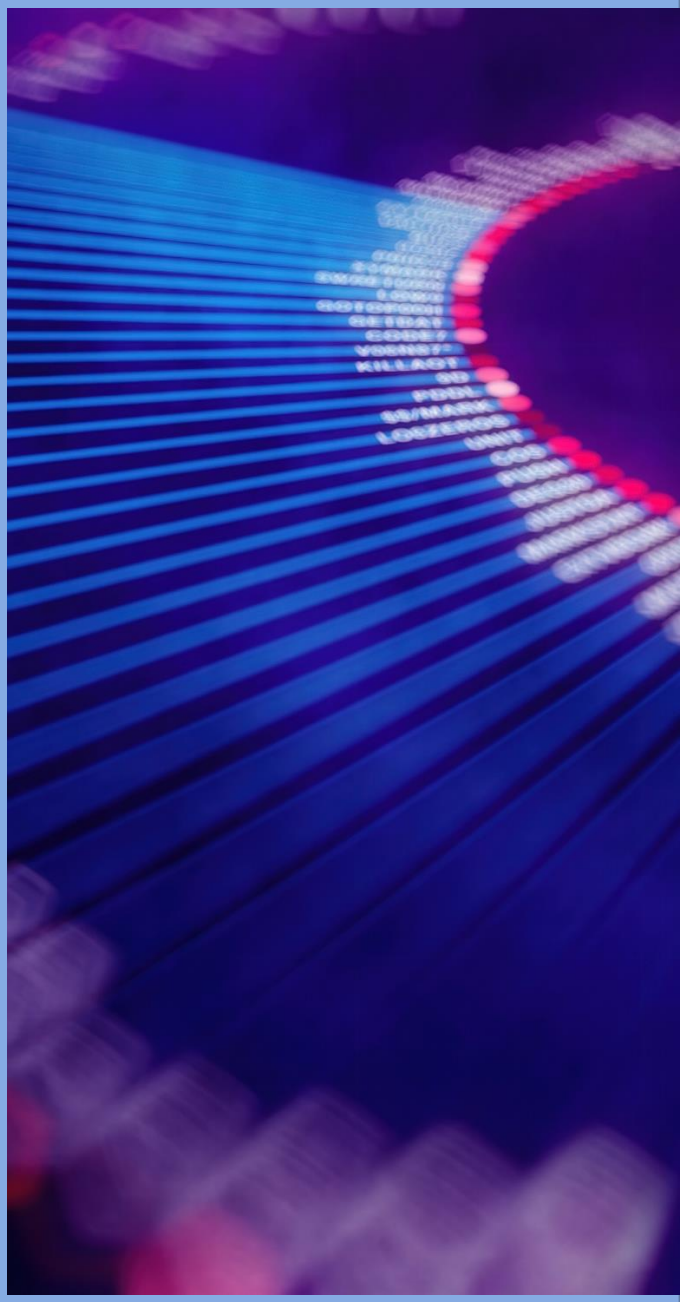
Bird & Bird

Cyber Resilience Act

Pubblicata la Proposta di Regolamento sui requisiti di cybersicurezza per *software* e *hardware*

2 novembre 2022



Cyber Resilience Act: pubblicata la Proposta di Regolamento sui requisiti di cybersicurezza per *software* e *hardware*

Il 15 settembre 2022 la Commissione europea ha pubblicato il testo della Proposta di Regolamento 272/2022 (il c.d. Cyber Resilience Act) (d'ora in avanti la "**Proposta**") con nuovi requisiti per la progettazione, lo sviluppo, la produzione, i processi di gestione delle vulnerabilità e l'immissione sul mercato di *software* e *hardware*.

La Proposta definisce:

a. i **requisiti per la progettazione, lo sviluppo, la produzione e l'immissione sul mercato** di prodotti con elementi digitali;
b. gli **obblighi in materia di cybersicurezza** per gli operatori economici in relazione ai prodotti con elementi digitali;
c. i **requisiti essenziali per i processi di gestione delle vulnerabilità** messi in atto dai produttori per garantire la sicurezza informatica dei prodotti con elementi digitali durante l'intero ciclo di vita;
d. le **norme sulla sorveglianza del mercato**.

In particolare, la Proposta si rivolge a tutti i prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile includa una connessione diretta o indiretta di dati logici o fisici a un dispositivo o a una rete.

Per poter essere immessi sul mercato, i prodotti con elementi digitali (e i relativi processi di fabbricazione) dovranno soddisfare i requisiti essenziali descritti nella Proposta e dovranno essere correttamente installati, manutenuti e utilizzati per lo scopo previsto o in condizioni ragionevolmente prevedibili e, se del caso, aggiornati.

Sono inoltre individuati gli obblighi per i produttori, gli importatori e i distributori di prodotti con elementi digitali.

Per esempio, tra gli obblighi per i produttori vi è quello di effettuare una **valutazione dei rischi di cybersicurezza** associati a un prodotto con elementi digitali e tenere conto del risultato di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto.

A tal fine, i produttori si assicurano che, quando integrano componenti provenienti da terzi in prodotti con elementi digitali, tali componenti non compromettano la sicurezza del prodotto.

Da sottolineare l'**obbligo per il produttore di notificare all'ENISA** (Agenzia dell'Unione europea per la cybersicurezza), senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui ne è venuto a conoscenza, **qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali**.

La Proposta racchiude in un allegato i prodotti con elementi digitali sono considerati **prodotti "critici" (*critical*), tenendo conto dell'impatto delle potenziali vulnerabilità di cybersecurity del prodotto**.

Nel determinare il livello di rischio di cybersicurezza connesso a un prodotto con elementi digitali, si tiene conto di alcuni criteri, tra i quali l'utilizzo previsto del prodotto in ambienti sensibili (per esempio, in ambito industriale) o l'esecuzione di funzioni critiche o sensibili, come il trattamento dei dati personali.

Gli Stati membri dovranno stabilire le sanzioni applicabili in caso di violazioni del Cyber Resilience Act da parte degli operatori economici, tenuto conto delle seguenti soglie massime delle **sanzioni amministrative** previste dalla Proposta:

- per l'**inosservanza dell'obbligo di rispettare i requisiti essenziali di cybersicurezza e dell'obbligo di notifica all'ENISA per i produttori**, è possibile l'applicazione di sanzioni amministrative pecuniarie fino a € 15 milioni o, se il trasgressore è un'impresa, fino al 2,5% del suo fatturato mondiale annuo totale dell'esercizio finanziario precedente, a seconda di quale sia l'importo più alto;
- per l'**inosservanza di qualsiasi altro obbligo previsto dalla normativa in esame**, è possibile l'applicazione di sanzioni amministrative pecuniarie fino a € 10 milioni o, se il trasgressore è un'impresa, fino al 2% del suo fatturato mondiale annuo totale dell'esercizio finanziario precedente, a seconda di quale sia l'importo più alto;
- in caso di **comunicazione di informazioni non corrette, incomplete o fuorvianti** agli organismi notificati e alle autorità di vigilanza del mercato di sorveglianza in risposta a una richiesta, è possibile l'applicazione di sanzioni amministrative fino a € 5 milioni o, se il trasgressore è un'impresa, fino all'1% del suo fatturato mondiale annuo totale dell'esercizio finanziario precedente, a seconda di quale sia l'importo più alto.

***

Successivamente all'approvazione della Proposta, il Cyber Resilience Act entrerà in vigore il ventesimo giorno successivo alla pubblicazione sulla Gazzetta Ufficiale dell'Unione europea.

Tuttavia, le relative disposizioni potranno essere applicate solamente dopo 24 mesi dalla predetta data, ad eccezione della previsione relativa all'obbligo di notifica all'ENISA da parte del produttore che sarà applicabile dopo un anno dalla data di entrata in vigore del Cyber Resilience Act.

Il nostro Studio è a disposizione per fornirvi aggiornamenti in merito alle previsioni e allo *status* di approvazione della Proposta.

Contatti

Gian Marco Rinaldi

Counsel

+390230356000
gianmarco.rinaldi@twobirds.com

Niccolò Anselmi

Associate

+390230356000
niccolo.anselmi@twobirds.com

Marta Breschi

Associate

+390230356000
marta.breschi@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw