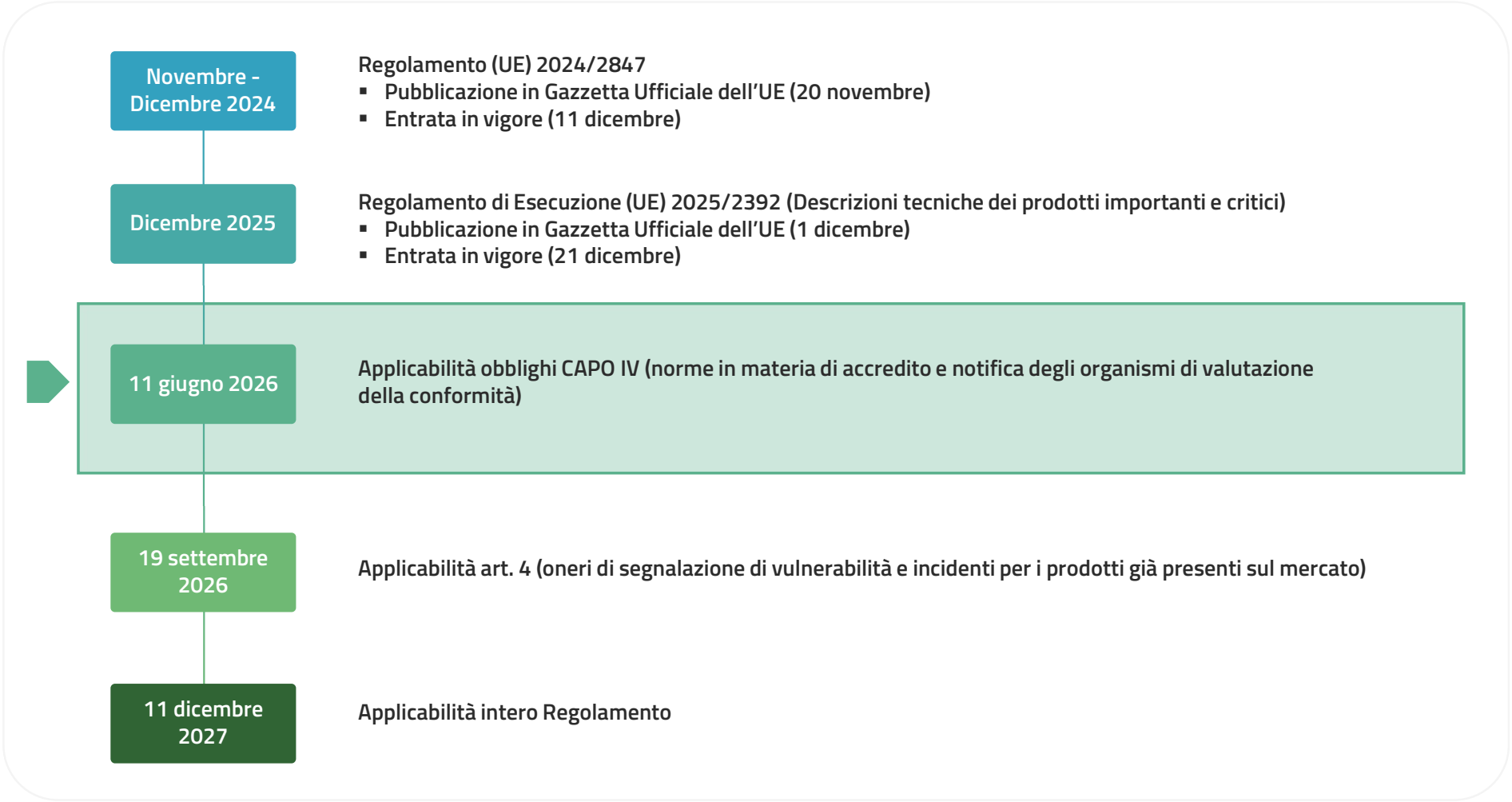
Cyber Resilience Act

12/03/2026

L’ambito di riferimento

Regolamento (UE) 2024/2847 (Cyber Resilience Act)



