COM(2022) 454 final

ASSEMBLÉE NATIONALE **SÉNAT**

Reçu à la Présidence de l'Assemblée nationale
le 25 octobre 2022

Enregistré à la Présidence du Sénat
le 25 octobre 2022

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

E17180

Conseil de
l'Union européenne

Bruxelles, le 16 septembre 2022
(OR. en)

12429/22

Dossier interinstitutionnel:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	15 septembre 2022
Destinataire:	Secrétariat général du Conseil
N° doc. Cion:	COM(2022) 454 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

Les délégations trouveront ci-joint le document COM(2022) 454 final.

p.j.: COM(2022) 454 final

COMMISSION
EUROPÉENNE

Bruxelles, le 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

(Texte présentant de l'intérêt pour l'EEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Les produits matériels et logiciels font de plus en plus l'objet de cyberattaques qui atteignent leur but, ce qui s'est traduit, en 2021, par un coût annuel mondial de la cybercriminalité estimé à 5 500 milliards d'EUR. Ces produits présentent deux problèmes majeurs qui représentent des coûts supplémentaires pour les utilisateurs et la société: 1) le niveau de cybersécurité des produits comportant des éléments numériques est faible, comme en témoignent les vulnérabilités généralisées et le manque de mises à jour de sécurité déployées de manière cohérente pour y remédier, et 2) les utilisateurs n'ont pas suffisamment accès aux informations et ne les comprennent pas bien, ce qui les empêche de choisir des produits dotés de propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée. Dans un environnement connecté, le moindre incident de cybersécurité dans un produit peut affecter toute une organisation ou toute une chaîne d'approvisionnement, en se propageant souvent au-delà des frontières du marché intérieur en quelques minutes à peine. Cela peut occasionner de graves perturbations des activités économiques et sociales, voire mettre des vies en danger.

La cybersécurité des produits comportant des éléments numériques revêt une forte dimension transfrontière, étant donné que les produits fabriqués dans un pays sont souvent utilisés dans l'ensemble du marché intérieur. En outre, les incidents affectant initialement une seule entité ou un seul État membre se propagent souvent en quelques minutes à l'ensemble du marché intérieur.

Si la législation en vigueur dans le marché intérieur s'applique à certains produits comportant des éléments numériques, la cybersécurité de la plupart des produits matériels et logiciels n'est actuellement couverte par aucune législation de l'Union. Plus particulièrement, le cadre juridique actuel de l'UE ne traite pas de la cybersécurité des logiciels non intégrés, même si les attaques de cybersécurité ciblent de plus en plus les vulnérabilités de ces produits, ce qui entraîne des coûts sociétaux et économiques importants. Il existe de nombreux exemples de cyberattaques notables résultant d'une sécurité de produit perfectible, tels que le ver rançongiciel WannaCry, qui exploitait une vulnérabilité de Windows et qui, en 2017, a touché 200 000 ordinateurs dans 150 pays et causé des dommages s'élevant à plusieurs milliards de dollars américains; l'attaque de la chaîne d'approvisionnement Kaseya VSA, qui a ciblé plus de 1 000 entreprises via le logiciel d'administration de réseau de Kaseya et a forcé une chaîne de supermarchés suédoise à fermer l'ensemble de ses 500 magasins dans le pays; ou les nombreux incidents dans lesquels des applications bancaires sont piratées pour voler de l'argent à des consommateurs qui ne se doutent de rien.

Deux objectifs principaux ont été recensés en vue de garantir le bon fonctionnement du marché intérieur: 1) créer les conditions nécessaires au développement de produits comportant des éléments numériques sécurisés, en veillant à ce que les produits matériels et logiciels mis sur le marché présentent moins de vulnérabilités et à ce que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit; et 2) créer des conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques. Quatre objectifs spécifiques ont été définis: i) faire en sorte que les fabricants améliorent la sécurité des produits comportant des éléments numériques dès la phase de conception et de développement et tout au long du cycle de vie; ii) assurer un cadre cohérent en matière de cybersécurité, en facilitant la mise en conformité pour les producteurs de matériel et de logiciels; iii) améliorer la transparence des

propriétés de sécurité des produits comportant des éléments numériques; et iv) permettre aux entreprises et aux consommateurs d'utiliser les produits comportant des éléments numériques en toute sécurité.

La nature fortement transfrontière de la cybersécurité et le nombre croissant d'incidents ayant des répercussions transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs ne peuvent pas être atteints efficacement par les seuls États membres. Compte tenu du caractère mondial des marchés de produits comportant des éléments numériques, les États membres sont confrontés, sur leur territoire, aux mêmes risques pour un même produit. L'apparition d'un cadre fragmenté de règles nationales potentiellement divergentes risque d'entraver la création d'un marché unique ouvert et concurrentiel pour les produits comportant des éléments numériques. Une action commune au niveau de l'UE est donc nécessaire pour accroître le niveau de confiance parmi les utilisateurs et renforcer l'attractivité des produits européens comportant des éléments numériques. Cela profiterait également au marché intérieur en créant une sécurité juridique et en instaurant des conditions de concurrence équitables pour les fournisseurs de produits comportant des éléments numériques, comme le souligne également le rapport final de la conférence sur l'avenir de l'Europe, dans lequel les citoyens appellent à un renforcement du rôle de l'UE dans la lutte contre les menaces en matière de cybersécurité.

- **Interaction avec les dispositions existantes dans le domaine d'action**

Le cadre de l'UE comprend plusieurs actes législatifs horizontaux qui couvrent certains aspects liés à la cybersécurité sous différents angles (produits, services, gestion des crises et criminalité). La directive relative aux attaques contre les systèmes d'information[1], qui visait à harmoniser la criminalisation et les sanctions applicables à un certain nombre d'infractions dirigées contre les systèmes d'information, est entrée en vigueur en 2013. En août 2016, la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (directive SRI)[2] est entrée en vigueur. Il s'agissait du premier acte législatif adopté à l'échelle de l'Union européenne dans le domaine de la cybersécurité. Sa révision, qui a abouti à la directive [directive XXX/XXXX (SRI 2)], relève le niveau commun d'ambition de l'UE. Le règlement de l'Union sur la cybersécurité[3], entré en vigueur en 2019, vise à renforcer la sécurité des produits, services et processus TIC en introduisant un cadre européen volontaire de certification en matière de cybersécurité[4].

La cybersécurité de l'ensemble de la chaîne d'approvisionnement n'est assurée que si tous ses éléments sont protégés contre les cybermenaces. La législation de l'UE susmentionnée

---

1 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

2 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194/1 du 19.7.2016, p. 1).

3 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

4 Le règlement sur la cybersécurité permet le développement de schémas de certification spécifiques. Chaque schéma comprend des références aux normes pertinentes, spécifications techniques ou autres exigences en matière de cybersécurité définies dans le schéma. La décision d'élaborer une certification de cybersécurité est fondée sur le risque.

présente toutefois des lacunes importantes à cet égard, car elle ne prévoit pas d'exigences contraignantes en matière de sécurité des produits comportant des éléments numériques.

Si la proposition de législation sur la cyberrésilience couvre les produits comportant des éléments numériques mis sur le marché, la directive [directive XXX/XXX (SRI 2)] vise à assurer un niveau élevé de cybersécurité des services fournis par des entités essentielles et importantes. La directive [directive XXX/XXXX (SRI 2)] exige des États membres qu'ils veillent à ce que les entités essentielles et importantes relevant du champ d'application, telles que les prestataires de soins de santé ou de services en nuage et les entités de l'administration publique, prennent des mesures de cybersécurité techniques, opérationnelles et organisationnelles appropriées et proportionnées. Parmi celles-ci figure notamment une exigence visant à assurer la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités. La directive [directive XXX/XXXX (SRI 2)] impose à la Commission d'adopter des actes d'exécution établissant les exigences techniques et méthodologiques de ces mesures dans un délai de 21 mois à compter de la date d'entrée en vigueur de cette directive pour certains types d'entités, telles que les fournisseurs de services d'informatique en nuage. Pour toutes les autres entités, la Commission peut adopter un acte d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles. Ce cadre garantira que des spécifications techniques et des mesures similaires aux exigences essentielles de cybersécurité de la législation sur la cyberrésilience sont également mises en œuvre pour la conception, le développement et le traitement des vulnérabilités des logiciels fournis en tant que service (Software-as-a-Service). Par exemple, cela pourrait être un moyen d'assurer un niveau élevé de cybersécurité dans des cas tels que celui des systèmes médicaux électroniques (DME), y compris lorsque ceux-ci sont fournis sous la forme de logiciel en tant que service (SaaS) ou développés au sein des établissements de santé (en interne), conformément à la proposition de [règlement sur l'Espace européen des données de santé].

- **Interaction avec les autres politiques de l'Union**

Comme indiqué dans la communication intitulée «Façonner l'avenir numérique de l'Europe»[5], il est essentiel que l'UE exploite pleinement les avantages de l'ère numérique et renforce sa capacité industrielle et d'innovation dans les limites imposées par la sécurité et les valeurs éthiques. La stratégie européenne pour les données définit quatre piliers – la protection des données, les droits fondamentaux, la sûreté et la cybersécurité – comme des conditions préalables essentielles pour une société à laquelle les données confèrent les moyens dont elle a besoin.

Le cadre actuel de l'UE[6] applicable aux produits susceptibles de comporter des éléments numériques comprend plusieurs actes législatifs, tels que la législation de l'Union sur des produits spécifiques concernant les aspects liés à la sécurité et la législation générale sur la responsabilité des produits. La proposition est cohérente avec le cadre réglementaire actuel de l'UE relatif aux produits, ainsi qu'avec des propositions législatives récentes telles que la proposition de règlement de la Commission [règlement sur l'intelligence artificielle (IA)][7].

---

5 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020 – «Façonner l'avenir numérique de l'Europe», COM(2020) 67 final.

6 Principalement les dispositifs du nouveau cadre législatif (NCL).

7 Proposition de règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union [COM(2021) 206 final].

Le règlement proposé s'appliquerait à tous les équipements radioélectriques relevant du champ d'application du règlement délégué (UE) 2022/30 de la Commission. En outre, les exigences établies par le présent règlement comprennent tous les éléments des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE, y compris les principaux éléments énoncés dans la [décision d'exécution XXX/2022 de la Commission relative à une demande de normalisation adressée aux organisations européennes de normalisation] émise sur la base dudit règlement délégué. Afin d'éviter un chevauchement des réglementations, il est envisagé que la Commission abroge ou modifie le règlement délégué relatif aux équipements radioélectriques couverts par la proposition de règlement, de sorte que ce dernier soit applicable à ces équipements, une fois en vigueur.

En outre, afin d'éviter une duplication des travaux, il est envisagé que la Commission et les organisations européennes de normalisation tiennent compte des travaux de normalisation menés dans le contexte de la décision d'exécution C(2022)5637 de la Commission relative à une demande de normalisation du règlement délégué RED [règlement (UE) 2022/30] lors de la préparation et de l'élaboration de normes harmonisées visant à faciliter la mise en œuvre du règlement.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la présente proposition est l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), qui prévoit l'adoption de mesures destinées à assurer l'établissement et le fonctionnement du marché intérieur. L'objectif de la proposition est d'harmoniser les exigences en matière de cybersécurité pour les produits comportant des éléments numériques dans tous les États membres et d'éliminer les obstacles à la libre circulation des biens.

