

Cyber Resilience Act (CRA)

Règlement (UE) 2024/2847 du 23 octobre 2024

Source officielle :  [Texte complet sur EUR-Lex](#)

1) Objectifs

- Renforcer la **cybersécurité des produits comportant des éléments numériques** sur tout leur cycle de vie (de la conception au retrait du marché).
- Protéger les utilisateurs contre les **vulnérabilités exploitables**.
- Instaurer une **approche commune à l'échelle de l'UE** en matière de sécurité produit.
- **Responsabiliser** les fabricants, importateurs et distributeurs.

2) Principales dispositions

- **Cybersécurité dès la conception** : exigences techniques obligatoires (mise à jour, journalisation, chiffrement, durabilité...).
- **Notification obligatoire** des incidents et vulnérabilités exploitées dans les **24 heures** à l'ENISA et aux autorités nationales.
- **Évaluation de conformité** : autoévaluation pour les produits standards, ou recours à un organisme notifié pour les produits critiques.
- **Documentation technique et suivi des vulnérabilités** : maintenance, support, gestion des failles pendant toute la durée de vie.
- **Marquage CE** obligatoire fondé sur la cybersécurité.

3) Entreprises / organisations concernées

- **Fabricants** de produits matériels ou logiciels avec composant numérique,
- **Importateurs et distributeurs** dans le marché intérieur,
- **Fournisseurs de logiciels embarqués** ou à usage général,
- **PME et grandes entreprises** produisant des applications ou systèmes commercialisés dans l'UE.

Exclusions :

- Logiciels libres *sans finalité commerciale directe*,
- Produits exclusivement destinés à des usages de défense ou de sécurité nationale.

4) Sanctions en cas de non-respect

En cas de non-conformité aux exigences du CRA :

- **Amendes administratives** :
 - Jusqu'à **15 000 000 €** ou **2,5 % du chiffre d'affaires annuel mondial**, si plus élevé, pour infraction aux obligations essentielles de cybersécurité.

- Jusqu'à **10 000 000 €** ou **2 % du CA mondial** pour défaut de notification, documentation ou marquage CE.
- Jusqu'à **5 000 000 €** ou **1 % du CA mondial** pour d'autres manquements.
- **Mesures correctives :**
 - Ordre de **mise en conformité, retrait du marché** ou **rappel produit** par les autorités nationales (ex. : ANSSI en France).
 - **Suspension de la mise sur le marché** en cas de risque immédiat pour la sécurité.
- **Responsabilité accrue des dirigeants** en cas de négligence grave dans la gestion de la conformité CRA.