Regolamento (UE) 2024/2847 (Cyber Resilience Act)

Il *Cyber Resilience Act* (CRA) intende introdurre **un sistema di certificazione e vigilanza** che ha lo scopo di migliorare, secondo parametri comuni, gli standard di cybersicurezza e resilienza per **garantire la protezione degli utilizzatori finali** e, di conseguenza, **aumentare la sicurezza dell'intero ecosistema digitale**.

Obiettivo

Affrontare in modo sistemico le vulnerabilità hardware e software lungo l'intero ciclo di vita del prodotto, dall'ideazione fino alla cessazione del supporto post-vendita (articolo 10; considerando 2 e 38)

Regolamento (UE) 2024/2847 (Cyber Resilience Act)

Prodotto con elementi digitali

Qualsiasi componente hardware o software, comprese le soluzioni di elaborazione dati da remoto, anche se commercializzato separatamente (art. 3).

Il *Cyber Resilience Act* (CRA) **introduce requisiti di sicurezza cibernetica da implementare nella progettazione, nello sviluppo e nella produzione dei prodotti con elementi digitali**, che prevedono, o possono ragionevolmente prevedere, una connessione – diretta o indiretta, logica o fisica – con un dispositivo o una rete, relative procedure di certificazione, obblighi di segnalazione, poteri di vigilanza e sanzione.

Classificazione Prodotti con elementi digitali

Categorie di prodotti con elementi digitali

Particolare regime di tutela e certificazione

- Software open source
- Sistemi IA ad alto rischio con elementi digitali

Prodotti con elementi digitali importanti (art. 7)

I **prodotti con elementi digitali importanti,** divisi in **Classe I** e **Classe II** tenuto conto del progressivo profilo di rischio, soddisfano almeno uno dei criteri seguenti:

a) il prodotto con elementi digitali svolge principalmente funzioni essenziali per la cibersicurezza di altri prodotti, reti o servizi, tra cui la sicurezza dell'autenticazione e dell'accesso, la prevenzione e il rilevamento delle intrusioni, la sicurezza dei terminali o la protezione della rete;

b) il prodotto con elementi digitali svolge una funzione che comporta un rischio significativo di avere effetti negativi in ragione della sua intensità e capacità di perturbare, controllare o danneggiare un gran numero di altri prodotti o la salute, la sicurezza o l'incolumità dei suoi utenti attraverso la manipolazione diretta, come una funzione centrale di sistema, compresi la gestione della rete, il controllo di configurazione, la virtualizzazione o il trattamento dei dati personali.

Prodotti con elementi digitali importanti (art. 7)

ALLEGATO III

PRODOTTI CON ELEMENTI DIGITALI IMPORTANTI

Classe I

1. Sistemi di gestione dell'identità e software e hardware per la gestione degli accessi privilegiati, compresi i lettori di autenticazione e controllo degli accessi, tra cui i lettori biometrici
2. browser autonomi e incorporati
3. sistemi di gestione delle password
4. software che cercano, rimuovono o mettono in quarantena i software maligni
5. prodotti con elementi digitali con funzione di rete privata virtuale (VPN)
6. sistemi di gestione della rete
7. sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)
8. boot manager
9. infrastrutture a chiave pubblica e software per il rilascio di certificati digitali
10. interfacce di rete fisiche e virtuali
11. sistemi operativi
12. router, modem per la connessione a Internet e switch
13. microprocessori con funzionalità legate alla sicurezza
14. microcontrollori con funzionalità legate alla sicurezza
15. circuiti integrati per applicazioni specifiche (ASIC) e reti di porte programmabili dall'utilizzatore (FPGA) con funzionalità legate alla sicurezza
16. assistenti virtuali di uso generale per case intelligenti
17. prodotti per case intelligenti con funzionalità di sicurezza, tra cui serrature intelligenti, telecamere di sicurezza, sistemi di monitoraggio dei neonati e sistemi di allarme
18. giocattoli connessi a Internet disciplinati dalla direttiva 2009/48/CE del Parlamento europeo e del Consiglio [1] che presentano funzionalità sociali interattive (in grado ad esempio di parlare o filmare) o di geolocalizzazione
19. prodotti indossabili personali da indossare o collocare sul corpo umano a fini di monitoraggio della salute (come il tracciamento) e ai quali non si applica il regolamento (UE) 2017/745 o il regolamento (UE) 2017/746, o prodotti indossabili personali destinati all'uso da parte dei bambini e per questi ultimi

Classe II

1. ipervisori e sistemi di *runtime container* che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili
2. firewall, sistemi di rilevamento e prevenzione delle intrusioni
3. microprocessori a prova di manomissione
4. microcontrollori a prova di manomissione

Prodotti con elementi digitali critici (art. 8)

I **prodotti con elementi digitali critici** di cui all'Allegato IV, sono qualificati dal CRA come una sottocategoria degli importanti e sono caratterizzati da un ruolo centrale nelle infrastrutture digitali, con un altissimo potenziale di impatto in caso di attacco.

ALLEGATO IV

PRODOTTI CON ELEMENTI DIGITALI CRITICI

1. Dispositivi hardware con cassette di sicurezza
2. gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio [1], e altri dispositivi a fini di sicurezza avanzati, compreso il trattamento crittografico sicuro
3. carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri

Sistemi IA ad alto rischio con elementi digitali (art. 12)

Un **sistema di intelligenza artificiale** rientra nel campo di applicazione del CRA se:

a) è distribuito o messo in servizio sul mercato dell'Unione;

b) ha una componente software che può essere connessa, anche indirettamente, a una rete;

c) rappresenta un potenziale vettore di vulnerabilità o rischi di cibersicurezza.

Tali prodotti sono considerati conformi ai sensi dell'AI Act (art. 15 dell'AI Act) se soddisfano i requisiti di sicurezza e i processi di fabbricazione CRA (allegato 1, rispettivamente parti 1 e 2) e se la conformità risulta dalla certificazione rilasciata ai sensi del CRA.

Se il sistema di IA è integrato in un prodotto che svolge funzioni di sicurezza o controllo di sistema (es. riconoscimento facciale per l'accesso fisico o logico), è possibile che esso rientri nella classe II dei prodotti digitali importanti (allegato III), comportando quindi la massima certificazione di conformità.

Un sistema di IA ad alto rischio dovrà inoltre garantire una gestione efficace delle vulnerabilità, notificare gli incidenti di sicurezza (articolo 14), e fornire aggiornamenti per tutto il periodo di assistenza previsto.

Requisiti per i prodotti (Allegato I)

I prodotti con elementi digitali devono:

- Essere **privi di vulnerabilità note** al momento dell'immissione sul mercato. Tale obbligo si estende anche ai componenti utilizzati (come ASIC, librerie software, ecc.). Da qui derivano:
  - l'obbligo implicito di adottare e mantenere un **Software Bill of Materials** (SBOM);
  - l'esigenza di una filiera di fornitura qualificata, in grado di gestire aggiornamenti e correzioni tempestive.
- Gestire in modo strutturato **vulnerabilità e aggiornamenti** durante l'intero ciclo di vita del prodotto. In particolare:
  - separare, ove possibile, gli aggiornamenti funzionali da quelli di sicurezza;
  - offrire strumenti per l'aggiornamento automatico.
- Integrare **buone pratiche di cybersicurezza**, tra cui:
  - security by design e configurazioni sicure per impostazione predefinita;
  - meccanismi di autenticazione e tracciamento degli eventi di sicurezza;
  - cancellazione sicura dei dati.

