BCLP. Client Intelligent

Insights

RÉFLEXION SUR LE NOUVEAU RÈGLEMENT SUR LA CYBER RÉSILIENCE DE L'UNION EUROPÉENNE

CE QUE LES ENTREPRISES DOIVENT SAVOIR

Nov 25, 2024

SUMMARY

Le règlement européen 2024/2847 sur la cyber résilience *(« CRA »)* est un texte législatif novateur destiné à renforcer la cybersécurité des produits et services numériques mis à disposition dans l'Union européenne. Entrant en vigueur le 10 décembre 2024, il marque le début d'une période de mise en œuvre progressive de trois ans. Le CRA vise à renforcer la résilience de l'économie numérique de l'UE en imposant des exigences plus strictes aux fabricants, importateurs et distributeurs de produits ou de logiciels ayant une composante numérique. Il aura à cet égard des conséquences importantes en matière de conformité pour de nombreuses entreprises.

QUI SERA CONCERNÉ ?

- Les fabricants ;
- les importateurs ; et
- les distributeurs de produits comportant un « élément numérique » dont l'utilisation nécessite une connexion numérique ou physique, directe ou indirecte, à un appareil ou à un réseau.

Le CRA définit un « *produit comportant un élément numérique* » comme un logiciel ou un matériel (ou un produit combinant les deux). Cette définition couvre de nombreux produits que nous utilisons tous dans notre vie quotidienne (des montres intelligentes aux assistants numériques en passant par les babyphones).

QUEL EST LE CHAMP D'APPLICATION TERRITORIAL DU CRA ?

Ce règlement s'applique aux fabricants, importateurs et distributeurs de produits et de services établis dans l'Union européenne.

Il est important de noter que, comme de nombreux règlements européens récemment adoptés, il a également un effet extraterritorial : tous les fabricants, qu'ils soient basés dans l'UE ou non, devront se conformer aux exigences du CRA pour pouvoir commercialiser leurs produits ou services sur le marché européen.

QUELLES MESURES LES ENTREPRISES DOIVENT-ELLES PRENDRE POUR SE CONFORMER AU CRA ?

Les obligations varient en fonction du rôle occupé par l'entreprise dans la chaîne d'approvisionnement des produits.

OBLIGATIONS DES FABRICANTS

Le CRA définit deux séries d'exigences pour les fabricants de produits comportant un composant numérique. Pour les exigences concernant les **propriétés du produit**, le fabricant doit :

- effectuer une évaluation des risques induits par le produit, qui doit être documentée et mise à jour afin de minimiser le risque cyber au stade du développement et pendant la maintenance du produit ;
- se conformer aux exigences essentielles de cybersécurité énoncées à l'annexe 1 du CRA et rédiger une déclaration de conformité pour le certifier ;
- fournir aux utilisateurs des informations concernant : (i) l'identification du produit (numéro de lot ou de série) ; (ii) les coordonnées du fabricant ; et (iii) la date de fin de toute période d'assistance ; et
- apposer sur le produit un marquage CE et un pictogramme ou un autre marquage indiquant le risque cyber, afin de permettre aux utilisateurs de faire un choix éclairé.

En ce qui concerne la **gestion des vulnérabilités**, le fabricant doit :

- corriger les vulnérabilités pendant une période d'au moins 5 ans à compter de la date de mise sur le marché du produit ; et
- notifier, par l'intermédiaire d'une plateforme de notification spécifiquement établie, le Centre de réponse aux incidents de sécurité informatique (CSIRT ou « *Computer Security Incident Response Team* ») compétent et l'Agence européenne de cybersécurité (ENISA) toute vulnérabilité effectivement exploitée dès qu'elle est découverte, d'abord sous la forme d'une alerte, puis sous la forme d'un rapport. La notification par le fabricant doit être faite rapidement :

- une notification d'alerte doit être émise sans délai excessif et, en tout état de cause, **dans les 24 heures** suivant la découverte de la vulnérabilité ;
- une notification de vulnérabilité doit ensuite être émise **dans les 72 heures** suivant la prise de connaissance de la vulnérabilité (en fournissant des informations sur la nature de l'incident ainsi que sur les mesures correctives ou d'atténuation prises ou que les utilisateurs peuvent prendre) ;
- enfin, le fabricant doit publier un rapport final énumérant les mesures correctives prises et les informations concernant tout acteur malveillant qui a exploité ou qui exploite la vulnérabilité, **au plus tard 14 jours** après qu'une mesure corrective ou d'atténuation est disponible.