L'article 114 du TFUE peut être utilisé comme base juridique pour prévenir l'apparition des obstacles résultant de divergences entre les législations et approches nationales quant à la manière de remédier aux incertitudes et lacunes juridiques dans les cadres juridiques existants[8]. En outre, la Cour de justice a reconnu que la mise en œuvre d'exigences techniques hétérogènes pouvait constituer un motif valable pour déclencher l'application de l'article 114 du TFUE[9].

Le cadre législatif actuel de l'Union applicable aux produits comportant des éléments numériques est fondé sur l'article 114 du TFUE et comprend plusieurs actes législatifs, portant notamment sur des produits spécifiques et des aspects liés à la sécurité ou une législation générale sur la responsabilité du fait des produits. Cependant, elle ne couvre que certains aspects relatifs à la cybersécurité des produits numériques matériels et, le cas échéant, des logiciels intégrés dans ces produits. Au niveau national, les États membres commencent à prendre des mesures exigeant des fournisseurs de produits numériques qu'ils renforcent leur cybersécurité[10]. Dans le même temps, la cybersécurité des produits numériques revêt une

---

8 CJUE, arrêt de la Cour (grande chambre) du 3 décembre 2019, République tchèque/Parlement européen et Conseil de l'Union européenne, affaire C-482/17, point 35.

9 CJUE, arrêt de la Cour (grande chambre) du 2 mai 2006, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord/Parlement européen et Conseil de l'Union européenne, affaire C-217/04, points 62 et 63.

10 Par exemple, en 2019, la Finlande a créé un système d'étiquetage pour les appareils de l'internet des objets, tels que les téléviseurs, téléphones et jouets intelligents, sur la base des normes ETSI.

dimension transfrontière particulièrement importante, étant donné que les produits fabriqués dans un pays sont souvent utilisés par des organisations et consommateurs dans l'ensemble du marché intérieur. Les incidents qui concernent initialement une seule entité ou un seul État membre se propagent souvent en quelques minutes entre organisations, secteurs et États membres.

Les divers actes et initiatives adoptés à ce jour aux niveaux européen et national ne traitent qu'en partie les problèmes recensés et risquent de créer une mosaïque législative dans le marché intérieur, ce qui aurait pour effet d'accroître l'insécurité juridique tant pour les fournisseurs que pour les utilisateurs de ces produits et d'alourdir inutilement la charge imposée aux entreprises pour se conformer à un certain nombre d'exigences pour des types de produits similaires.

Le règlement proposé harmoniserait et rationaliserait le paysage réglementaire de l'UE en introduisant des exigences en matière de cybersécurité pour les produits comportant des éléments numériques et éviterait le chevauchement d'exigences découlant de différents actes législatifs. Cela créerait une plus grande sécurité juridique pour les opérateurs et les utilisateurs dans l'ensemble de l'Union, ainsi qu'une meilleure harmonisation du marché unique européen, en créant des conditions plus viables pour les opérateurs désireux de pénétrer sur le marché de l'Union.

- **Subsidiarité (en cas de compétence non exclusive)**

La nature fortement transfrontière de la cybersécurité en général et le nombre croissant de risques et d'incidents ayant des répercussions transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs de la présente intervention ne peuvent pas être atteints efficacement par les seuls États membres. Les approches nationales pour faire face aux problèmes, et en particulier les approches introduisant des exigences contraignantes, sont de nature à créer une insécurité juridique et des obstacles juridiques supplémentaires. Les entreprises risqueraient de ne pas pouvoir étendre leurs activités de manière fluide à d'autres États membres, privant les utilisateurs du bénéfice de leurs produits.

Une action commune au niveau de l'UE est donc nécessaire pour établir un niveau élevé de confiance parmi les utilisateurs, en augmentant l'attractivité des produits de l'UE comportant des éléments numériques. Elle profiterait également au marché unique numérique et au marché intérieur en général en assurant la sécurité juridique et en créant des conditions de concurrence équitables pour les fabricants de produits comportant des éléments numériques.

Enfin, les conclusions du Conseil du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne invitent la Commission à proposer, d'ici à la fin 2022, des exigences communes en matière de cybersécurité pour les dispositifs connectés.

- **Proportionnalité**

S'agissant de la proportionnalité de la proposition de règlement, les mesures prévues dans les options envisagées n'excéderaient pas ce qui est nécessaire pour atteindre les objectifs généraux et spécifiques et n'entraîneraient pas de coûts disproportionnés. Plus précisément, l'intervention envisagée garantirait que les produits comportant des éléments numériques soient sécurisés tout au long de leur cycle de vie et proportionnellement aux risques encourus grâce à des exigences axées sur les objectifs et technologiquement neutres qui restent raisonnables et correspondent généralement à l'intérêt des entités concernées.

L'Allemagne a récemment introduit un label de sécurité pour les routeurs à haut débit, les téléviseurs intelligents, les caméras, les haut-parleurs, les jouets ainsi que les robots de nettoyage et de jardinage.

Les exigences essentielles de la proposition en matière de cybersécurité s'appuient sur des normes largement utilisées, et le processus de normalisation qui suivra tiendra compte des spécificités techniques des produits. Cela signifie que les contrôles de sécurité seraient adaptés lorsque cela se révélerait nécessaire pour un niveau de risque donné. En outre, les règles horizontales envisagées ne prévoiraient une évaluation par un tiers que pour les produits critiques. Celle-ci ne concernerait donc qu'une part restreinte du marché des produits comportant des éléments numériques. L'incidence sur les PME dépendrait de leur présence sur le marché de ces catégories de produits spécifiques.

S'agissant de la proportionnalité des coûts pour l'évaluation de la conformité, les organismes notifiés chargés des évaluations par des tiers tiendraient compte de la taille de l'entreprise lors de la fixation de leurs redevances. Une période de transition raisonnable de 24 mois serait également prévue pour préparer la mise en œuvre, de manière à donner le temps aux marchés concernés de se préparer, tout en fournissant une orientation claire pour les investissements en R&D. Tous les coûts de conformité pour les entreprises seraient compensés par les avantages apportés par un niveau plus élevé de sécurité des produits comportant des éléments numériques et, en fin de compte, par une confiance plus grande des utilisateurs dans ces produits.

- **Choix de l'instrument**

Une intervention réglementaire supposerait l'adoption d'un règlement et non d'une directive. En effet, pour ce type particulier de législation sur les produits, un règlement permettrait de gérer les problèmes recensés et d'atteindre les objectifs formulés plus efficacement, étant donné qu'il s'agit d'une intervention qui conditionne la mise sur le marché intérieur d'une très large catégorie de produits. Dans le cas d'une directive, le processus de transposition pourrait laisser trop de marge de manœuvre au niveau national, ce qui pourrait conduire à un manque d'uniformité de certaines exigences essentielles en matière de cybersécurité, à une insécurité juridique, à une fragmentation accrue ou même à des situations transfrontières discriminatoires, d'autant plus que les produits couverts pourraient avoir de multiples finalités ou usages et que les fabricants peuvent produire de multiples catégories de tels produits.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Consultation des parties intéressées**

La Commission a consulté un large éventail de parties intéressées. Les États membres et les parties intéressées ont été invités à participer à la consultation publique ouverte et aux enquêtes et ateliers organisés dans le cadre d'une étude menée par un consortium formé du cabinet Wavestone, du Centre for European Policy Studies (CEPS) et de l'organisme de recherche politique ICF qui a appuyé les travaux préparatoires de la Commission en vue de l'analyse d'impact. Les parties intéressées consultées incluaient les autorités nationales de surveillance du marché, les organismes de l'Union chargés de la cybersécurité, les fabricants de matériel et de logiciels, les importateurs et distributeurs de matériel et de logiciels, les associations professionnelles, les organisations de consommateurs et les utilisateurs de produits comportant des éléments numériques, des citoyens, chercheurs et universitaires, les organismes notifiés et les organismes d'accréditation, ainsi que les professionnels du secteur de la cybersécurité.

La consultation comprenait les activités suivantes:

- une première étude réalisée par un consortium composé d'ICF, Wavestone, Carsa et le CEPS, qui a été publiée en décembre 2021[11]. Cette étude a mis au jour plusieurs défaillances du marché et évalué les interventions réglementaires possibles;
- une consultation publique ouverte ciblant les citoyens, les parties prenantes et les experts en cybersécurité. 176 réponses ont été reçues. Celles-ci ont contribué à la collecte d'avis et d'expériences diverses auprès de tous les groupes d'intervenants;
- des ateliers organisés dans le cadre de l'étude visant à étayer les travaux préparatoires de la Commission en vue de l'adoption d'une législation sur la cyberrésilience, qui ont rassemblé une centaine de représentants de diverses parties prenantes venus des 27 États membres de l'Union;
- des entretiens d'experts menés afin de mieux comprendre les défis actuels en matière de cybersécurité liés aux produits comportant des éléments numériques et de discuter des options stratégiques pour une éventuelle intervention réglementaire;
- des discussions bilatérales avec les autorités nationales chargées de la cybersécurité, le secteur privé et les organisations de consommateurs;
- des activités de sensibilisation ciblées menées auprès des principales parties prenantes des PME.

- **Obtention et utilisation d'expertise**

Les activités de consultation visaient à recueillir des contributions sur les cinq principaux critères d'évaluation fondés sur les lignes directrices de l'UE pour une meilleure réglementation (efficacité, efficience, pertinence, cohérence, valeur ajoutée de l'UE) ainsi que sur les incidences potentielles des options possibles pour l'avenir. Le contractant a non seulement contacté les parties prenantes directement concernées par la proposition de règlement, mais a également consulté un large éventail d'experts dans le domaine de la cybersécurité.

- **Analyse d'impact**

La Commission a réalisé une analyse d'impact pour la présente proposition, qui a été examinée par le comité d'examen de la réglementation de la Commission. Une réunion avec le comité a eu lieu le 6 juillet 2022 et a été suivie d'un avis positif. L'analyse d'impact a été ajustée afin de tenir compte des recommandations et observations du comité.

La Commission a examiné différentes options stratégiques pour atteindre les objectifs généraux de la proposition.

- Approche non contraignante et mesures volontaires (option nº 1): cette option ne suit pas la voie d'une intervention réglementaire contraignante. Au lieu de cela, la Commission publierait des communications, des orientations, des recommandations et éventuellement des codes de conduite pour encourager les mesures volontaires. Des régimes nationaux, volontaires ou contraignants,

[11] Study on the need of Cybersecurity requirements for ICT products – nº 2020-0715, Final Study Report, disponible à l'adresse suivante: https://digital-strategy.ec.europa.eu/fr/library/study-need-cybersecurity-requirements-ict-products (en anglais).

continueraient à être développés pour pallier l'absence de règles horizontales de l'UE.

- Intervention réglementaire ad-hoc pour la cybersécurité des produits matériels comportant des éléments numériques et de leurs logiciels intégrés (option nº 2): cette option supposerait une intervention réglementaire ad hoc spécifique au produit qui se limiterait à l'ajout et/ou à la modification des exigences en matière de cybersécurité dans la législation existante ou à l'introduction d'une nouvelle législation à mesure que de nouveaux risques apparaissent, y compris potentiellement pour les logiciels non intégrés.

