

DISPOSITIFS



Ordinateurs portables



Smartphones



Appareils mobiles



Appareils portables de surveillance de la santé



Routeurs



Produits pour maison intelligente



Passerelle de compteur intelligent



Cartes à puce

LOGICIEL



Systèmes de gestion des identités



Navigateurs



Gestionnaires de mots de passe



Système SIEM



Logiciel d'émission de certificats numériques



Micrologiciel



Système d'exploitation



Applications



Jeux vidéo



Pare-feu

Loi sur la cyber-résilience (CRA)

Qui

Opérateurs économiques : fabricants, distributeurs et importateurs

Hors champ d'application : logiciels/matériel fournis dans le cadre d'un service (c'est-à-dire non vendus séparément). Exemple : service cloud ou lecteur de carte fourni par votre banque.

Exigences en matière de cybersécurité

- 1 Les risques liés à la cybersécurité** sont documentés, régulièrement évalués, traités et communiqués
- 2 Exigences essentielles en matière de cybersécurité pour les phases de planification, de conception, de développement, de production, de livraison et de maintenance.** Sécurité de la chaîne d'approvisionnement et diligence raisonnable
- 3 Exigences en matière de gestion des vulnérabilités,** y compris mises à jour de sécurité pendant plus de 5 ans
- 4 Attestation et transparence:** informations claires sur les risques liés à la cybersécurité et instructions à l'intention de l'utilisateur, évaluation de la conformité, documentation technique, marquage CE
- 5 Signalement** des vulnérabilités activement exploitées et des incidents graves



Chronologie

10 Décembre
2024



entre en
vigueur

D'ici le 11
Septembre 2026



Commencez à
signaler les
vulnérabilités et
les incidents
activement
exploités.

D'ici au 11
Décembre 2027



date limite pour
mettre en
œuvre toutes
les autres
exigences

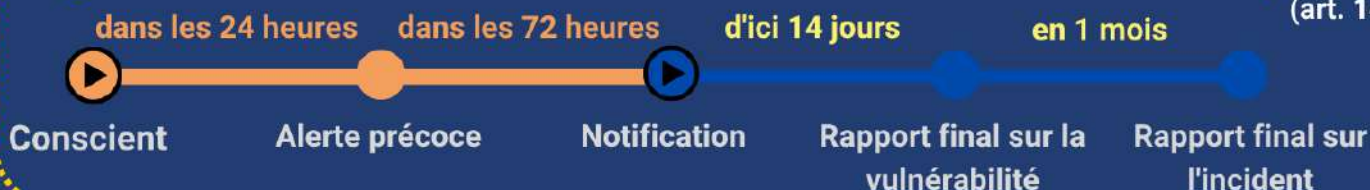


41 normes horizontales
spécifiques à des produits
adoptées par l'UE, 10 actes
délégués, 8 actes d'exécution
et 1 document d'orientation

Résultant en

Déclaration de conformité UE et peut
apposer le marquage CE

Signalement des vulnérabilités et incidents activement exploités (art. 14)



Sanctions (art. 64)

Non-respect des exigences essentielles :

- jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel

Informations incorrectes, incomplètes ou trompeuses :

- jusqu'à 5 millions d'euros ou 1 % du chiffre d'affaires annuel

Points d'attention

- Nouveau cadre législatif (comme la sécurité)
- Évaluation de la conformité par soi-même ou par un tiers
- Condition d'accès au marché de l'UE
- Responsabilité accrue en raison d'éventuelles poursuites civiles liées à des problèmes de conformité CE

Le projet financé dans le cadre de la convention de subvention n° 101190193 est soutenu par le Centre européen de compétence en matière de cybersécurité.



Co-funded by
the European Union



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



CONFIRMATE