Soggetti CRA e principali obblighi

Soggetti CRA

Fabbricante

Persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o che fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, di monetizzazione o gratuito

Rappresentante autorizzato

Persona fisica o giuridica stabilita nell'Unione che abbia ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti (sub specie di fabbricanti)

Importatore

Persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione

Distributore

Persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà

Gestore di software open source

Persona giuridica, diversa dal fabbricante, che ha la finalità o l'obiettivo di fornire un sostegno sistematico e duraturo per lo sviluppo di prodotti specifici con elementi digitali, che si qualificano come software liberi e open source e destinati ad attività commerciali, e che garantisce la sostenibilità economica di tali prodotti

Soggetti CRA

Fabbricante (artt. 13 e 14)

- Progettazione, sviluppo e produzione, assicurando che il prodotto soddisfi i requisiti essenziali di cybersicurezza
- Gestisce le vulnerabilità per tutto il periodo di assistenza (minimo 5 anni)
- Valutazione e documentazione dei rischi
- Predisposizione della documentazione tecnica e la mantiene disponibile (almeno 10 anni)
- Redige la SBOM
- Notifica gli incidenti ad ENISA
- Appone la marcatura CE e redige la dichiarazione di conformità
- Fornisce le istruzioni sull'uso
- Adotta tutte le misure post market, incluse quelle correttive

Rappresentante autorizzato (art. 18)

Il mandato del rappresentate autorizzato gli consente di:

- Conservare e mettere a disposizione la dichiarazione di conformità UE e la documentazione tecnica
- Fornire informazioni alle Autorità di vigilanza
- Cooperare con le Autorità di vigilanza per eliminare i rischi presentati dal prodotto

È l'interfaccia documentale e amministrativo con le Autorità!

Non può ricevere in delega gli obblighi di:

- Progettazione
- Sviluppo
- Produzione
- Gestione delle vulnerabilità

Obblighi per i fabbricanti (art. 13)

I **fabbricanti** sono i principali responsabili della conformità dei prodotti con elementi digitali e devono assicurarsi che tali prodotti siano progettati, sviluppati e prodotti in modo sicuro. In particolare, devono:

1. **Progettare e fabbricare i prodotti** in conformità con i requisiti essenziali di cibersicurezza (art. 13, par. 1).
2. Integrare misure per **minimizzare le vulnerabilità** e garantire aggiornamenti di sicurezza durante il **periodo di supporto** (art. 13, par. 8).
3. Effettuare la **valutazione della conformità** seguendo la procedura appropriata in base alla categoria del prodotto (articoli da 32 a 36).
4. Redigere e conservare la **documentazione tecnica** (art. 31) e la **dichiarazione UE di conformità** (art. 28).
5. Apporre la **marcatura CE** sul prodotto (art. 30).
6. Fornire **istruzioni d'uso chiare e complete**, comprensive di informazioni sulla cibersicurezza (art. 13, par. 16).
7. Notificare senza ritardo agli organismi competenti qualsiasi **vulnerabilità attivamente sfruttata o incidente di sicurezza grave** (art. 14).
8. **Registrarsi nella banca dati europea delle vulnerabilità** e rispettare gli obblighi di gestione delle vulnerabilità.
9. **Collaborare con le autorità di vigilanza del mercato** e fornire le informazioni necessarie.

Obblighi per i rappresentanti autorizzati (art. 18)

Il **rappresentante autorizzato** fornisce una copia del mandato alle autorità di vigilanza del mercato, su richiesta.

In base al mandato, il rappresentante autorizzato deve almeno:

A. Mettere a disposizione delle autorità di vigilanza del mercato la **dichiarazione di conformità UE** e la **documentazione tecnica** per un periodo di **almeno dieci anni** dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato o per la **durata del periodo di assistenza**, se quest'ultimo è superiore.

B. Su richiesta motivata, fornire all'autorità di vigilanza del mercato tutte le **informazioni** e la **documentazione** necessarie a dimostrare la conformità del prodotto con elementi digitali.