Les options nºs 3 et 4 supposent une intervention réglementaire horizontale de portée variable, suivant en grande partie le nouveau cadre législatif (NCL). Ce cadre fixe des exigences essentielles comme condition à la mise de certains produits sur le marché intérieur. En plus, le NCL prévoit généralement une évaluation de la conformité, processus mené par le fabricant pour démontrer que les exigences spécifiées relatives à un produit ont été satisfaites.

- Approche mixte, comprenant des règles horizontales contraignantes pour la cybersécurité des produits matériels comportant des éléments numériques et leurs logiciels intégrés et une approche graduelle pour les logiciels non intégrés (option nº 3): cette option reposerait sur un règlement introduisant des exigences horizontales de cybersécurité pour tous les produits matériels comportant des éléments numériques et les logiciels qui y sont intégrés, comme condition de mise sur le marché, et comprendrait deux sous-options avec et sans évaluation obligatoire par un tiers (3i et 3ii). Les logiciels non intégrés ne seraient pas réglementés.
- Une intervention réglementaire horizontale instaurant des exigences en matière de cybersécurité pour une vaste gamme de produits matériels et immatériels comportant des éléments numériques, y compris les logiciels non intégrés (option nº 4): cette option est semblable à l'option nº 3, hormis son champ d'application. En effet, dans le cadre de l'option nº4, le champ d'application de l'éventuel règlement s'étendrait aux logiciels non intégrés [avec deux sous-options englobant, respectivement, uniquement les logiciels critiques (4a) ou tous les logiciels (4b)]. Pour chaque sous-option, des alternatives identiques à celles de l'option nº 3 seraient envisagées concernant l'évaluation de la conformité.

L'option nº 4 (avec des sous-options couvrant tous les logiciels et requérant une évaluation de la conformité par un tiers pour les produits critiques) est apparue comme la voie à privilégier, à la lumière de l'évaluation de l'efficacité par rapport aux objectifs spécifiques recherchés et de l'efficacité coûts-bénéfices. Cette option garantirait la définition d'exigences horizontales spécifiques en matière de cybersécurité pour tous les produits comportant des éléments numériques mis à disposition ou mis sur le marché intérieur. Elle serait en outre la seule à couvrir l'ensemble de la chaîne d'approvisionnement numérique. Les logiciels non intégrés, souvent exposés à des vulnérabilités, seraient également concernés par une telle intervention réglementaire, ce qui garantirait une approche cohérente à l'égard de tous les produits comportant des éléments numériques, avec une répartition claire des responsabilités entre les différents opérateurs économiques.

Cette option apporte en outre une valeur ajoutée, car elle couvre les aspects du devoir de diligence et du cycle de vie complet après la mise sur le marché des produits comportant des éléments numériques. Il devient ainsi possible de garantir, entre autres, des informations appropriées sur l'assistance en matière de sécurité et la fourniture de mises à jour de sécurité.

Cette option viendrait également compléter plus efficacement la récente révision du cadre SRI, en mettant en place les conditions préalables à un renforcement de la sécurité de la chaîne d'approvisionnement.

L'option privilégiée présenterait des avantages significatifs pour les différentes parties prenantes. Du point de vue des entreprises, elle éviterait l'application de règles de sécurité divergentes aux produits comportant des éléments numériques et réduirait les coûts de conformité à la législation en matière de cybersécurité. Elle ferait diminuer le nombre de cyberincidents, les coûts liés à la gestion de ces incidents et les atteintes à la réputation des entreprises. Pour l'ensemble de l'UE, on estime qu'elle se traduirait par une réduction de quelque 180 à 290 milliards d'EUR par an des coûts liés aux incidents affectant les entreprises. Cette option entraînerait une hausse du chiffre d'affaires des entreprises, résultant de l'augmentation de la demande en produits comportant des éléments numériques. Elle améliorerait la réputation mondiale des entreprises, avec, à la clé, un accroissement de la demande en dehors de l'UE. Du point de vue des utilisateurs, l'option privilégiée améliorerait la transparence des propriétés de sécurité des produits et faciliterait l'utilisation de produits comportant des éléments numériques. Les consommateurs et les citoyens bénéficieraient également d'une meilleure protection de leurs droits fondamentaux, tels que la vie privée et la protection des données.

Interrogés sur l'efficacité des interventions envisagées, les répondants à la consultation publique se sont accordés à dire que l'option nº 4 serait la plus efficace (4,08 sur une échelle de 1 à 5). Parmi ces répondants figuraient des organisations de consommateurs (5,00), des personnes se présentant comme utilisateurs (4,22), des organismes notifiés (4,17), des autorités de surveillance du marché (5,00) et des fabricants de produits comportant des éléments numériques (3,85), dont des PME (4,05).

- **Réglementation affûtée et simplification**

Cette proposition établit des exigences qui s'appliqueront aux fabricants de logiciels et de matériel. Il est nécessaire de garantir la sécurité juridique et d'éviter une nouvelle fragmentation, sur le marché intérieur, des exigences en matière de cybersécurité. Cette nécessité a été démontrée par le large soutien des diverses parties prenantes en faveur d'une intervention horizontale. La proposition réduira au minimum la charge réglementaire imposée aux fabricants par la multiplication des actes législatifs relatifs à la sécurité des produits. L'alignement sur le NCL sera synonyme d'un meilleur fonctionnement de l'intervention et de son application. La proposition simplifie le processus des procédures de sauvegarde en y associant les fabricants et les États membres avant la notification à la Commission. Une grande partie des fabricants visés par la proposition connaissent déjà le fonctionnement du NCL, ce qui facilitera sa compréhension et sa mise en œuvre. Du point de vue des consommateurs et des entreprises, la proposition renforcera la confiance dans les produits comportant des éléments numériques.

- **Droits fondamentaux**

Toutes les options politiques envisagées devraient renforcer dans une certaine mesure la protection des libertés et droits fondamentaux tels que la vie privée, la protection des données à caractère personnel, la liberté d'entreprise et la protection des biens ou de la dignité et de l'intégrité des personnes. En particulier, l'option nº 4 privilégiée, qui consisterait en des interventions réglementaires horizontales ayant une vaste portée politique, serait la plus efficace à cet égard, car elle serait mieux à même de réduire le nombre et la gravité des incidents, y compris les violations de données à caractère personnel. Elle renforcerait également la sécurité juridique et créerait des conditions de concurrence équitables pour les

opérateurs économiques, et elle renforcerait la confiance des utilisateurs et l'attractivité des produits de l'UE comportant des éléments numériques dans leur ensemble, protégeant ainsi la propriété et améliorant les conditions d'activité des opérateurs économiques.

Les exigences horizontales en matière de cybersécurité contribueraient à la sécurité des données à caractère personnel en protégeant la confidentialité, l'intégrité et la disponibilité des informations contenues dans les produits comportant des éléments numériques. Le respect de ces exigences facilitera le respect de l'exigence de sécurité du traitement des données à caractère personnel en vertu du règlement (UE) 2016/679 relatif à la protection des données (RGPD)[12]. La proposition améliorerait la transparence et l'information des utilisateurs, y compris ceux dont les compétences en cybersécurité pourraient être moindres. Les utilisateurs seraient également mieux informés des risques, des capacités et des limites des produits comportant des éléments numériques, ce qui les placerait dans une meilleure position pour prendre les mesures de prévention et d'atténuation nécessaires en vue de réduire les risques résiduels.

4. INCIDENCE BUDGÉTAIRE

Afin de s'acquitter des tâches qui lui sont dévolues en vertu du présent règlement, l'Agence de l'Union européenne pour la cybersécurité (ENISA) devra réaffecter des ressources à hauteur d'environ 4,5 ETP. La Commission devrait allouer 7 ETP pour s'acquitter de ses responsabilités en matière d'application du présent règlement.

Une vue d'ensemble détaillée des coûts engendrés est présentée dans la «fiche financière» qui accompagne la présente proposition.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La Commission suivra la mise en œuvre, l'application et le respect de ces nouvelles dispositions pour évaluer leur efficacité. Le règlement prévoira une évaluation et un réexamen par la Commission et la présentation d'un rapport public à cet égard au Parlement européen et au Conseil au plus tard 36 mois après la date d'entrée en vigueur du présent règlement et tous les quatre ans par la suite.

- **Explication détaillée des dispositions spécifiques de la proposition**

Dispositions générales (chapitre I)

La présente proposition de règlement établit a) des règles pour la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits; b) les exigences essentielles relatives à la conception, au développement et à la fabrication de produits comportant des éléments numériques ainsi que les obligations incombant aux opérateurs économiques en ce qui concerne ces produits en matière de cybersécurité; c) les exigences essentielles relatives aux processus de gestion de la vulnérabilité mis en place par les fabricants afin de garantir la cybersécurité des produits comportant des éléments numériques tout au long de leur cycle de vie, et les obligations

[12] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

incombant aux opérateurs économiques en ce qui concerne ces processus; d) les règles relatives à la surveillance du marché et à l'application des règles et exigences susmentionnées.

Le règlement proposé s'appliquera à tous les produits comportant des éléments numériques dont l'utilisation prévue et raisonnablement prévisible comprend une connexion logique ou physique directe ou indirecte à un appareil ou à un réseau.

Le règlement proposé ne s'appliquera pas aux produits comportant des éléments numériques relevant du champ d'application du règlement (UE) 2017/745 [dispositifs médicaux à usage humain et accessoires pour ces dispositifs] et du règlement (UE) 2017/746 [dispositifs médicaux de diagnostic *in vitro* à usage humain et accessoires pour ces dispositifs], étant donné que ces deux règlements contiennent des exigences concernant les dispositifs, y compris les logiciels et les obligations générales des fabricants, couvrant l'ensemble du cycle de vie des produits, ainsi que des procédures d'évaluation de la conformité. Le présent règlement ne s'appliquera pas aux produits comportant des éléments numériques qui ont été certifiés conformément au règlement (UE) 2018/1139 [niveau uniforme élevé de sécurité de l'aviation civile], ni aux produits auxquels s'applique le règlement (UE) 2019/2144 [concernant les prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques destinés à ces véhicules].

Les produits critiques comportant des éléments numériques sont soumis à des procédures spécifiques d'évaluation de la conformité et sont divisés en classes I et II, comme indiqué à l'annexe III, en fonction de leur niveau de risque de cybersécurité, la classe II représentant un risque plus élevé. Un produit comportant des éléments numériques est considéré comme critique et figure donc à l'annexe III compte tenu de l'incidence des vulnérabilités potentielles en matière de cybersécurité qu'il présente. La fonctionnalité liée à la cybersécurité du produit comportant des éléments numériques et son utilisation prévue dans des environnements sensibles tels qu'un environnement industriel, entre autres, sont prises en considération dans la détermination du risque de cybersécurité.

