PAVESIO
STUDIO LEGALE

Luglio 2026

Cyber Resilience Act
Novità normative per i prodotti con elementi digitali

Il Regolamento (UE) 2024/2847 (**Cyber Resilience Act**) introduce un quadro armonizzato a livello europeo in materia di cybersicurezza applicabile ai **prodotti con elementi digitali**.

La nuova disciplina si inserisce nella più ampia strategia dell'Unione europea volta al rafforzamento della resilienza cyber del mercato interno, in modo sinergico rispetto al quadro normativo esistente – in particolare con la normativa NIS 2, incentrata sui presìdi di sicurezza delle reti e dei sistemi informativi nelle organizzazioni obbligate – con l'obiettivo di garantire un livello elevato e uniforme di cybersicurezza dei prodotti lungo l'intero ciclo di vita.

Ambito di applicazione

Il Cyber Resilience Act si applica a tutti i **prodotti con elementi digitali** – qualsiasi prodotto hardware o software e le relative soluzioni di elaborazione dati da remoto – la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile **include una connessione logica o fisica** (diretta o indiretta) a un dispositivo o a una rete.

Restano **esclusi dall'ambito di applicazione i prodotti con elementi digitali già disciplinati da normative settoriali equivalenti**, tra cui, a titolo esemplificativo, quella sui dispositivi medici e medico-diagnostici in vitro, sui veicoli soggetti a omologazione automotive (appartenenti alle categorie M, N e O), sugli aeromobili.

Obblighi per i fabbricanti

A decorrere dall'**11 settembre 2026**, i fabbricanti di prodotti con elementi digitali sono tenuti a:

- notificare, tramite la c.d. piattaforma unica di comunicazione, in corso di istituzione, le **vulnerabilità "attivamente sfruttate"**, vale a dire quelle per le quali sussistono prove attendibili di uno sfruttamento da parte da un soggetto terzo non autorizzato dal proprietario del sistema, nonché gli incidenti gravi che incidono sulla sicurezza dei prodotti (art. 14);

- informare gli **utilizzatori del prodotto con elementi digitali** – siano essi direttamente interessati ovvero, ove opportuno, la generalità degli utilizzatori – della vulnerabilità o dell'incidente rilevato, fornendo indicazioni chiare in merito alle eventuali **misure di mitigazione del rischio/azioni correttive da adottare**, anche mediante formati strutturati idonei a consentirne l'elaborazione automatizzata (art. 14).

A decorrere dall'**11 dicembre 2027**, i fabbricanti di prodotti con elementi digitali hanno specifici obblighi, tra i quali, a titolo esemplificativo:

- assicurare che il prodotto sia stato **progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cybersicurezza** previsti (art. 13, in combinato disposto con Allegato I, Parte I);

Pavesio Studio Legale
info@pavesioassociati.it
www.pavesioassociati.it

Torino
Corso Vittorio Emanuele II, 68
10121 Torino
T. +39 011 51121

Milano
Via Bigli, 2
20121
T. +39 02 303049

- integrare i **principi di sicurezza** sin dalla progettazione e per impostazione predefinita (*security by design e by default*) e adottare un **approccio strutturato di gestione del rischio cyber** lungo l'intero ciclo di vita del prodotto (art. 13);

- garantire di aver adottato **processi di gestione delle vulnerabilità**, comprensivi del rilascio tempestivo di aggiornamenti di sicurezza (art. 13, in combinato disposto con art. 14 e Allegato I, Parte II);

- adempiere agli **obblighi informativi** nei confronti degli utenti, con particolare riferimento ai rischi, alle modalità di utilizzo sicuro e agli aggiornamenti disponibili (art. 13, in combinato disposto con Allegato II);

- apporre la **marcatura CE** quale attestazione di conformità ai requisiti di cybersicurezza applicabili (art. 30);

- redigere e aggiornare la **documentazione tecnica di conformità** del prodotto con elementi digitali includendo **la valutazione dei rischi di cybersicurezza** (art. 31, in combinato disposto con Allegato VII);

- eseguire (o far eseguire) le **procedure di valutazione della conformità** prescelte (art. 32, in combinato disposto con Allegato VIII);

Per i prodotti che rientrano anche tra **i sistemi di IA ad alto rischio**, il Cyber Resilience Act introduce un importante principio di integrazione dei requisiti: la conformità ai requisiti di cybersicurezza del Cyber Resilience Act, può valere anche ai fini dell'**AI Act**, evitando duplicazioni. In estrema sintesi, i requisiti di cybersecurity dell'AI Act si considerano soddisfatti se il prodotto è conforme ai requisiti essenziali e ai processi organizzativi di cui all'Allegato I del Cyber Resilience Act.

Il Cyber Resilience Act segna un cambio di paradigma, imponendo agli operatori economici di **integrare la cybersicurezza quale elemento strutturale dei prodotti digitali**, trasformandola da mero requisito tecnico a vero e proprio fattore strategico di mercato e di responsabilità lungo l'intero ciclo di vita del prodotto.

In tale contesto, è opportuno verificare se l'azienda immetta sul mercato prodotti con elementi digitali e rientri nell'ambito di applicazione del Cyber Resilience Act, al fine di predisporre per tempo le misure necessarie ad assicurare la conformità ai relativi obblighi formali e sostanziali.

Contatti

Torino Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121
Milano Via Bigli 2, 20121 | T. +39 02 303049

info@pavesioassociati.it – www.pavesioassociati.it

Per maggiori informazioni:
AreaCompliance@pavesioassociati.it
AreaLegalTech@pavesioassociati.it

Disclaimer

Il presente documento è redatto in termini generali, unicamente a fini divulgativi e di aggiornamento normativo.