_swissprivacy.law

Cyber Resilience Act : la cybersécurité des produits numériques

David Pressouyre, le 14 septembre 2026

Le règlement européen sur la cyberrésilience imposera de nouvelles exigences aux produits numériques commercialisés dans l'Union européenne. Si l'essentiel de ses dispositions s'appliquera à compter du 11 décembre 2027, certaines obligations de notification des vulnérabilités et des incidents entrent en vigueur dès le 11 septembre 2026.

Le règlement (UE) 2024/2847 du 23 octobre 2024 sur la cyberrésilience (« *Cyber Resilience Act* », « CRA ») établit des règles relatives à la mise sur le marché de produits comportant des éléments numériques afin de garantir leur cybersécurité. Il fixe des exigences en la matière concernant leur conception, leur développement et leur production, ainsi que des obligations à la charge des différents opérateurs économiques, principalement les fabricants (art. 13 ss CRA), mais également les importateurs (art. 19 CRA) et les distributeurs (art. 20 CRA).

Le CRA sera principalement applicable à compter du 11 décembre 2027 (art. 71 CRA). Mais certaines règles, en particulier les obligations de communication d'informations incombant aux fabricants selon l'art. 14 CRA, s'appliqueront toutefois dès le 11 septembre 2026.

Le 27 juillet 2026, la Commission européenne a publié des lignes directrices et des orientations pratiques, notamment à destination des PME, qui précisent le champ d'application du règlement, la détermination des périodes d'assistance, l'évaluation des risques ainsi que la notification des vulnérabilités et des incidents de cybersécurité.

Un champ d'application étendu

Le CRA s'applique aux « produits comportant des éléments numériques » mis à disposition sur le marché de l'Union européenne (UE) et dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau (art. 2 par. 1 CRA). Cette notion recouvre un produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels mis sur le marché séparément (art. 3 chif. 1 CRA).

Le règlement couvre ainsi une gamme très étendue de produits immatériels (logiciels autonomes, applications, systèmes d'exploitation, antivirus, etc.) et matériels (objets connectés,

machines industrielles, smartphones, appareils électroménagers, etc.). Il a également une portée extraterritoriale, puisqu'il peut s'appliquer aux fabricants établis hors de l'UE qui commercialisent des produits au sein d'un ou plusieurs États membres.

Certains produits, relevant par exemple d'une réglementation particulière de l'UE, sont cependant exclus du dispositif. C'est notamment le cas des dispositifs médicaux, des véhicules à moteur, de certains produits de l'aviation civile, des équipements marins, de certaines pièces de rechange, ainsi que de certains produits développés ou modifiés exclusivement à des fins de sécurité nationale ou de défense et de ceux conçus pour traiter des informations classifiées (art. 2 par. 2 à 7 CRA).

Principales obligations du fabricant

Le fabricant doit s'assurer que le produit satisfait aux exigences essentielles de cybersécurité visées à l'annexe I, partie I, CRA et mettre en place des processus de gestion des vulnérabilités conformes à l'annexe I, partie II CRA (art. 6 et art. 13 par. 1 CRA). Le produit doit ainsi être conçu, développé et fabriqué selon un niveau de cybersécurité adapté aux risques. Le fabricant procède notamment à une évaluation des risques avant la mise sur le marché, écarte les vulnérabilités exploitables connues, prévoit une configuration sécurisée par défaut, des mises à jour régulières et des mécanismes appropriés de contrôle d'accès. Il doit également garantir la minimisation, la disponibilité, l'intégrité et la confidentialité des données stockées.

L'évaluation des risques est documentée, actualisée et intégrée à la documentation technique (art. 13 par. 2 et 3, art. 31 CRA). Avant la mise sur le marché, le fabricant applique la procédure d'évaluation de la conformité appropriée, établit la déclaration UE de conformité et appose le marquage CE (art. 13 par. 12, art. 27 ss CRA).

Le CRA prévoit également des obligations renforcées pour certains produits particulièrement exposés, dits « importants » ou « critiques ». Les produits « importants » de l'annexe III CRA (e.g. : systèmes de gestion des identités et des accès, navigateurs, gestionnaires de mots de passe, VPN, systèmes d'exploitation, jouets connectés, produits domotiques, etc.) sont ainsi soumis à des exigences et procédures spécifiques. Certains produits « critiques » de l'annexe IV CRA (e.g. dispositifs matériels avec boîtier de sécurité, passerelles pour compteur intelligent, cartes à puces, etc.) devront obtenir un certificat européen de cybersécurité au niveau d'assurance au moins « substantiel ».

Les obligations se prolongent après la commercialisation du produit. Pendant la période

d'assistance, fixée en fonction de la durée d'utilisation du produit, et en principe pour une durée d'au moins cinq ans, le fabricant recense, documente, traite et corrige sans retard les vulnérabilités, teste régulièrement le produit et organise leur divulgation coordonnée. Il accompagne le produit des informations et instructions prévues à l'annexe II CRA, désigne un point de contact unique et maintient des procédures internes assurant la conformité. Il coopère enfin avec les autorités de surveillance et prend, si nécessaire, les mesures correctives, de retrait ou de rappel.

Notification des vulnérabilités et des incidents graves

Le fabricant notifie les vulnérabilités ou incidents graves dont il prend connaissance au centre de réponse aux incidents de sécurité informatique (« CSIRT ») désigné comme coordinateur national et à l'Agence européenne pour la cybersécurité (« ENISA »), par l'intermédiaire de la plateforme unique de signalement (art. 14 par. 1 et 3 CRA). Une alerte précoce intervient au plus tard dans les 24 heures suivant la prise de connaissance de la vulnérabilité, la notification complète dans les 72 heures, puis le rapport final au plus tard 14 jours après la mise à disposition d'une mesure de correction ou d'atténuation (art. 14 par. 2 et 4 CRA).

Ces obligations seront applicables dès le 11 septembre 2026 à tous les produits comportant des éléments numériques relevant du champ d'application du CRA, y compris ceux mis sur le marché avant le 11 décembre 2027 (art. 69 par. 3 CRA).

Importateurs et distributeurs

L'importateur ne met sur le marché que des produits conformes aux exigences essentielles et vérifie notamment que le fabricant a réalisé l'évaluation de la conformité, établi la documentation technique et la déclaration UE de conformité, apposé le marquage CE et fourni les informations requises. Le distributeur est soumis à une obligation générale de diligence. Il contrôle la conformité avant la mise à disposition, s'abstient de commercialiser un produit non conforme et veille ensuite aux mesures de mise en conformité, de retrait ou de rappel. Les importateurs et les distributeurs doivent également signaler les risques ou vulnérabilités pertinents et coopérer avec les autorités (art. 19 et art. 20 CRA).

Sanctions

Les États membres devront préciser le régime des sanctions. Le non-respect des exigences essentielles de cybersécurité visées à l'annexe I CRA ou des principales obligations des fabri-

cants peut toutefois entraîner une amende allant jusqu'à EUR 15'000'000.- ou, pour une entreprise, 2,5 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 64 par. 2 CRA).

Pour les autres obligations, notamment celles des importateurs et des distributeurs, ainsi que certaines obligations en matière de processus de certification CE, le plafond est fixé à EUR 10'000'000.- ou à 2 % du chiffre d'affaires (art. 64 par. 3 CRA).

Enfin, la fourniture d'informations inexactes, incomplètes ou trompeuses peut être sanctionnée jusqu'à EUR 5'000'000.- ou 1 % du chiffre d'affaires annuel mondial total (art. 64 par. 4 CRA).

Et en Suisse ?

À ce jour, la Suisse ne dispose pas d'une législation comparable au CRA en matière de cyber-résilience des produits. Le 20 août 2025, le Conseil fédéral a toutefois chargé le DDPS, en collaboration avec le DETEC et le DEFR, de préparer un projet législatif destiné à être mis en consultation. Un projet de loi est attendu à l'automne 2026. Dans l'intervalle, des exigences de cybersécurité peuvent notamment, selon les cas, découler indirectement des règles suisses relatives à la protection des données personnelles (LPD, OPDo et OCPD), à la sécurité de l'information (LSI et OSI) ou à certains produits, notamment dans le domaine des télécommunications (LTC et OIT).

L'absence de réglementation suisse équivalente ne signifie toutefois pas que les entreprises suisses échappent au CRA. Celui-ci s'applique également aux entreprises établies hors de l'UE lorsqu'elles y commercialisent des produits numériques. Une entreprise suisse qui vend un logiciel ou un appareil connecté sur le territoire d'un état membre peut donc être concernée. Si c'est le cas, elle doit être en mesure de notifier les vulnérabilités et les incidents graves dès le 11 septembre 2026. Elle doit également préparer la mise en conformité de ses produits avec les exigences de cybersécurité nécessaires à l'apposition du marquage CE d'ici au 11 décembre 2027.

Proposition de citation : David Pressouyre, Cyber Resilience Act : la cybersécurité des produits numériques, 14 septembre 2026 *in* www.swissprivacy.law/418

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.