La Commission est également habilitée à adopter des actes délégués pour compléter le présent règlement en précisant des catégories de produits hautement critiques comportant des éléments numériques pour lesquels les fabricants sont tenus d'obtenir un certificat européen de cybersécurité dans le cadre d'un schéma européen de certification de cybersécurité afin de démontrer la conformité aux exigences essentielles énoncées à l'annexe I, ou à certaines de celles-ci. Lorsqu'elle établit ces catégories de produits hautement critiques comportant des éléments numériques, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits en question, à la lumière d'un ou de plusieurs des critères pris en considération pour l'inscription des produits critiques comportant des éléments numériques à l'annexe III, ainsi que de l'évaluation visant à déterminer si les entités essentielles du type visé à l'annexe [annexe I] de la directive [directive XXX/ XXXX (SRI 2)] utilisent cette catégorie de produits ou en dépendent ou si cette catégorie de produits aura une potentielle importance à l'avenir pour les activités de ces entités, ou est pertinente pour la résilience de l'ensemble de la chaîne d'approvisionnement des produits comportant des éléments numériques face à des événements perturbateurs.

Obligations des opérateurs économiques (chapitre II)

La proposition intègre des obligations pour les fabricants, les importateurs et les distributeurs qui s'appuient sur les dispositions de référence prévues dans la décision nº 768/2008/CE. En vertu des exigences et obligations essentielles en matière de cybersécurité, tous les produits comportant des éléments numériques ne peuvent être mis à disposition sur le marché que si, lorsqu'ils sont dûment fournis, correctement installés, entretenus et utilisés conformément à

leur utilisation prévue ou dans des conditions raisonnablement prévisibles, ils satisfont aux exigences essentielles en matière de cybersécurité énoncées dans le présent règlement.

Les exigences et obligations essentielles contraindraient les fabricants à tenir compte de la cybersécurité dans la conception, le développement et la fabrication des produits comportant des éléments numériques, à exercer une diligence raisonnable sur les aspects de sécurité lors de la conception et du développement de leurs produits, à être transparents sur les aspects de cybersécurité qui doivent être portés à la connaissance des clients, à assurer une assistance en matière de sécurité (sous forme de mises à jour) de manière proportionnée et à se conformer aux exigences en matière de gestion des vulnérabilités.

Des obligations seraient mises en place pour les opérateurs économiques, depuis les fabricants jusqu'aux distributeurs et aux importateurs, en ce qui concerne la mise sur le marché de produits comportant des éléments numériques, en fonction de leur rôle et de leurs responsabilités dans la chaîne d'approvisionnement.

Conformité du produit comportant des éléments numériques (chapitre III)

Le produit comportant des éléments numériques, conforme à des normes harmonisées ou à des parties de celles-ci dont les références ont été publiées au *Journal officiel de l'Union européenne*, est présumé conforme aux exigences essentielles couvertes par la présente proposition de règlement. En l'absence de normes harmonisées, ou si celles-ci sont insuffisantes, si la procédure de normalisation accuse des retards indus ou si la demande de la Commission n'a pas été acceptée par les organisations européennes de normalisation, la Commission peut, au moyen d'actes d'exécution, adopter des spécifications communes.

En outre, les produits comportant des éléments numériques qui ont été certifiés ou pour lesquels une déclaration UE de conformité ou un certificat ont été délivrés au titre d'un schéma européen de certification de cybersécurité conformément au règlement (UE) 2019/881, et pour lesquels la Commission a précisé par voie d'acte d'exécution que ce document pouvait fournir une présomption de conformité aux fins du présent règlement, sont présumés conformes aux exigences essentielles du présent règlement, ou à des parties de celui-ci, dans la mesure où la déclaration UE de conformité ou le certificat de cybersécurité, ou des parties de ceux-ci, couvrent ces exigences.

De plus, afin d'éviter une charge administrative excessive pour les fabricants, le cas échéant, la Commission devrait préciser si un certificat de cybersécurité délivré dans le cadre d'un tel schéma européen de certification de cybersécurité élimine l'obligation, pour les fabricants, de faire procéder à une évaluation de conformité par un tiers conformément au présent règlement pour les exigences correspondantes.

Le fabricant doit procéder à une évaluation de la conformité du produit comportant des éléments numériques et des processus de traitement des vulnérabilités qu'il a mis en place afin de démontrer leur conformité aux exigences essentielles énoncées à l'annexe I en suivant l'une des procédures énoncées à l'annexe VI. Les fabricants de produits critiques des classes I et II doivent utiliser les modules respectifs nécessaires à la conformité. Les fabricants de produits critiques de classe II doivent associer un tiers à leur évaluation de la conformité.

Notification des organismes d'évaluation de la conformité (chapitre IV)

Le bon fonctionnement des organismes notifiés est essentiel pour assurer un niveau élevé de cybersécurité et pour la confiance de toutes les parties intéressées dans le système de la nouvelle approche. Par conséquent, conformément à la décision 768/2008/CE, la proposition définit des exigences pour les autorités nationales responsables des organismes d'évaluation de la conformité (organismes notifiés). Elle confie aux États membres la responsabilité ultime de la désignation et de la surveillance des organismes notifiés. Les États membres désignent

une autorité notifiante responsable de la mise en place et de l'application des procédures nécessaires à l'évaluation et à la notification des organismes d'évaluation de la conformité ainsi qu'au contrôle des organismes notifiés.

Surveillance du marché et contrôle de l'application de la législation (chapitre V)

Conformément au règlement (UE) 2019/1020, les autorités nationales de surveillance du marché assurent la surveillance du marché sur le territoire de l'État membre concerné. Les États membres peuvent choisir de désigner toute autorité existante ou nouvelle pour agir en qualité d'autorité de surveillance du marché, y compris les autorités nationales compétentes établies conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] ou les autorités nationales de certification de cybersécurité désignées conformément à l'article 58 du règlement (UE) 2019/881. Les opérateurs économiques sont invités à coopérer pleinement avec les autorités de surveillance du marché et les autres autorités compétentes.

Pouvoirs délégués et procédure de comité (chapitre VI)

Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du TFUE est délégué à la Commission pour lui permettre de mettre à jour la liste des produits critiques des classes I et II et de préciser les définitions de ces produits; de préciser si une limitation ou une exclusion est nécessaire pour les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui établissent des exigences assurant le même niveau de protection que le présent règlement; de rendre obligatoire la certification de certains produits hautement critiques comportant des éléments numériques sur la base des critères énoncés dans le présent règlement; de spécifier le contenu minimal de la déclaration UE de conformité et de compléter les éléments à inclure dans la documentation technique.

La Commission est également habilitée à adopter des actes d'exécution pour: préciser le format ou les éléments des obligations de signalement et de la nomenclature des logiciels; préciser les schémas européens de certification de cybersécurité qui peuvent être utilisés pour démontrer la conformité aux exigences essentielles énoncées dans le présent règlement ou à une partie de celles-ci; adopter des spécifications communes; fixer les spécifications techniques relatives à l'apposition du marquage CE; adopter des mesures correctives ou restrictives au niveau de l'Union dans des circonstances exceptionnelles justifiant une intervention immédiate afin de préserver le bon fonctionnement du marché intérieur.

Confidentialité et sanctions (chapitre VII)

Toutes les parties qui appliquent le présent règlement respectent la confidentialité des informations et données obtenues dans l'accomplissement de leurs tâches et activités.

Afin de garantir une application efficace des obligations prévues par le présent règlement, chaque autorité de surveillance du marché devrait avoir le pouvoir d'imposer ou de demander l'imposition d'amendes administratives. Dans le même ordre d'idées, le présent règlement fixe des montants maximaux pour les amendes administratives qui devraient être prévues dans les législations nationales en cas de non-respect des obligations énoncées dans le présent règlement.

Dispositions transitoires et finales (chapitre VIII)

Afin de laisser aux fabricants, aux organismes notifiés et aux États membres le temps de s'adapter aux nouvelles exigences, le règlement proposé deviendra applicable [24 mois] après son entrée en vigueur, à l'exception de l'obligation de signalement pour les fabricants, qui s'appliquera [12 mois] après la date d'entrée en vigueur.

2022/0272 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Il est nécessaire d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme concernant les exigences essentielles en matière de cybersécurité aux fins de la mise sur le marché de l'Union de produits comportant des éléments numériques. Deux problèmes majeurs représentant des coûts supplémentaires pour les utilisateurs et la société devraient être réglés: d'une part, le niveau de cybersécurité des produits comportant des éléments numériques est faible, comme en témoignent les vulnérabilités généralisées et le manque de mises à jour de sécurité déployées de manière cohérente pour y remédier, et, d'autre part, les utilisateurs n'ont pas suffisamment accès aux informations et ne les comprennent pas bien, ce qui les empêche de choisir des produits dotés de propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée.

(2) Le présent règlement vise à définir les conditions aux limites pour le développement de produits comportant des éléments numériques sécurisés en faisant en sorte que les produits matériels et logiciels mis sur le marché présentent moins de vulnérabilités et que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit. Il a également pour but de créer des conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques.

(3) La législation pertinente de l'Union actuellement en vigueur comprend plusieurs ensembles de règles horizontales qui traitent de certains aspects liés à la cybersécurité sous différents angles, y compris des mesures destinées à améliorer la sécurité de la

[1] JO C du , p. .
[2] JO C du , p. .

chaîne d'approvisionnement numérique. Toutefois, la législation existante de l'Union relative à la cybersécurité, dont la [directive XXX/XXXX (SRI 2)] et le règlement (UE) 2019/881 du Parlement européen et du Conseil[3], ne couvre pas directement les exigences contraignantes en matière de sécurité des produits comportant des éléments numériques.

(4) Bien que la législation de l'Union en vigueur s'applique à certains produits comportant des éléments numériques, il n'existe pas de cadre réglementaire horizontal de l'Union établissant des exigences complètes en matière de cybersécurité pour tous les produits comportant des éléments numériques. Les différents actes et initiatives adoptés à ce jour aux niveaux européen et national n'abordent qu'en partie les problèmes et risques recensés concernant la cybersécurité, ce qui a pour effet de créer une mosaïque législative au sein du marché intérieur et d'accroître l'insécurité juridique tant pour les fabricants que pour les utilisateurs de ces produits et d'alourdir inutilement la charge imposée aux entreprises pour se conformer à un certain nombre d'exigences pour des types de produits similaires. La cybersécurité de ces produits revêt une dimension transfrontière particulièrement forte, étant donné que les produits fabriqués dans un pays sont souvent utilisés par des organisations et des consommateurs dans l'ensemble du marché intérieur. Il est donc nécessaire de réglementer cette question au niveau de l'Union. Le paysage réglementaire de l'Union devrait être harmonisé en introduisant des exigences en matière de cybersécurité pour les produits comportant des éléments numériques. Il convient en outre de garantir la sécurité des opérateurs et des utilisateurs dans l'ensemble de l'Union, ainsi que de renforcer l'harmonisation du marché unique, en créant des conditions plus viables pour les opérateurs désireux de pénétrer sur le marché de l'Union.

(5) Au niveau de l'Union, divers documents programmatiques et politiques, tels que la stratégie de cybersécurité de l'Union pour la décennie numérique[4], les conclusions du Conseil du 2 décembre 2020 et du 23 mai 2022 ou encore la résolution du Parlement européen du 10 juin 2021[5], appelaient à l'adoption par l'Union d'exigences spécifiques en matière de cybersécurité pour les produits numériques ou connectés, étant donné que plusieurs pays à travers le monde introduisaient des mesures pour réglementer cette question de leur propre initiative. Dans le rapport final de la conférence sur l'avenir de l'Europe[6], les citoyens ont préconisé de «renforcer le rôle de l'Union dans la lutte contre les menaces de cybersécurité».

