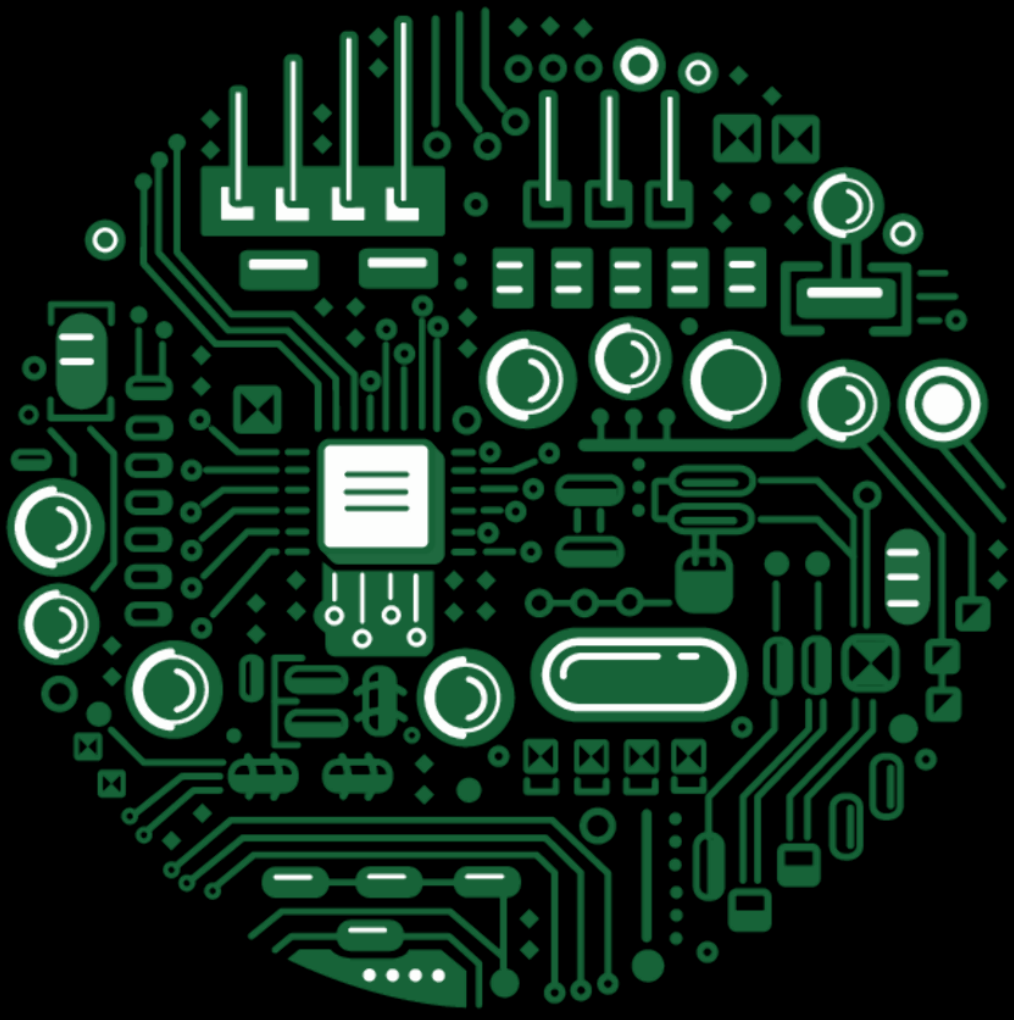
Deloitte.
Legal



Data Protection | *Breaking news*

Novità normative in materia di Cyber Security - Il Cyber Resilience Act

Ottobre 2022

La cybersecurity dei prodotti digitali

La **Commissione europea** ha adottato **una proposta di Regolamento europeo sulla cyber sicurezza, il cd. Cyber Resilience Act**.

