applicazione gli obblighi di segnalazione previsti dal CRA.
- 11 DICEMBRE 2027** → Diventano applicabili i principali obblighi del Cyber Resilience Act.

Le nuove linee guida, pur non essendo giuridicamente vincolanti, offrono alle imprese un quadro operativo per iniziare a prepararsi con anticipo.



PERCHÉ È IMPORTANTE

Il CRA introduce un cambio di prospettiva: la ciphersicurezza diventa un requisito da presidiare lungo l'intero ciclo di vita dei prodotti digitali, dalla progettazione fino al supporto post-vendita e alla gestione delle vulnerabilità. La guida della Commissione punta a trasformare la compliance da obbligo regolamentare a processo operativo, fornendo alle aziende strumenti concreti per capire cosa devono fare e quando farlo.



IL PUNTO CHIAVE

Il Cyber Resilience Act è già in vigore dal dicembre 2024: ora l'Europa accelera sulla sua applicazione, offrendo alle imprese indicazioni pratiche per arrivare preparate alle scadenze del 2026 e del 2027.