(6) Pour accroître le niveau global de cybersécurité de tous les produits comportant des éléments numériques mis sur le marché intérieur, il est nécessaire d'introduire des exigences de cybersécurité essentielles, axées sur l'objectif et technologiquement neutres pour ces produits, qui s'appliquent horizontalement.

---

3 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_FR.html.

6 *Conférence sur l'avenir de l'Europe – Rapport sur les résultats finaux*, mai 2022, proposition 28, point 2. La conférence s'est tenue entre avril 2021 et mai 2022. Il s'est agi d'un exercice unique de démocratie délibérative menée par les citoyens à l'échelle paneuropéenne, qui a impliqué des milliers de citoyens européens ainsi que des acteurs politiques, des partenaires sociaux, des représentants de la société civile et des parties prenantes clefs.

(7) Dans certaines conditions, tous les produits comportant des éléments numériques intégrés ou connectés à un système d'information électronique plus vaste peuvent servir de vecteur d'attaque pour des acteurs malveillants. En conséquence, même le matériel et les logiciels considérés comme moins critiques peuvent faciliter une première compromission d'un appareil ou d'un réseau, permettant à des acteurs malveillants d'obtenir un accès privilégié à un système ou de se déplacer latéralement entre différents systèmes. Les fabricants devraient donc veiller à ce que tous les produits connectables comportant des éléments numériques soient conçus et développés conformément aux exigences essentielles énoncées dans le présent règlement. Cela comprend à la fois les produits qui peuvent être connectés physiquement via des interfaces matérielles et les produits qui sont connectés logiquement, notamment par des connecteurs logiciels, tuyauteries, fichiers, interfaces de programmation d'application ou tout autre type d'interface logicielle. Étant donné que les menaces de cybersécurité peuvent se propager via divers produits comportant des éléments numériques avant d'atteindre une cible donnée, par exemple en enchaînant plusieurs exploits de vulnérabilité, les fabricants devraient également assurer la cybersécurité des produits qui ne sont connectés qu'indirectement à d'autres dispositifs ou réseaux.

(8) La définition d'exigences en matière de cybersécurité des produits comportant des éléments numériques aux fins de leur mise sur le marché renforcera la cybersécurité de ces produits, tant pour les consommateurs que pour les entreprises. Parmi ces exigences figurent également des exigences de mise sur le marché applicables aux produits de consommation destinés aux consommateurs vulnérables, tels que les jouets et les moniteurs pour bébés.

(9) Le présent règlement garantit un niveau élevé de cybersécurité des produits comportant des éléments numériques. Il ne réglemente pas les services, tels que le logiciel en tant que service (SaaS), à l'exception des solutions de traitement de données à distance relatives à un produit comportant des éléments numériques, par lesquelles on entend tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant du produit concerné ou sous la responsabilité de celui-ci, et dont l'absence empêcherait ledit produit d'exécuter l'une de ses fonctions. La [directive XXX/XXXX (SRI 2)] met en place des exigences en matière de cybersécurité et de signalement des incidents pour les entités essentielles et importantes, telles que les infrastructures critiques, en vue d'accroître la résilience des services qu'elles fournissent. La [directive XXX/XXXX (SRI 2)] s'applique aux services d'informatique en nuage et aux modèles de services en nuage, tels que le SaaS. Toutes les entités fournissant des services d'informatique en nuage dans l'Union, qui atteignent ou dépassent le seuil fixé pour les entreprises de taille moyenne relèvent du champ d'application de cette directive.

(10) Afin de ne pas entraver l'innovation ou la recherche, les logiciels libres et ouverts développés ou fournis en dehors du cadre d'une activité commerciale ne devraient pas être couverts par le présent règlement. C'est notamment le cas des logiciels, y compris leurs codes sources et versions modifiées, qui sont librement partagés et accessibles, utilisables, modifiables et redistribuables. En ce qui concerne le logiciel, l'activité commerciale peut être caractérisée non seulement par le prix facturé pour un produit, mais également par le prix des services d'assistance technique, par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, ou par l'utilisation de données à caractère personnel pour des raisons autres

qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel.

(11) Un internet sécurisé est indispensable au fonctionnement des infrastructures critiques et à la société dans son ensemble. La [directive XXX/XXXX (SRI 2)] vise à garantir un niveau élevé de cybersécurité des services fournis par des entités essentielles et importantes, y compris les fournisseurs d'infrastructures numériques qui soutiennent les fonctions essentielles de l'internet ouvert, assurent l'accès à l'internet et les services internet. Il est donc important que les produits comportant des éléments numériques dont les fournisseurs d'infrastructures numériques ont besoin pour assurer le fonctionnement de l'internet soient développés de manière sécurisée et qu'ils respectent les normes de sécurité de l'internet bien établies. Le présent règlement, qui s'applique à tous les matériels et logiciels connectables, vise également à faciliter le respect, par les fournisseurs d'infrastructures numériques, des exigences de la chaîne d'approvisionnement en vertu de la [directive XXX/XXXX (SRI 2)], en veillant à ce que les produits comportant des éléments numériques qu'ils utilisent pour la fourniture de leurs services soient développés de manière sécurisée et à ce qu'ils aient accès à des mises à jour de sécurité en temps utile pour ces produits.

(12) Le règlement (UE) 2017/745 du Parlement européen et du Conseil[7] établit des règles relatives aux dispositifs médicaux et le règlement (UE) 2017/746 du Parlement européen et du Conseil[8] définit des règles relatives aux dispositifs médicaux de diagnostic *in vitro*. Ces deux règlements traitent des risques de cybersécurité et suivent des approches particulières qui sont également abordées dans le présent règlement. Plus précisément, les règlements (UE) 2017/745 et (UE) 2017/746 établissent des exigences essentielles pour les dispositifs médicaux qui fonctionnent au moyen d'un système électronique ou sont eux-mêmes des logiciels. Certains logiciels non intégrés et l'approche du cycle de vie complet relèvent également du champ d'application de ces règlements. Ces exigences obligent les fabricants à développer et à fabriquer leurs produits en appliquant des principes de gestion des risques et en définissant des exigences concernant les mesures de sécurité informatique, ainsi que les procédures d'évaluation de la conformité correspondantes. En outre, des orientations spécifiques sur la cybersécurité des dispositifs médicaux sont en place depuis décembre 2019. Elles fournissent aux fabricants de dispositifs médicaux, notamment de dispositifs de diagnostic *in vitro*, des orientations quant à la manière de satisfaire à toutes les exigences essentielles pertinentes énoncées à l'annexe I de ces règlements en ce qui concerne la cybersécurité[9]. Les produits comportant des éléments numériques relevant de l'un ou l'autre de ces règlements ne devraient donc pas être soumis au présent règlement.

---

7 Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1).

8 Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic *in vitro* et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

9 MDCG 2019-16, approuvé par le groupe de coordination en matière de dispositifs médicaux (GCDM) institué par l'article 103 du règlement (UE) 2017/745.

(13) Le règlement (UE) 2019/2144 du Parlement européen et du Conseil[10] établit des exigences pour la réception par type des véhicules, ainsi que de leurs systèmes et composants, et introduit certaines exigences en matière de cybersécurité, notamment concernant le fonctionnement d'un système de gestion de cybersécurité certifié et les mises à jour logicielles. Il couvre entre autres les politiques et processus des organisations en matière de cyber-risques liés à l'ensemble du cycle de vie des véhicules, des équipements et des services, conformément aux réglementations des Nations unies applicables en matière de spécifications techniques et de cybersécurité[11], et prévoit des procédures spécifiques d'évaluation de la conformité. Dans le domaine de l'aviation, l'objectif principal du règlement (UE) 2018/1139 du Parlement européen et du Conseil[12] est d'établir et de maintenir un niveau uniforme élevé de sécurité dans l'aviation civile dans l'Union. Ce règlement crée un cadre pour les exigences essentielles en matière de navigabilité des produits, pièces et équipements aéronautiques, y compris les logiciels, qui tiennent compte des obligations de protection contre les menaces relatives à la sécurité de l'information. Les produits comportant des éléments numériques auxquels s'applique le règlement (UE) 2019/2144 et les produits certifiés conformément au règlement (UE) 2018/1139 ne sont donc pas soumis aux exigences essentielles et aux procédures d'évaluation de la conformité énoncées dans le présent règlement. Le processus de certification prévu par le règlement (UE) 2018/1139 garantit le niveau d'assurance visé par le présent règlement.

(14) Le présent règlement établit des règles horizontales de cybersécurité qui ne sont pas spécifiques aux secteurs ou à certains produits comportant des éléments numériques. Néanmoins, des règles sectorielles ou spécifiques aux produits pourraient être introduites au niveau de l'Union, établissant des exigences qui couvrent tout ou partie des risques auxquels s'appliquent les exigences essentielles établies par le présent règlement. Dans de tels cas, l'application du présent règlement aux produits comportant des éléments numériques relevant d'autres règles de l'Union établissant des exigences qui couvrent tout ou partie des risques auxquels s'appliquent les exigences essentielles énoncées à l'annexe I du présent règlement peut être limitée ou exclue lorsque cette limitation ou exclusion est compatible avec le cadre réglementaire global applicable à ces produits et lorsque les règles sectorielles permettent d'atteindre un niveau de protection identique à celui prévu par le présent règlement. La

---

10 Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) nº 78/2009, (CE) nº 79/2009 et (CE) nº 661/2009 du Parlement européen et du Conseil et les règlements (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010, (UE) nº 1008/2010, (UE) nº 1009/2010, (UE) nº 19/2011, (UE) nº 109/2011, (UE) nº 458/2011, (UE) nº 65/2012, (UE) nº 130/2012, (UE) nº 347/2012, (UE) nº 351/2012, (UE) nº 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

11 Règlement ONU nº 155 – Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité [2021/387].

12 Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) nº 2111/2005, (CE) nº 1008/2008, (UE) nº 996/2010, (UE) nº 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) nº 552/2004 et (CE) nº 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) nº 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

Commission est habilitée à adopter des actes délégués pour modifier le présent règlement en identifiant de tels produits et règles. S'agissant de la législation de l'Union en vigueur à laquelle ces limitations ou exclusions devraient s'appliquer, le présent règlement contient des dispositions spécifiques visant à clarifier sa relation avec cette législation de l'Union.

(15) Le règlement délégué (UE) 2022/30 précise que les exigences essentielles énoncées à l'article 3, paragraphe 3, point d) (dommages au réseau et mauvaise utilisation des ressources du réseau), point e) (données à caractère personnel et vie privée) et point f) (fraude), de la directive 2014/53/UE s'appliquent à certains équipements radio. La [décision d'exécution (UE) XXX/2022 de la Commission relative à une demande de normalisation adressée aux organisations européennes de normalisation] fixe des exigences pour l'élaboration de normes spécifiques précisant la manière dont ces trois exigences essentielles doivent être traitées. Les exigences essentielles établies par le présent règlement comprennent tous les éléments des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE. En outre, les exigences essentielles énoncées dans le présent règlement sont alignées sur les objectifs des exigences relatives à des normes spécifiques incluses dans cette demande de normalisation. Par conséquent, si la Commission abroge ou modifie le règlement délégué (UE) 2022/30 de sorte qu'il cesse de s'appliquer à certains produits soumis au présent règlement, la Commission et les organisations européennes de normalisation devraient tenir compte des travaux de normalisation menés dans le cadre de la décision d'exécution C(2022)5637 de la Commission relative à une demande de normalisation du règlement délégué RED [règlement (UE) 2022/30] lors de l'élaboration et du développement de normes harmonisées visant à faciliter la mise en œuvre du présent règlement.