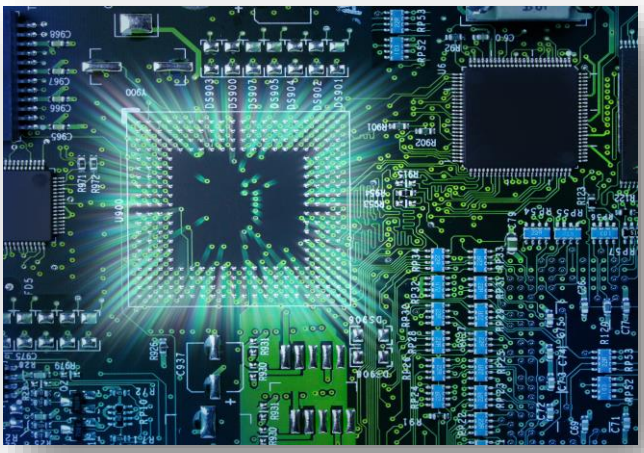
Le regole sono volte a:

- assicurare che **i prodotti con elementi digitali** immessi nel mercato unico europeo siano sicuri;
- i produttori restino responsabili della sicurezza dei dispositivi durante tutto il **ciclo di vita dei prodotti**, fin dall'immissione nel mercato;
- assicurare la **trasparenza** verso i consumatori in merito alle caratteristiche cyber dei prodotti.

Gli obblighi, di natura **tecnica** ma anche **organizzativa**, sono in capo a tutti i soggetti che partecipano alla filiera di prodotti con elementi digitali: **produttori**, **importatori** e **distributori**.

La proposta contiene requisiti «orizzontali» per tutti i prodotti digitali:

- **Hardware**;
- **Software**;
- **Soluzioni di elaborazione di dati a distanza**.



Diverse categorie e rischi

Le nuove regole distinguono i prodotti con elementi digitali in **tre categorie**:

- **Prodotti di default,** prodotti non critici (e.g., smart speakers, giochi elettronici, smart TV, camere digitali) - soggetti a ***self assessment*** sui rischi di cybersecurity;
- **Prodotti critici di Classe I** (e.g., password managers, browsers, mobile device management software, firewalls, intrusion detection e intrusion prevention systems, IoT non rientranti in Class II) - richiedono l'applicazione di uno **standard/schemi di certificazione** o un ***assessment*** **da terze parti**;
- **Prodotti critici di Classe II** (e.g., sistemi operativi per server, desktop e dispositivi mobili, firewall industriali, smartcards, smart readers e contatori smart) - richiedono obbligatoriamente l'***assessment*** **di una terza parte**.

I principali obblighi

Il Cyber Resilience Act prevede diversi obblighi relativi alla **progettazione**, **sviluppo** e **produzione** di prodotti digitali, tra cui i seguenti:

- svolgere una **valutazione dei rischi** cyber (deve essere svolta **e continuativamente aggiornata**);
- nel caso d'inclusione di **componenti di terze parti**, verificare **che l'integrazione non comprometta la sicurezza del prodotto**;
- **assicurare che le eventuali vulnerabilità individuate saranno trattate** efficacemente per tutto il ciclo di vita del prodotto (o per 5 anni dal lancio sul mercato dello stesso, quale sia inferiore);
- adottare adeguate **policy** e **procedure** per **gestire e rimediare a potenziali vulnerabilità d**el prodotto;
- predisporre la necessaria **documentazione tecnica** contenente informazioni facilmente comprensibili inerenti la sicurezza cyber del prodotto (e.g. finalità, versione, processo di gestione delle vulnerabilità, valutazione dei rischi cyber, ecc.).

In caso di **incidenti di sicurezza**:

- notificare all'ENISA (European Union Agency for Cybersecurity) entro 24 ore da quando ha conoscenza;
- informare gli utenti dell'incidente e delle misure correttive da adottare per mitigare l'impatto.

