20 novembre 2024

lawalert

le ultime novità in tema di normative e giurisprudenza

CYBER NEWS: pubblicato il Cyber Resilience Act (Reg. UE 2024/2847) relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali.

In data 20 novembre 2024 è stato pubblicato in Gazzetta Ufficiale il Regolamento (UE) 2024/2847 (di seguito, il «Regolamento»), che troverà applicazione (salvo alcune specifiche eccezioni indicate nel corpo dell'articolo) dall'11 dicembre 2027, e stabilisce:

- norme per la messa a disposizione sul mercato di prodotti con elementi digitali, al fine di garantire la loro sicurezza informatica;
- requisiti essenziali di cibersicurezza per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione alla cybersecurity di tali prodotti;
- requisiti essenziali di cibersicurezza per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cibersicurezza dei prodotti con elementi digitali durante il periodo in cui si prevede che i prodotti siano in uso e obblighi per gli operatori economici in relazione a tali processi;
- norme sulla vigilanza del mercato, compreso il monitoraggio, e sull'applicazione delle norme e dei requisiti di cui al Regolamento.

AMBITO DI APPLICAZIONE

Il Regolamento si applica ai prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete (salvo alcune esclusioni).

OBBLIGHI

Per essere immessi sul mercato i prodotti con elementi digitali (ossia i prodotti hardware o software e le relative soluzioni di elaborazione dati da remoto, inclusi i componenti hardware/software immessi sul mercato separatamente) devono rispettare i seguenti requisiti:

- Soddisfare i requisiti essenziali di ciber-sicurezza di cui all'Allegato I, parte I del Regolamento, a condizione che i prodotti con elementi digitali stessi siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se applicabile, siano installati i necessari aggiornamenti di sicurezza.

  Tra i requisiti rientrano ad esempio i seguenti: garantire che le vulnerabilità possano essere affrontate mediante aggiornamenti di sicurezza anche automatici, garantire la protezione all'accesso non autorizzato mediante adeguati meccanismi di controllo, proteggere la sicurezza dei dati personali conservati, ridurre al minimo l'impatto negativo dei prodotti stessi o dei dispositivi connessi sulla disponibilità dei servizi forniti da altri dispositivi;
- Realizzare prodotti mediante processi messi in atto dal fabbricante che rispettino i requisiti essenziali di cibersicurezza di cui all'Allegato I, parte II del Regolamento.

  Tra i requisiti summenzionati rientrano i seguenti: identificare e documentare le vulnerabilità ed i componenti contenuti nel prodotto con elementi digitali, affrontare e correggere tempestivamente le vulnerabilità (anche fornendo aggiornamenti di sicurezza), effettuare prove e riesami periodici ed efficaci della sicurezza dei prodotti con elementi digitali.

- Qualora si tratti di «prodotti con elementi digitali importanti» (come sistemi di gestione dell'identità e hardware per la gestione di accessi privilegiati, browser autonomi ed incorporati, sistemi di gestione delle password, sistemi operativi), tali prodotti dovranno essere sottoposti a procedure di valutazione della conformità, e soddisfare i criteri previsti dall'art. 7, comma 2, lett. a) e b) del regolamento.
- Qualora si tratti di «prodotti con elementi digitali critici» (come dispositivi hardware con cassette di sicurezza, gateway per contatori intelligenti, carte intelligenti o dispositivi analoghi), potrebbero essere tenuti ad ottenere un certificato europeo di cibersicurezza, a seconda di quanto specificherà la Commissione Europea mediante appositi atti delegati.
- Qualora si tratti di prodotti con elementi digitali classificati come sistemi di IA ad alto rischio, per essere giudicati conformi ai requisiti relativi alla cibersicurezza di cui all'art. 15 dell'AI ACT qualora: i) soddisfino i requisiti di cui all'allegato I, parte I del Regolamento; ii) i processi messi in atto dai fabbricanti siano conformi ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte II del Regolamento; iii) il conseguimento del livello di protezione della cibersicurezza richiesta a norma dell'art. 15 dell'AI ACT sia dimostrato nella dichiarazione di conformità UE rilasciata a norma del Regolamento.

Sono previsti specifici obblighi per i fabbricanti (come ad esempio obblighi di segnalazione), per i rappresentanti autorizzati, per gli importatori, per i distributori, per i gestori di software open source.

Il Regolamento prevede altresì appositi obblighi di conformità dei prodotti con elementi digitali (ad esempio: i fabbricanti dovranno redigere una dichiarazione di conformità UE, sono indicate regole sulla marchiatura CE, sulla redazione della documentazione tecnica).

TIMELINE

Il Regolamento entra in vigore 20 giorni dopo la sua pubblicazione, avvenuta in data 20 novembre 2024;

L'applicabilità del Regolamento è prevista a partire dall'11 dicembre 2024;

L'articolo 14 (obblighi di segnalazione dei fabbricanti) si applica a decorrere dall'11 settembre 2026;

Il Capo IV (notifica degli organismi di valutazione della conformità) si applica a decorrere dall'11 giugno 2026.

SANZIONI

Le sanzioni saranno stabilite dai singoli Stati menbri dell'UE, e possono ammontare in alcuni casi fino a 15 milioni di euro o al 2,5 % del fatturato mondiale totale annuo dell'esercizio precedente.

Questo articolo è redatto a scopo informativo.
Non si tratta di un parere legale esaustivo in materia di Cibersicurezza. Per eventuali ulteriori informazioni e approfondimenti specifici vi invitiamo a contattare roberto.camilli@bdo.it, gabriele.ferrante@bdo.it e sofia.ferri@bdo.it.

CONTATTI

Viale Abruzzi, 94
20131 Milano
Tel. 02 58 20 10

BDO Law S.r.l. Sta

bdolaw@bdo.it

BDO è tra le principali organizzazioni internazionali di servizi alle imprese.

La Law Alert viene pubblicata con l'intento di tenere aggiornati i clienti sugli sviluppi in ambito legale. Questa pubblicazione non può, in nessuna circostanza, essere associata, in parte o in toto, ad un'opinione espressa da BDO. Nonostante l'attenzione con cui è preparata, BDO non può essere ritenuta responsabile di eventuali errori od omissioni contenuti nel documento. La redazione di questo numero è stata completata il 20 novembre 2024.

www.bdo.it

NEWSLETTER

Vuoi ricevere le notizie da BDO direttamente via email?
Iscriviti alle nostre mailing list.