C. Su richiesta, **collaborare con le autorità di vigilanza del mercato** a qualsiasi azione intrapresa per eliminare i rischi posti da un prodotto con elementi digitali che rientra nel suo mandato.

Soggetti CRA

Importatore (art. 19)

Prima dell'immissione nel mercato, verifica:

- L'assolvimento delle procedure di conformità
- La redazione della documentazione tecnica
- La presenza della marcatura CE, della dichiarazione di conformità e delle istruzioni di utilizzo
- Identifica il fabbricante e il suo punto di contatto
- Indica sul prodotto i propri dati di contatto
- Mantiene copia della dichiarazione di conformità (minimo 10 anni)

Se ritiene che il prodotto non sia conforme o presenta rischi di cybersicurezza significativi:
Non lo immette sul mercato e informa le autorità di vigilanza

Quando il prodotto è sul mercato:

- Comunica al fabbricante le vulnerabilità di cui viene a conoscenza
- Adotta le misure correttive e procedere al ritiro/richiamo del prodotto non conforme

Distributore (art. 20)

Prima dell'immissione nel mercato, verifica:

- L'apposizione della marcatura CE
- La disponibilità della dichiarazione di conformità e delle istruzioni in lingua comprensibile
- La presenza dei dati di contatto del fabbricante e dell'importatore

Se ritiene che il prodotto non sia conforme o presenta rischi di cybersicurezza significativi:
Non lo immette sul mercato e informa il fabbricante e l'autorità di vigilanza

Quando il prodotto è sul mercato:

- Comunica al fabbricante le vulnerabilità di cui viene a conoscenza
- Fornisce alle autorità di vigilanza la documentazione necessaria a dimostrare la conformità

Obblighi per gli importatori (art. 19)

Gli **importatori**, che immettono sul mercato dell'Unione prodotti fabbricati in paesi terzi, devono:

1. Verificare che il **prodotto sia conforme** ai requisiti del Regolamento e che sia dotato della documentazione corretta, marcatura CE e dichiarazione di conformità.
2. Assicurarsi che il fabbricante abbia eseguito la **valutazione della conformità** e predisposto la **documentazione tecnica**.
3. Riportare sul prodotto o sull'imballaggio il proprio **nome, indirizzo e marchio registrato**, così da garantire tracciabilità.
4. Non immettere sul mercato prodotti che presentano **rischi noti di cibersicurezza**.
5. Collaborare con le autorità per fornire, su richiesta, **documentazione e informazioni tecniche**.

Obblighi per i distributori (art. 20)

I **distributori**, che vendono o rendono disponibili sul mercato prodotti con elementi digitali, devono:

1. Verificare che i prodotti portino la **marcatura CE**, siano accompagnati dalla dichiarazione UE di conformità e da **istruzioni e informazioni di sicurezza**.
2. Non mettere a disposizione prodotti **non conformi o a rischio**.
3. Garantire che le condizioni di **stoccaggio e trasporto** non compromettano la conformità del prodotto.
4. Interrompere la distribuzione e adottare misure correttive qualora identifichino un **prodotto non conforme**.
5. Cooperare con le autorità competenti su richiesta, fornendo **documentazione tecnica e informazioni**.

Soggetti CRA: Nota strutturale e regola di assimilazione

Nota strutturale del CRA

Il Regolamento è costruito su un'asimmetria tra fabbricante e tutti gli altri soggetti:
Tutti gli obblighi sostanziali di sicurezza (Progettazione, Sviluppo, Produzione, Gestione delle vulnerabilità) sono:

- Intrasferibili
- Sempre responsabilità del fabbricante per l'intero ciclo di vita del prodotto

Gli altri operatori economici hanno obblighi subordinati:

- Verifica documentale
- Segnalazione
- Cooperazione con l'autorità

Si attivano solo in presenza di condizioni di rischio o non conformità

Regola di assimilazione al fabbricante (art. 21)