Sanzioni

Il Cyber Resilience Act prevede **sanzioni rilevanti** in caso di non conformità con gli obblighi ivi previsti:

- per violazioni gravi: **fino a 15 milioni di euro** o **fino al 2,5% del fatturato annuo globale dell'anno precedente**, se superiore;
- per violazioni meno gravi: fino a **10 milioni di euro** o **fino al 2% del fatturato annuo globale dell'anno precedente**, se superiore.

Gli Stati membri saranno chiamati ad individuare un'**autorità** competente per assicurare l'efficace applicazione del regolamento.

L'interazione con il quadro normativo dell'Unione

Il Cyber Resilience Act si inserisce nell'ambito di un **framework normativo già strutturato** ma allo stesso tempo **in grande evoluzione**, che include:

- la Direttiva (UE) 2013/40 relativa agli **attacchi contro i sistemi di informazione**;
- la Direttiva (UE) 2016/1148 recante misure per un **livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione** (nota come **NIS**) e la proposta della Commissione europea di una nuova direttiva in materia, nota come **NIS2**;
- il Regolamento (UE) 2019/881 (**Cybersecurity Act**) relativo all'**ENISA** e alla **certificazione della cybersicurezza** per le tecnologie dell'informazione e della comunicazione;
- il quadro normativo derivante dalla Direttiva 2014/513 **RED** (*radio equipment directive*).

Il Cyber Resilience Act, inoltre, arricchisce anche il quadro normativo per la **strategia digitale europea** che include, tra gli altri:.

1) la **proposta di un Regolamento E-Privacy** (che andrà a sostituire la Direttiva 2002/58, la cd. E-Privacy Directive);

2) il Regolamento 2022/1925 (il **Digital Markets Act**);

3) il Regolamento (UE) 2022/868 (Data Governance Act), già in vigore;

4) la proposta di Regolamento nota con il nome di Data Act (in ambito perlopiù IOT).

La proposta del Cyber Resilience Act si interseca poi anche con l'altra proposta della Commissione europea di un Regolamento riguardante l'intelligenza artificiale (**AI Act**).

Il Cyber Resilience Act prevede un meccanismo di conformità anche all'AI Act dei sistemi ad alto rischio che sono ritenuti conformi ai requisiti del Cyber Resilience Act.

Approccio tecnico e legale alla compliance cyber

Le norme di futura introduzione richiedono agli operatori del settore digitale di adottare un **approccio** alla «**compliance cyber**» analogo a quello che deve essere seguito in ambito **data protection**. È richiesto, infatti, a chi produce, importa, distribuisce prodotti aventi componenti digitali, tra l'altro, anche di: verificare tutti i possibili rischi e adottare soluzioni adeguate per gestirli, svolgere assessment in accountability, assicurare la trasparenza, mantenere il controllo sulla catena di fornitura, gestire gli incidenti tempestivamente, ecc. Pertanto, in questo ambito, occorre costruire un **impianto organizzativo** che non può prescindere da **competenze legali** che integrino quelle **tecniche**.

Experience the future of law, today

Deloitte Legal affronta le tue sfide con un approccio multidisciplinare e una prospettiva globale, collegando le specifiche esigenze aziendali e utilizzando la tecnologia per sperimentare soluzioni innovative.

Make an impact that matters. Per lasciare un segno significativo è necessario un consulente esperto, che sia allo stesso tempo pragmatico e pioniere.

Deloitte Legal integra consulenza legale, strategia e tecnologia per sviluppare soluzioni innovative, creare valore per te e per il tuo business e trasformare il mondo dei servizi di consulenza legale.

The future of law is here, today.

Il nostro impegno concreto per un'evoluzione sostenibile

Key Contacts

Ida Palombella
Partner | ipalombella@deloitte.it

Pietro Boccaccini
Director | pboccaccini@deloitte.it

Simone Prelati | Federico Vota | Alessandro Amoroso | Camilla Torresan | Gulin Guney

Deloitte.
Legal