

Cyber Resilience Act (CRA) — règlement (UE) 2024/2847

Mise à jour le 29/10/2026

1. Nature et état du texte

Le Cyber Resilience Act est un RÈGLEMENT européen adopté, entré en vigueur le 10 décembre 2024. Il encadre la cybersécurité des produits comportant des éléments numériques mis sur le marché de l'Union européenne. Il ne s'agit pas d'une simple recommandation ni d'une norme ISO.

Les obligations principales de conception, de conformité et de surveillance s'appliqueront dans leur ensemble à partir du 11 décembre 2027. Il faut toutefois distinguer les obligations déjà applicables en 2026.

2. Calendrier à retenir

- Depuis le 11 juin 2026 : dispositions relatives à la notification des organismes chargés des évaluations de conformité.
- Depuis le 11 septembre 2026 : obligation de signaler certaines vulnérabilités activement exploitées et certains incidents graves.
- À compter du 11 décembre 2027 : application générale des exigences de cybersécurité, de conformité et de marquage CE dans les conditions du règlement.

3. Champ d'application

Produits matériels et logiciels ayant une connexion directe ou indirecte à un appareil ou à un réseau : équipements connectés, dispositifs IoT et logiciels commercialisés, sous réserve des exclusions prévues par le règlement et des législations sectorielles spécifiques.

Les fabricants portent des obligations centrales ; importateurs, distributeurs et certains responsables de logiciels libres (« open-source software stewards ») relèvent de dispositions adaptées. Ne pas présumer que chaque projet open source bénévole est soumis au même régime qu'un fabricant commercial.

4. Exigences techniques et organisationnelles

- Analyse des risques de cybersécurité et sécurité dès la conception et par défaut.
- Traitement des vulnérabilités pendant la période de support ; mises à jour de sécurité et information des utilisateurs.
- Documentation technique, évaluation de conformité et déclaration UE de conformité lorsque requises.
- Surveillance post-commercialisation et coordination avec les acteurs de la chaîne de distribution.

5. Déclaration des vulnérabilités et incidents : exigible en 2026

Depuis le 11 septembre 2026, les fabricants doivent notifier les vulnérabilités activement exploitées et les incidents graves ayant une incidence sur la sécurité de leurs produits. Une alerte précoce est transmise dans les 24 heures à compter de la connaissance, suivie d'une notification complète dans les 72 heures ; les rapports finaux suivent les échéances prévues par le règlement.

Le signalement s'effectue via la plateforme unique de déclaration (Single Reporting Platform) gérée par l'ENISA, à destination du CSIRT compétent. La règle « 24 heures » seule, sans évoquer le suivi à 72 heures ni le périmètre des signalements, est incomplète.

6. Démarche de conformité pour une organisation

1) Cartographier produits, composants et fournisseurs. 2) Qualifier les exclusions et dates d'application. 3) Documenter risques et mesures. 4) Organiser la gestion des vulnérabilités, les notifications et les preuves. 5) Préparer les évaluations de conformité et le marquage réglementaire selon les produits.

Sources institutionnelles

<https://digital-strategy.ec.europa.eu/fr/policies/cyber-resilience-act>

<https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

<https://eur-lex.europa.eu/eli/reg/2024/2847/oj>