L'importatore ed il distributore sono soggetti a tutti gli obblighi del fabbricante se:

- Immettono sul mercato il prodotto con il proprio nome e marchio commerciale
- Apportano una modifica sostanziale a un prodotto già immesso sul mercato

Nota bene: la modifica sostanziale fa riconfigurare completamente la catena della responsabilità

Obblighi per i gestori di software open source (art. 24)

I **gestori di SW open source** devono:

1. Mettere in atto e documentare in modo verificabile una **politica in materia di cibersicurezza per promuovere lo sviluppo di un prodotto con elementi digitali sicuro nonché una gestione efficace delle vulnerabilità da parte degli sviluppatori** di tale prodotto. La politica include aspetti relativi alla documentazione, al trattamento e alla correzione delle vulnerabilità e promuove la condivisione di informazioni relative alle vulnerabilità individuate nell'ambito della comunità open source.
2. A richiesta, **cooperare con le autorità di vigilanza del mercato**, al fine di attenuare i rischi di cibersicurezza presentati da un prodotto con elementi digitali che si qualificano come software liberi e open source.
3. A seguito di una richiesta motivata, i gestori di software open source forniscono all'autorità di vigilanza del mercato, in una lingua che possa essere facilmente compresa da quest'ultima, la **politica in materia di cibersicurezza**, in formato cartaceo o elettronico.
4. Nella misura in cui sono coinvolti nello sviluppo dei prodotti con elementi digitali, notificare senza ritardo agli organismi competenti qualsiasi **vulnerabilità attivamente sfruttata** o **incidente di sicurezza grave** (art. 14, par. 1).

Nota bene: gli obblighi si applicano purché il prodotto sia destinato, in ultima istanza, al mercato o sia integrato in contesti commerciali!

Autorità di Sorveglianza del mercato

Vigilanza del mercato e controllo dei prodotti (art. 52)

Autorità di vigilanza del mercato

- Garantire l'efficace attuazione del Regolamento
- Eseguire le attività di vigilanza del mercato in relazione agli obblighi per i gestori di software open source
- Fornire agli operatori economici orientamenti e consulenza sull'attuazione del presente regolamento
- Informare i consumatori riguardo a dove possono presentare reclami rispetto a prodotti con elementi digitali che potrebbero presentare una non conformità

Procedura a livello nazionale relativa ai prodotti che presentano un rischio di cibersicurezza significativo (art. 54)

Autorità di vigilanza del mercato

Effettua, senza indebito ritardo e, se del caso, in cooperazione con il pertinente CSIRT, una valutazione del prodotto con elementi digitali interessato per quanto riguarda la sua conformità a tutti i requisiti di cui al Regolamento. Gli operatori economici interessati cooperano con l'autorità di vigilanza del mercato se necessario.

Prodotto con elementi digitali a rischio significativo non conforme

Chiede senza indugio all'operatore economico interessato di adottare tutte le opportune misure correttive al fine di rendere il prodotto con elementi digitali conforme ai suddetti requisiti, oppure di ritirarlo o di richiamarlo dal mercato entro un termine ragionevole e proporzionato alla natura del rischio di cibersicurezza.

Prodotti conformi che presentano un rischio di cibersicurezza significativo (art. 57)

Autorità di vigilanza del mercato

Chiede a un operatore economico di adottare **tutte le misure del caso** qualora, dopo aver effettuato una valutazione ai sensi dell'articolo 54, ritenga che, sebbene conforme al Regolamento, il prodotto con elementi digitali e i processi messi in atto dal fabbricante presentino un **rischio di cibersicurezza significativo** e comporti inoltre un rischio per:

a) la salute o la sicurezza delle persone;

b) la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali;

c) la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali del tipo di cui all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555 (NIS 2);

d) altri aspetti della tutela dell'interesse pubblico.


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT