BCLP. Client Intelligent

Insights

LE RÈGLEMENT SUR LA CYBER-RÉSILIENCE REDÉFINIT LES RÈGLES EN MATIÈRE DE SÉCURITÉ DES PRODUITS NUMÉRIQUES

Nov 07, 2025

Le Règlement sur la cyber-résilience (règlement (UE) 2024/2847 ou *« CRA »*) (ci-après « Règlement ») établit des exigences obligatoires en matière de cybersécurité pour les produits comportant des éléments numériques, qu'il s'agisse de matériel ou de logiciels connectés au réseau internet ou traitant des données, dans le but de créer un écosystème de produits plus sûr, transparent et réactif pour le marché européen.

Au cœur du Règlement se trouve la mise en place d'une chaîne de responsabilité en cascade tout au long du cycle de vie du produit, dans laquelle les fabricants assurent les obligations principales, tandis que les importateurs et les distributeurs assurent des obligations secondaires, notamment la vérification de la conformité et la notification des vulnérabilités et incidents aux autorités compétentes. Les fabricants doivent intégrer la cybersécurité dès la phase de conception, en garantissant une sécurité continue durant la production, la mise sur le marché et après la commercialisation du produit.

Ces exigences ont suscité des inquiétudes importantes auprès des opérateurs économiques de différentes tailles en ce qui concerne la complexité de la mise en œuvre et les ressources nécessaires. Néanmoins, les fabricants doivent repenser fondamentalement leurs processus de développement, de production et de service après-vente afin de garantir la conformité avec le Règlement pour tous les produits mis sur le marché européen.

QUELLES ENTITÉS SONT CONCERNÉES ?

Le Règlement s'applique aux opérateurs économiques impliqués dans la conception, le développement, la fabrication et la distribution de produits comportant des éléments numériques. Son champ d'application comprend :

1. **Les fabricants** : les entités qui développent ou fabriquent des produits comportant des éléments numériques. Cela englobe les fabricants de :

- Produits matériels comportant des éléments numériques (par exemple, appareils IoT, routeurs, appareils intelligents, équipements industriels connectés),
- Des produits logiciels, y compris les logiciels autonomes et les micrologiciels,
- Solutions de traitement de données à distance (par exemple, applications fondées sur le cloud, services web, applications mobiles).

2. **Importateurs**
3. **Distributeurs**
4. **Fournisseurs de solutions de traitement de données à distance** : entités proposant des produits logiciels permettant le traitement de données à distance, notamment :
   - Plateformes *SaaS (Software-as-a-Service)*,
   - Les applications et services fondés sur le cloud,
   - Solutions logicielles fondées sur le Web,
   - Les applications mobiles avec traitement en arrière-plan.

Le Règlement s'applique quel que soit le lieu d'établissement du fabricant ou de tout autre opérateur économique, à condition que les produits comportant des éléments numériques soient mis sur le marché de l'UE ou mis en service au sein de l'UE. Cette application extraterritoriale garantit que tous les produits disponibles pour les consommateurs et les entreprises de l'UE répondent aux normes de cybersécurité du Règlement, quelle que soit leur origine.

QUELLES SONT LES PRINCIPALES OBLIGATIONS DES FABRICANTS DE PRODUITS ?

En vertu du Règlement, les fabricants sont les premiers responsables de la conformité des produits comportant des éléments numériques aux exigences essentielles en matière de cybersécurité tout au long de leur cycle de vie. Ces obligations comprennent :

SÉCURITÉ DÈS LA CONCEPTION ET PAR DÉFAUT

Les fabricants doivent veiller à ce que les produits comportant des éléments numériques soient conçus, développés et fabriqués conformément aux exigences essentielles en matière de cybersécurité énoncées dans le Règlement.

ÉVALUATION DES RISQUES ET DOCUMENTATION TECHNIQUE

Les fabricants doivent procéder à des évaluations complètes des risques liés à la cybersécurité afin d'identifier les risques potentiels tout au long du cycle de vie du produit et mettre en œuvre des mesures d'atténuation appropriées.