(16) La directive 85/374/CEE[13] complète le présent règlement. Cette directive établit des règles en matière de responsabilité du fait des produits défectueux afin que les victimes puissent demander réparation lorsqu'un dommage a été causé par de tels produits. Elle établit le principe selon lequel le fabricant d'un produit est responsable des dommages causés par un défaut de sécurité de son produit, indépendamment de la faute («responsabilité objective»). Lorsqu'un tel défaut de sécurité consiste en un manque de mises à jour de sécurité après la mise sur le marché du produit, et qu'il en résulte des dommages, la responsabilité du fabricant pourrait être engagée. Le présent règlement devrait faire obligation aux fabricants de fournir de telles mises à jour de sécurité.

(17) Le présent règlement devrait s'appliquer sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil[14], et notamment de ses dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. De telles opérations pourraient être intégrées dans un

[13] Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux (JO L 210 du 7.8.1985).

[14] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

produit comportant des éléments numériques. La protection des données dès la conception et par défaut ainsi que la cybersécurité en général sont des éléments clés du règlement (UE) 2016/679. En protégeant les consommateurs et les organisations contre les risques de cybersécurité, les exigences essentielles en matière de cybersécurité énoncées dans le présent règlement doivent également contribuer à renforcer la protection des données à caractère personnel et de la vie privée des personnes. Des synergies en matière de normalisation et de certification sur les aspects de la cybersécurité devraient être envisagées dans le cadre de la coopération entre la Commission, les organisations européennes de normalisation, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le comité européen de la protection des données institué par le règlement (UE) 2016/679 et les autorités nationales de contrôle de la protection des données. Il convient également de créer des synergies entre le présent règlement et la législation de l'Union en matière de protection des données dans le domaine de la surveillance du marché et du contrôle de l'application. À cette fin, les autorités nationales de surveillance du marché désignées en vertu du présent règlement devraient coopérer avec les autorités chargées de surveiller l'application de la législation de l'Union en matière de protection des données. Ces dernières devraient également avoir accès aux informations nécessaires à l'accomplissement de leurs tâches.

(18) Dans la mesure où leurs produits relèvent du champ d'application du présent règlement, les émetteurs de portefeuilles européens d'identité numérique visés à l'article [article 6 *bis*, paragraphe 2, du règlement (UE) nº 910/2014, tel que modifié par la proposition de règlement modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique] devraient se conformer à la fois aux exigences essentielles horizontales établies par le présent règlement et aux exigences de sécurité spécifiques établies par l'article [article 6 *bis* du règlement (UE) nº 910/2014, tel que modifié par la proposition de règlement modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen pour une identité numérique]. Afin de faciliter la conformité, les émetteurs de portefeuilles devraient pouvoir démontrer la conformité des portefeuilles européens d'identité numérique aux exigences énoncées respectivement dans les deux actes en certifiant leurs produits dans le cadre d'un schéma européen de certification de cybersécurité établi en vertu du règlement (UE) 2019/881 et pour lequel la Commission a établi, par acte d'exécution, une présomption de conformité pour le présent règlement, dans la mesure où le certificat, ou des parties de celui-ci, couvre ces exigences.

(19) Certaines tâches prévues par le présent règlement devraient être exécutées par l'ENISA, conformément à l'article 3, paragraphe 2, du règlement (UE) 2019/881. L'ENISA devrait notamment recevoir des notifications des fabricants concernant les vulnérabilités activement exploitées des produits comportant des éléments numériques ainsi que les incidents ayant une incidence sur la sécurité de ces produits. L'ENISA devrait également transmettre ces notifications aux centres de réponse aux incidents de sécurité informatique (CSIRT) concernés ou, respectivement, aux points de contact uniques pertinents des États membres désignés conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)], et informer les autorités de surveillance du marché concernées de la vulnérabilité notifiée. Sur la base des informations qu'elle recueille, l'ENISA devrait préparer un rapport technique bisannuel sur les tendances émergentes concernant les risques de cybersécurité dans les produits comportant des éléments numériques et le soumettre au groupe de coopération visé dans la directive [directive XXX/XXXX (SRI 2)]. En outre, eu égard à son expertise et à son

mandat, l'ENISA devrait être en mesure de soutenir le processus de mise en œuvre du présent règlement. Elle devrait notamment pouvoir proposer des activités conjointes à mener par les autorités de surveillance du marché sur la base d'indications ou d'informations concernant une non-conformité potentielle au présent règlement, dans plusieurs États membres, de produits comportant des éléments numériques ou recenser les catégories de produits pour lesquelles des actions de contrôle coordonnées simultanées devraient être organisées. Dans des circonstances exceptionnelles, à la demande de la Commission, l'ENISA devrait être en mesure de procéder à des évaluations portant sur des produits comportant des éléments numériques spécifiques qui présentent un risque de cybersécurité important, lorsqu'une intervention immédiate est nécessaire pour préserver le bon fonctionnement du marché intérieur.

(20) Le marquage CE devrait être apposé sur les produits comportant des éléments numériques pour indiquer leur conformité avec le présent règlement, afin qu'ils puissent circuler librement dans le marché intérieur. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché de produits comportant des éléments numériques qui satisfont aux exigences fixées dans le présent règlement et portent le marquage CE.

(21) Afin de garantir que les fabricants puissent mettre à disposition des logiciels à des fins d'essai avant de soumettre leurs produits à une évaluation de la conformité, les États membres ne devraient pas empêcher la mise à disposition de logiciels inachevés, tels que des versions alpha, des versions beta ou des versions candidates à la diffusion, pour autant que la version en question ne soit mise à disposition que pendant le temps nécessaire pour la tester et recueillir des commentaires. Les fabricants devraient veiller à ce que les logiciels mis à disposition dans ces conditions ne soient diffusés qu'après une évaluation des risques et soient conformes, dans la mesure du possible, aux exigences de sécurité relatives aux propriétés des produits comportant des éléments numériques imposées par le présent règlement. Les fabricants devraient également mettre en œuvre les exigences de gestion des vulnérabilités dans la mesure du possible. Les fabricants ne devraient pas forcer les utilisateurs à passer à des versions uniquement diffusées à des fins d'essais.

(22) Afin de garantir que les produits comportant des éléments numériques, lorsqu'ils sont mis sur le marché, ne présentent pas de risques de cybersécurité pour les personnes et les organisations, il convient de fixer des exigences essentielles pour ces produits. Lorsque ces produits sont modifiés ultérieurement, par des moyens physiques ou numériques, d'une manière qui n'est pas prévue par le fabricant et qui peut impliquer qu'ils ne satisfont plus aux exigences essentielles pertinentes, la modification devrait être considérée comme substantielle. Par exemple, les mises à jour de logiciels ou les réparations pourraient être assimilées à des opérations d'entretien pour autant qu'elles ne modifient pas un produit déjà mis sur le marché d'une manière qui soit susceptible d'en compromettre la conformité aux exigences applicables ou de modifier l'utilisation prévue pour laquelle le produit a été évalué. Comme c'est le cas pour les réparations ou modifications physiques, un produit comportant des éléments numériques doit être considéré comme substantiellement modifié par une modification logicielle lorsque la mise à jour du logiciel modifie les fonctions, le type ou les performances initialement prévues du produit et que ces modifications n'ont pas été prévues dans l'évaluation initiale des risques, ou lorsque la nature du danger a changé ou que le niveau de risque a augmenté en raison de la mise à jour du logiciel.

(23) Conformément à la notion généralement établie de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, chaque fois que se produit

une modification substantielle de nature à affecter la conformité d'un produit au présent règlement ou lorsque l'utilisation prévue de ce produit change, il convient de vérifier la conformité du produit comportant des éléments numériques et, le cas échéant, de le soumettre à une nouvelle évaluation de la conformité. Le cas échéant, si le fabricant a recours à une évaluation de la conformité faisant intervenir un tiers, les modifications susceptibles d'entraîner des modifications substantielles devraient être notifiées à ce dernier.

(24) La remise à neuf, l'entretien et la réparation d'un produit comportant des éléments numériques, tels que définis dans le règlement [règlement sur l'écoconception], n'entraînent pas nécessairement une modification substantielle du produit, par exemple si l'utilisation et les fonctionnalités prévues ne sont pas modifiées et que le niveau de risque demeure inchangé. Toutefois, la mise à niveau d'un produit par le fabricant pourrait entraîner des modifications dans la conception et le développement du produit et donc avoir une incidence sur son utilisation prévue et sa conformité aux exigences énoncées dans le présent règlement.

(25) Les produits comportant des éléments numériques devraient être considérés comme critiques si l'exploitation de vulnérabilités potentielles de cybersécurité dans ces produits peut avoir de graves répercussions en raison, entre autres, de la fonctionnalité liée à la cybersécurité ou de l'utilisation prévue. En particulier, les vulnérabilités de produits comportant des éléments numériques qui ont une fonctionnalité liée à la cybersécurité, tels que les éléments sécurisés, peuvent provoquer une propagation des problèmes de sécurité tout au long de la chaîne d'approvisionnement. La gravité des effets d'un incident de cybersécurité peut également augmenter selon l'utilisation prévue du produit, par exemple s'il est employé dans un cadre industriel ou dans le contexte d'une entité essentielle du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)], ou pour l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel.

(26) Les produits critiques comportant des éléments numériques devraient être soumis à des procédures d'évaluation de la conformité plus strictes, tout en conservant une approche proportionnée. À cette fin, les produits critiques comportant des éléments numériques devraient être divisés en deux catégories, reflétant le niveau de risque de cybersécurité lié à ces catégories de produits. Un cyberincident potentiel impliquant des produits de classe II pourrait avoir des conséquences négatives plus importantes qu'un incident impliquant des produits de classe I, par exemple en raison de la nature de leur fonction liée à la cybersécurité ou de leur utilisation prévue dans des environnements sensibles, et ces produits devraient donc faire l'objet d'une procédure d'évaluation de la conformité plus stricte.

(27) Les catégories de produits critiques comportant des éléments numériques figurant à l'annexe III du présent règlement devraient être considérées comme regroupant les produits possédant les fonctionnalités essentielles du type figurant à l'annexe III du présent règlement. Par exemple, l'annexe III du présent règlement énumère les produits qui sont définis par leur fonctionnalité de base comme des microprocesseurs à usage général de classe II. Par conséquent, les microprocesseurs à usage général sont soumis à une évaluation de conformité obligatoire par un tiers. Ce n'est pas le cas pour d'autres produits qui ne sont pas explicitement mentionnés à l'annexe III du présent règlement et qui peuvent intégrer un microprocesseur à usage général. La Commission devrait adopter des actes délégués [au plus tard douze mois après l'entrée en vigueur du présent règlement] pour préciser les définitions des catégories de produits relevant des classes I et II, telles qu'elles figurent à l'annexe III.