OBLIGATIONS DES IMPORTATEURS

Les importateurs doivent vérifier, avant de mettre le produit sur le marché, que celui-ci est conforme aux exigences essentielles de cybersécurité imposées par le CRA et que le fabricant a mis en place des processus de gestion des vulnérabilités suffisant. Il doit également : (i) obtenir du fabricant un ensemble de documents attestant du respect des exigences fixées par le CRA et (ii) faire figurer ses coordonnées sur le produit, sur son emballage ou dans un document accompagnant le produit.

OBLIGATIONS DES DISTRIBUTEURS

Les distributeurs doivent vérifier que le produit porte le marquage CE et que le fabricant et l'importateur ont respecté leurs obligations respectives au titre du CRA.

S'il existe un risque qu'un produit ne soit pas conforme aux exigences du règlement CRA, les importateurs et les distributeurs ne doivent pas mettre le produit sur le marché de l'UE et doivent en informer, dans les meilleurs délais, le fabricant du produit et les autorités compétentes en matière de surveillance du marché des États membres dans lesquels ils ont mis le produit à disposition.

Il est important de noter qu'un importateur ou un distributeur sera également considéré comme un fabricant (aux fins d'application du CRA) lorsqu'il met sur le marché un produit contenant des éléments numériques sous son nom ou sa marque ou lorsqu'il apporte une modification substantielle à un produit déjà mis sur le marché.

QUELLES SONT LES AUTORITÉS CHARGÉES DE L'APPLICATION DU CRA ?

- Un CSIRT désigné par chaque État membre coordonnera les divulgations de vulnérabilités. Il facilitera, si nécessaire, l'interaction entre la personne signalant une vulnérabilité et le fabricant ou le fournisseur des produits ou services potentiellement vulnérables. Il recevra également toute notification d'incident grave ayant un impact sur la sécurité d'un produit contenant des éléments numériques.
- L'ENISA est l'autorité compétente, au niveau de l'UE, pour recevoir les notifications d'incidents graves ayant un impact sur la sécurité d'un produit contenant des éléments numériques.
- Les États membres désigneront également des autorités de surveillance du marché chargées de contrôler les ventes de produits dans chaque État membre. Cette autorité peut demander aux opérateurs de prendre toutes les mesures correctives appropriées pour mettre le produit en conformité, le retirer du marché ou le rappeler dans un délai raisonnable.

QUELLES SONT LES SANCTIONS PRÉVUES PAR LE CRA ?

Les entreprises qui ne se conforment pas au CRA s'exposent à des amendes très importantes :

- Les fabricants peuvent se voir infliger une amende allant jusqu'à 15.000.000 € ou 2,5 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).
- Les importateurs et les distributeurs peuvent se voir infliger des amendes allant jusqu'à 10.000.000 € ou 2 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).
- Des amendes allant jusqu'à 5.000.000 € ou 1 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu) peuvent sanctionner la fourniture d'informations inexactes aux organismes d'évaluation de la conformité et/ou aux autorités de contrôle.

LES PROCHAINES ÉTAPES DE MISE EN ŒUVRE DU CRA

Le règlement CRA entrera en vigueur le 10 décembre 2024 et s'appliquera 36 mois après son entrée en vigueur, soit le **11 décembre 2027**. Certaines dispositions s'appliqueront néanmoins plus tôt, notamment l'obligation du fabricant de signaler toute vulnérabilité activement exploitée qui s'appliquera 21 mois après l'entrée en vigueur de l'ARC, soit le **11 septembre 2026**.

RELATED CAPABILITIES

- Data Privacy & Security
- Technology Transactions

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