PROCÉDURES D'ÉVALUATION DE LA CONFORMITÉ

En fonction de la classification du produit, les fabricants doivent se soumettre à des procédures d'évaluation de conformité appropriées afin de garantir le respect des exigences en matière de cybersécurité énoncées dans le Règlement.

ASSISTANCE ET MISES À JOUR EN MATIÈRE DE SÉCURITÉ

Les fabricants doivent fournir des mises à jour de sécurité pour les produits pendant au moins cinq ans à compter de la date de commercialisation du produit, ou durant toute la durée de vie prévue du produit si celle-ci est plus courte.

INFORMATIONS DESTINÉES AUX UTILISATEURS

Les fabricants doivent fournir aux utilisateurs des instructions claires et complètes ainsi que des informations relatives à la sécurité.

MARQUAGE CE ET DÉCLARATION DE CONFORMITÉ

Les fabricants doivent apposer le marquage « *CE* » sur les produits conformes avant de les mettre sur le marché.

GESTION DES VULNÉRABILITÉS ET SIGNALEMENT DES INCIDENTS

Les fabricants doivent mettre en place et maintenir des processus permettant d'identifier, de traiter et de signaler les vulnérabilités et les incidents.

TENUE DES REGISTRES

Les fabricants doivent conserver les registres des non-conformités, des vulnérabilités et des incidents pendant dix ans après la mise sur le marché du produit, et les mettre à la disposition des autorités de surveillance du marché sur demande.

OBLIGATION DE PRENDRE DES MESURES CORRECTIVES

Lorsque les fabricants ont des raisons de croire que les produits qu'ils ont mis sur le marché ne sont pas conformes au Règlement, ils doivent immédiatement prendre des mesures correctives pour mettre le produit en conformité, le retirer ou le rappeler.

OBLIGATIONS DES AUTRES OPÉRATEURS ÉCONOMIQUES

Les importateurs et les distributeurs ont des obligations similaires en matière de vérification et de surveillance du marché, bien que les importateurs aient des responsabilités plus étendues. Tous deux doivent vérifier la conformité du produit avant sa mise à disposition sur le marché, agir en cas de non-conformité en refusant l'accès au marché ainsi que coopérer avec les autorités en fournissant des documents sur demande et signaler les vulnérabilités au fabricant.

Le Règlement est directement applicable dans tous les États membres, son application étant déléguée aux autorités nationales de surveillance du marché.

Chaque État membre doit établir des sanctions efficaces, proportionnées et dissuasives en cas d'infraction, avec des amendes maximales pouvant atteindre 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial total de l'entreprise pour l'exercice financier précédent. Le montant le plus élevé est retenu dans ce cas.

Le non-respect de ces dispositions peut entraîner des ordonnances de retrait de produits, l'interdiction de mise sur le marché, des sanctions financières et une atteinte à la réputation, notamment lorsque les vulnérabilités entraînent des incidents de sécurité affectant les utilisateurs ou les infrastructures critiques.

DEVEZ-VOUS VOUS PRÉPARER À DES OBLIGATIONS DE DÉCLARATION ANTICIPÉE ?

Les fabricants sont soumis à des obligations de notification des vulnérabilités et des incidents qui sont exigibles avant l'entrée en vigueur du Règlement.

Alors que les dispositions substantielles du Règlement entreront en vigueur le 11 décembre 2027, les obligations de notification s'appliqueront à partir du 11 septembre 2026, soit plus d'un an plus tôt, ce qui oblige les fabricants à mettre en place des processus conformes dès maintenant. Les obligations de notification s'appliqueront à tous les produits numériques régis par le Règlement, quelle que soit la date à laquelle ils ont été mis sur le marché de l'Union.

Le Règlement établit un cadre de notification en trois étapes conçu pour permettre à l'*ENISA (European Union Agency for Cybersecurity)* et aux *CSIRT* (*Computer Security Incident Response Teams*) nationaux de surveiller les menaces émergentes en matière de cybersécurité et de

coordonner des réponses rapides aux vulnérabilités activement exploitées ainsi qu'aux incidents graves. Le cadre impose des délais stricts que les fabricants doivent respecter.

QUEL EST LE CALENDRIER DE MISE EN CONFORMITÉ ?

Le Règlement est entrée en vigueur le 10 décembre 2024, mais ses dispositions de fond deviennent applicables progressivement afin de laisser aux fabricants et aux opérateurs économiques suffisamment de temps pour adapter leurs processus et leurs produits.

Le Règlement établit le calendrier de conformité suivant :

- **11 septembre 2026** : les obligations de notification des vulnérabilités et des incidents deviennent applicables aux fabricants de produits comportant des éléments numériques déjà mis sur le marché, ce qui nécessite une préparation opérationnelle immédiate pour le cadre de notification en trois étapes.
- **11 décembre 2027** : les dispositions générales du Règlement deviennent pleinement applicables.

Les produits légalement mis sur le marché avant le 11 décembre 2027 ne sont pas rétroactivement soumis aux obligations du Règlement. Toutefois, si ces produits subissent une modification substantielle après cette date, ils doivent être conformes au Règlement, et la personne apportant les modifications assume le rôle de fabricant du produit modifié.

QUELLES MESURES DEVEZ-VOUS PRENDRE DÈS À PRÉSENT ?

Les obligations de déclaration prévues par le Règlement entrant en vigueur le 11 septembre 2026 et devenant pleinement applicables le 11 décembre 2027, les fabricants de produits comportant des éléments numériques doivent agir rapidement pour aligner leurs opérations, leurs infrastructures techniques et leurs accords contractuels. Les mesures suivantes sont essentielles pour garantir la conformité et atténuer les risques juridiques et commerciaux :

- **Évaluation et classification des produits**
- **Préparation de l'évaluation de la conformité**
- **Rédaction de la documentation obligatoire**
- **Définition de la période de support de sécurité**
- **Mise en œuvre d'un processus de gestion des vulnérabilités**
- **Révision et réécriture des contrats avec les clients et les tiers**
- **Suivi de la publication des normes harmonisées de l'UE**

COMMENT POUVONS-NOUS VOUS AIDER ?

L'équipe de BCLP est en mesure d'aider votre organisation à naviguer dans le paysage réglementaire introduit par le Règlement sur la cyber-résilience.

Nous vous aidons à identifier les produits comportant les éléments numériques concernés par le Règlement grâce à des analyses complètes de vos catalogues.

Nous évaluons la classification des produits afin de déterminer les procédures d'évaluation de conformité applicables et vous aidons à préparer la documentation technique ainsi que les déclarations de conformité européennes nécessaires.

Nos conseils s'étendent à la sélection et à la mise en œuvre de voies d'évaluation de la conformité appropriées, y compris la collaboration avec les organismes notifiés, l'application de normes harmonisées et l'évaluation des systèmes européens de certification en matière de cybersécurité tels que l'EUCC *(EU Common Criteria Certification)*.

Afin de garantir une conformité à long terme, nous proposons un suivi juridique continu des actes délégués, des mesures d'exécution et des normes harmonisées au fur et à mesure de leur adoption. Nous organisons des sessions de formation sur mesure à l'intention des équipes juridiques, techniques et de développement de produits internes, afin de leur permettre de rester informées et préparées.

En répondant de manière proactive à ces obligations, les fabricants atténuent non seulement les risques juridiques et évitent des sanctions importantes, mais renforcent également leur position concurrentielle sur un marché de plus en plus soucieux de la sécurité, en renforçant la confiance des clients grâce à un engagement démontrable en matière de cybersécurité.

RELATED CAPABILITIES

- Fintech
- Data Privacy & Security
- Intellectual Property & Technology Disputes

MEET THE TEAM

Pierre-Emmanuel Froge

Counsel, Paris

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