(28) Le présent règlement aborde les risques de cybersécurité de manière ciblée. Les produits comportant des éléments numériques peuvent toutefois présenter d'autres risques pour la sécurité qui ne sont pas liés à la cybersécurité. Ces risques devraient continuer à être réglementés par d'autres actes législatifs pertinents de l'Union relatifs aux produits. Si aucune autre législation d'harmonisation de l'Union ne leur est applicable, ils devraient être soumis au règlement [règlement relatif à la sécurité générale des produits]. Par conséquent, compte tenu du caractère ciblé du présent règlement, par dérogation à l'article 2, paragraphe 1, troisième alinéa, point b), du règlement [règlement relatif à la sécurité générale des produits], le chapitre III, section 1, les chapitres V et VII, et les chapitres IX à XI du règlement [règlement relatif à la sécurité générale des produits] devraient s'appliquer aux produits comportant des éléments numériques en ce qui concerne les risques pour la sécurité qui ne sont pas couverts par le présent règlement, si ces produits ne sont pas soumis à des exigences spécifiques imposées par une autre législation d'harmonisation de l'Union au sens de l'[article 3, point 25), du règlement relatif à la sécurité générale des produits].

(29) Les produits comportant des éléments numériques classés comme systèmes d'IA à haut risque conformément à l'article 6 du règlement[15] [règlement sur l'IA] qui relèvent du champ d'application du présent règlement devraient satisfaire aux exigences essentielles énoncées dans celui-ci. Lorsque ces systèmes d'IA à haut risque satisfont aux exigences essentielles du présent règlement, ils devraient être réputés conformes aux exigences en matière de cybersécurité énoncées à l'article [article 15] du règlement [règlement sur l'IA], dans la mesure où ces exigences sont couvertes par la déclaration UE de conformité, ou par certaines parties de celle-ci, délivrée en vertu du présent règlement. S'agissant des procédures d'évaluation de la conformité relatives aux exigences essentielles de cybersécurité d'un produit comportant des éléments numériques couvert par le présent règlement et classé comme système d'IA à haut risque, les dispositions pertinentes de l'article 43 du règlement [règlement sur l'IA] devraient de manière générale s'appliquer en lieu et place des dispositions correspondantes du présent règlement. Toutefois, l'application de cette règle ne devrait pas entraîner de réduction du niveau d'assurance nécessaire pour les produits critiques comportant des éléments numériques couverts par le présent règlement. Par conséquent, par dérogation à cette règle, les systèmes d'IA à haut risque qui relèvent du champ d'application du règlement [règlement sur l'IA] et sont également considérés comme des produits critiques comportant des éléments numériques en vertu du présent règlement et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI du règlement [règlement sur l'IA] devraient être soumis aux dispositions du présent règlement relatives à l'évaluation de la conformité en ce qui concerne les exigences essentielles énoncées dans celui-ci. Dans ce cas, pour tous les autres aspects couverts par le règlement [règlement sur l'IA], les dispositions correspondantes relatives à l'évaluation de la conformité fondée sur le contrôle interne énoncées à l'annexe VI du règlement [règlement sur IA] devraient s'appliquer.

(30) Les machines et produits connexes relevant du champ d'application du règlement [proposition de règlement sur les machines et produits connexes] qui sont des produits comportant des éléments numériques au sens du présent règlement et pour lesquelles une déclaration de conformité a été délivrée sur la base du présent règlement devraient

[15] Règlement [le règlement sur l'IA].

être considérés comme conformes aux exigences essentielles de santé et de sécurité énoncées à l'[annexe III, sections 1.1.9 et 1.2.1] du règlement [proposition de règlement sur les machines], en ce qui concerne la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de contrôle, pour autant que la conformité à ces exigences soit démontrée par la déclaration UE de conformité délivrée au titre du présent règlement.

(31) Le règlement [proposition de règlement relatif à l'espace européen des données de santé] complète les exigences essentielles énoncées dans le présent règlement. Les systèmes de dossiers médicaux électroniques («systèmes DME») relevant du champ d'application du règlement [proposition de règlement relatif à l'espace européen des données de santé] qui sont des produits comportant des éléments numériques au sens du présent règlement devraient donc également satisfaire aux exigences essentielles énoncées dans le présent règlement. Leurs fabricants devraient démontrer la conformité comme l'exige le règlement [proposition de règlement relatif à l'espace européen des données de santé]. Pour faciliter la mise en conformité, les fabricants peuvent établir une documentation technique unique contenant les éléments requis par les deux actes législatifs. Étant donné que le présent règlement ne couvre pas le SaaS en tant que tel, les systèmes DME proposés par l'intermédiaire du modèle de licence et de livraison du SaaS ne relèvent pas du champ d'application du présent règlement. De même, les systèmes DME mis au point et utilisés en interne ne relèvent pas du champ d'application du présent règlement, car ils ne sont pas mis sur le marché.

(32) Afin de garantir la sécurité des produits comportant des éléments numériques au moment de leur mise sur le marché et tout au long de leur cycle de vie, il est nécessaire de définir des exigences essentielles en matière de gestion de la vulnérabilité et des exigences essentielles en matière de cybersécurité concernant les propriétés des produits comportant des éléments numériques. Les fabricants devraient se conformer à toutes les exigences essentielles liées à la gestion des vulnérabilités et veiller à ce que tous leurs produits soient livrés sans aucune vulnérabilité exploitable connue, mais ils devraient en outre déterminer les autres exigences essentielles liées aux propriétés du produit pertinentes pour le type de produit concerné. À cette fin, les fabricants devraient entreprendre une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques afin de recenser les risques et les exigences essentielles pertinents et d'appliquer de manière appropriée des normes harmonisées ou des spécifications communes appropriées.

(33) Afin d'améliorer la sécurité des produits comportant des éléments numériques mis sur le marché intérieur, il est nécessaire d'établir des exigences essentielles. Ces exigences essentielles ne devraient pas porter atteinte aux évaluations coordonnées des risques de l'Union portant sur les chaînes d'approvisionnement critiques et établies par l'[article X] de la [directive XXX/XXXX (SRI 2)][16], qui tiennent compte à la fois des facteurs de risque techniques et, le cas échéant, non techniques, tels que l'influence indue d'un pays tiers sur les fournisseurs. En outre, elles devraient s'exercer sans préjudice des prérogatives des États membres d'établir des exigences supplémentaires qui tiennent compte de facteurs non techniques afin de garantir un niveau élevé de résilience, y compris celles définies dans la recommandation (UE) 2019/534, dans l'évaluation coordonnée des risques de la sécurité des réseaux 5G à l'échelle de

[16] Directive XXX du Parlement européen et du Conseil du [date] [concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (JO L xx, date, p. x)].

l'Union et dans la boîte à outils de l'UE sur la cybersécurité 5G convenue par le groupe de coopération SRI conformément à la [directive XXX/XXXX (SRI 2)].

(34) Afin de garantir que les CSIRT nationaux et le guichet unique désigné conformément à l'article [article X] de la directive [directive XX/XXXX (SRI 2)] reçoivent les informations nécessaires à l'accomplissement de leurs tâches et à l'élévation du niveau global de cybersécurité des entités essentielles et importantes, et afin de garantir le fonctionnement efficace des autorités de surveillance du marché, les fabricants de produits comportant des éléments numériques devraient notifier à l'ENISA les vulnérabilités activement exploitées. Étant donné que la plupart des produits comportant des éléments numériques sont commercialisés sur l'ensemble du marché intérieur, toute vulnérabilité exploitée dans un de ces produits devrait être considérée comme une menace pour le fonctionnement du marché intérieur. Les fabricants devraient également envisager de communiquer les vulnérabilités fixes à la base de données européenne sur les vulnérabilités établie en vertu de la directive [directive XX/XXXX (SRI 2)] et gérée par l'ENISA ou à toute autre base de données sur les vulnérabilités accessible au public.

(35) Les fabricants devraient également signaler à l'ENISA tout incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques. Nonobstant les obligations de signalement d'incidents prévues par la directive [directive XXX/XXXX (SRI 2)] pour les entités essentielles et importantes, il est essentiel que l'ENISA, les guichets uniques désignés par les États membres conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] et les autorités de surveillance du marché reçoivent des informations des fabricants de produits comportant des éléments numériques leur permettant d'évaluer la sécurité de ces produits. Afin de garantir que les utilisateurs puissent réagir rapidement aux incidents ayant un impact sur la sécurité de leurs produits comportant des éléments numériques, les fabricants devraient également informer leurs utilisateurs de tout incident de ce type et, le cas échéant, de toute mesure corrective que les utilisateurs peuvent mettre en œuvre pour atténuer l'impact de l'incident, par exemple en publiant des informations pertinentes sur leur site internet ou, lorsque le fabricant est en mesure de contacter les utilisateurs et lorsque les risques le justifient, en contactant directement les utilisateurs.

(36) Les fabricants de produits comportant des éléments numériques devraient mettre en place des politiques de divulgation coordonnée des vulnérabilités afin de faciliter le signalement desdites vulnérabilités par des personnes ou des entités. Toute politique de divulgation coordonnée des vulnérabilités devrait définir un processus structuré dans lequel les vulnérabilités sont signalées à un fabricant de manière à lui donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. Étant donné que les informations sur les vulnérabilités exploitables dans les produits comportant des éléments numériques largement utilisés peuvent être vendues à des prix élevés sur le marché noir, les fabricants de ces produits devraient pouvoir utiliser, dans le cadre de leurs politiques de divulgation coordonnée des vulnérabilités, des programmes visant à encourager le signalement des vulnérabilités en veillant à ce que les personnes ou les entités soient reconnues et récompensées pour leurs efforts (dans le cadre de programmes dits de «prime aux bogues»).

(37) Afin de faciliter l'analyse de la vulnérabilité, les fabricants devraient répertorier et documenter les composants contenus dans les produits comportant des éléments numériques, notamment en établissant une nomenclature des logiciels. Une

nomenclature des logiciels peut fournir à ceux qui fabriquent, achètent et exploitent des logiciels des informations de nature à améliorer leur compréhension de la chaîne d'approvisionnement, ce qui présente de multiples avantages. Elle peut plus particulièrement aider les fabricants et les utilisateurs à suivre les vulnérabilités et les risques émergents nouvellement apparus. Il est particulièrement important pour les fabricants de s'assurer que leurs produits ne contiennent pas de composants vulnérables développés par des tiers.

(38) Afin de faciliter l'évaluation de la conformité aux exigences établies par le présent règlement, il convient de prévoir une présomption de conformité pour les produits dont les éléments numériques sont conformes à des normes harmonisées, qui traduisent les exigences essentielles du présent règlement en spécifications techniques détaillées et sont adoptées conformément au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[17]. Le règlement (UE) nº 1025/2012 prévoit une procédure pour la formulation d'objections à l'encontre de normes harmonisées lorsque celles-ci ne satisfont pas pleinement aux exigences du présent règlement.

(39) Le règlement (UE) 2019/881 établit un cadre européen de certification volontaire de cybersécurité pour les produits, processus et services TIC. Les schémas européens de certification de cybersécurité peuvent couvrir des produits comportant des éléments numériques relevant du présent règlement. Le présent règlement devrait créer des synergies avec le règlement (UE) 2019/881. Afin de faciliter l'évaluation de la conformité aux exigences énoncées dans le présent règlement, les produits comportant des éléments numériques qui sont certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 et qui ont été désignés par la Commission dans un acte d'exécution sont présumés conformes aux exigences essentielles du présent règlement pour autant que le certificat ou la déclaration de conformité ou des parties de ceux-ci couvrent ces exigences. La nécessité de nouveaux schémas européens de certification de cybersécurité pour les produits comportant des éléments numériques devrait être évaluée à la lumière du présent règlement. Ces futurs schémas européens de certification de cybersécurité, destinés à couvrir les produits comportant des éléments numériques, devraient tenir compte des exigences essentielles énoncées dans le présent règlement et faciliter le respect de celui-ci. Il convient d'habiliter la Commission à préciser, au moyen d'actes d'exécution, les schémas européens de certification de cybersécurité qui peuvent être utilisés pour démontrer la conformité aux exigences essentielles énoncées dans le présent règlement. En outre, afin d'éviter une charge administrative excessive pour les fabricants, le cas échéant, la Commission devrait préciser si un certificat de cybersécurité délivré dans le cadre de ces schémas européens de certification élimine l'obligation pour les fabricants de faire procéder à une évaluation de conformité par un tiers conformément au présent règlement pour les exigences correspondantes.

(40) Dès l'entrée en vigueur de l'acte d'exécution établissant le [règlement d'exécution (UE)°.../... de la Commission du XXX relatif au schéma européen de certification de cybersécurité fondé sur des critères communs] (CCUE) portant sur les

[17] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

produits matériels couverts par le présent règlement, tels que les modules de sécurité matériels et les microprocesseurs, la Commission peut préciser, au moyen d'un acte d'exécution, comment la certification CCUE crée une présomption de conformité aux exigences essentielles visées à l'annexe I du présent règlement ou à certaines de ses parties. En outre, cet acte d'exécution peut définir comment un certificat délivré au titre de la CCUE élimine l'obligation pour les fabricants d'avoir recours à une évaluation par un tiers, comme l'exige le présent règlement, pour les exigences correspondantes.

(41) En l'absence de normes harmonisées ou lorsque les normes harmonisées ne répondent pas suffisamment aux exigences essentielles du présent règlement, la Commission devrait pouvoir adopter des spécifications communes au moyen d'actes d'exécution. Les raisons de l'élaboration de telles spécifications communes, en lieu et place de normes harmonisées, pourraient inclure un refus de la demande de normalisation par l'une des organisations européennes de normalisation, des retards indus dans la mise en place de normes harmonisées appropriées ou un non-respect des exigences du présent règlement ou d'une demande de la Commission. Afin de faciliter l'évaluation de la conformité aux exigences essentielles prévues par le présent règlement, il convient d'établir une présomption de conformité pour les produits comportant des éléments numériques répondant aux spécifications communes adoptées par la Commission en vertu du présent règlement, aux fins de l'expression de spécifications techniques détaillées sur la base de ces exigences.

(42) Il y a lieu que les fabricants établissent une déclaration UE de conformité afin de fournir les informations requises par le présent règlement concernant la conformité des produits comportant des éléments numériques aux exigences prévues par le présent règlement et, le cas échéant, par d'autres législations d'harmonisation de l'Union applicables. Les fabricants peuvent également être tenus d'établir une déclaration UE de conformité en vertu d'une autre législation de l'Union. Pour garantir un accès effectif aux informations à des fins de surveillance du marché, une déclaration UE de conformité unique attestant le respect de tous les actes de l'Union devrait être établie. Pour réduire la charge administrative pesant sur les opérateurs économiques, cette déclaration UE de conformité unique devrait pouvoir être un dossier composé des différentes déclarations de conformité pertinentes.

(43) Le marquage CE, qui matérialise la conformité d'un produit, est le résultat visible de tout un processus englobant l'évaluation de conformité au sens large. Le règlement (CE) nº 765/2008 du Parlement européen et du Conseil[18] établit les principes généraux régissant le marquage CE. Les règles régissant l'apposition du marquage CE sur les produits comportant des éléments numériques devraient être définies par le présent règlement. Le marquage CE devrait être le seul marquage garantissant la conformité d'un produit comportant des éléments numériques aux exigences du présent règlement.

(44) Afin de permettre aux opérateurs économiques de démontrer qu'ils respectent les exigences essentielles énoncées dans le présent règlement et aux autorités de surveillance du marché de s'assurer que les produits comportant des éléments numériques mis à disposition sur le marché sont conformes à ces exigences, il est

[18] Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) nº 339/93 (JO L 218 du 13.8.2008, p. 30).

nécessaire de prévoir des procédures d'évaluation de la conformité. La décision nº 768/2008/CE du Parlement européen et du Conseil[19] établit des modules pour l'évaluation de la conformité, dont les procédures sont proportionnées au risque encouru et au niveau de sécurité requis. Afin d'assurer la cohérence entre les secteurs et d'éviter une multiplication de variantes ad hoc, des procédures adéquates ont été fondées sur ces modules afin de vérifier la conformité des produits comportant des éléments numériques aux exigences essentielles énoncées dans le présent règlement. Les procédures d'évaluation de la conformité devraient examiner et vérifier les exigences relatives aux produits et aux processus couvrant l'ensemble du cycle de vie des produits comportant des éléments numériques, y compris la planification, la conception, le développement ou la production, les essais et l'entretien du produit.

(45) En règle générale, l'évaluation de la conformité des produits comportant des éléments numériques devrait être effectuée par le fabricant sous sa propre responsabilité, conformément à la procédure fondée sur le module A de la décision 768/2008/CE. Le fabricant devrait conserver la possibilité de choisir une procédure d'évaluation de la conformité plus stricte faisant intervenir un tiers. Si le produit est classé comme produit critique de classe I, une assurance supplémentaire est requise pour démontrer la conformité aux exigences essentielles énoncées dans le présent règlement. Le fabricant devrait appliquer des normes harmonisées, des spécifications communes ou des schémas de certification de cybersécurité au titre du règlement (UE) 2019/881, répertoriés par la Commission dans un acte d'exécution, s'il souhaite effectuer l'évaluation de la conformité sous sa propre responsabilité (module A). Si le fabricant n'applique pas ces normes harmonisées, spécifications communes ou schémas de certification de cybersécurité, il devrait se soumettre à une évaluation de la conformité par un tiers. Compte tenu de la charge administrative pesant sur les fabricants et du fait que la cybersécurité joue un rôle important dans la phase de conception et de développement des produits matériels et immatériels comportant des éléments numériques, les procédures d'évaluation de la conformité fondées respectivement sur les modules B+C ou H de la décision 768/2008/CE ont été retenues comme étant les plus appropriées pour évaluer de manière proportionnée et efficace la conformité des produits critiques comportant des éléments numériques. Le fabricant qui fait procéder à l'évaluation de conformité par un tiers peut choisir la procédure qui convient le mieux à son processus de conception et de production. Compte tenu du risque de cybersécurité encore plus grand lié à l'utilisation de produits classés comme produits critiques de classe II, l'évaluation de la conformité de ces produits devrait toujours prévoir l'intervention d'un tiers.

(46) Si la création de produits matériels comportant des éléments numériques nécessite généralement des efforts substantiels de la part des fabricants tout au long des phases de conception, de développement et de production, la création de produits comportant des éléments numériques sous la forme de logiciels se concentre presque exclusivement sur la conception et le développement, tandis que la phase de production joue un rôle mineur. Néanmoins, dans de nombreux cas, les produits logiciels doivent encore être compilés, construits, conditionnés, mis à disposition pour téléchargement ou copiés sur des supports physiques avant leur mise sur le marché. Ces activités devraient être assimilées à des activités de production lors de

[19] Décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

l'application des modules d'évaluation pertinents pour vérifier la conformité du produit aux exigences essentielles du présent règlement au cours des phases de conception, de développement et de production.

(47) Afin de permettre la réalisation d'une évaluation de la conformité par un tiers pour des produits comportant des éléments numériques, les autorités nationales notifiantes devraient notifier les organismes d'évaluation de la conformité à la Commission et aux autres États membres, pour autant qu'ils respectent un ensemble d'exigences, notamment en matière d'indépendance, de compétence et d'absence de conflits d'intérêts.

(48) Afin d'assurer un niveau de qualité homogène des évaluations de la conformité de produits comportant des éléments numériques, il est également nécessaire de définir les exigences auxquelles doivent satisfaire les autorités notifiantes et les autres organismes qui participent à l'évaluation, à la notification et à la surveillance des organismes notifiés. Le système défini dans le présent règlement devrait être complété par le système d'accréditation prévu dans le règlement (CE) nº 765/2008. Dans la mesure où l'accréditation constitue un moyen essentiel pour vérifier la compétence des organismes d'évaluation de la conformité, il y a lieu d'y avoir également recours aux fins de la notification.

(49) L'accréditation organisée de manière transparente, ainsi que le prévoit le règlement (CE) nº 765/2008 pour assurer le niveau nécessaire de confiance dans les certificats de conformité, devrait être considérée par les autorités publiques nationales dans l'ensemble de l'Union comme le moyen privilégié de démontrer la compétence technique des organismes d'évaluation de la conformité. Cependant, les autorités nationales peuvent estimer qu'elles disposent des moyens appropriés pour procéder elles-mêmes à cette évaluation. Dans ce cas, afin de garantir le niveau suffisant de crédibilité des évaluations réalisées par d'autres autorités nationales, elles devraient fournir à la Commission et aux autres États membres les preuves documentaires nécessaires démontrant que les organismes d'évaluation de la conformité qui font l'objet de ladite évaluation satisfont aux exigences réglementaires pertinentes.

(50) Les organismes d'évaluation de la conformité sous-traitent fréquemment une partie de leurs activités liées à l'évaluation de la conformité, ou ont recours à une filiale. Afin de préserver le niveau de protection requis pour les produits comprenant des éléments numériques destinés à être mises sur le marché, il est primordial que les sous-traitants et les filiales qui réalisent l'évaluation de la conformité respectent les mêmes exigences que les organismes notifiés pour ce qui est de la réalisation des tâches d'évaluation de la conformité.

(51) L'autorité notifiante devrait envoyer la notification d'un organisme d'évaluation de la conformité à la Commission et aux autres États membres par l'intermédiaire du système d'information NANDO (New Approach Notified and Designated Organisations). Le système NANDO est l'outil de notification électronique développé et géré par la Commission, où une liste de tous les organismes notifiés peut être trouvée.

(52) Étant donné que les organismes notifiés peuvent offrir leurs services dans l'ensemble de l'Union, il convient de donner aux autres États membres et à la Commission la possibilité de soulever des objections à l'égard d'un organisme notifié. Il est donc important de prévoir une période pendant laquelle d'éventuels doutes ou inquiétudes quant à la compétence d'organismes d'évaluation de la conformité peuvent être levés, avant que ceux-ci ne débutent leurs activités en tant qu'organismes notifiés.

(53) Pour des raisons de compétitivité, il est essentiel que les organismes notifiés appliquent les procédures d'évaluation de la conformité sans imposer une charge inutile aux opérateurs économiques. Pour les mêmes raisons et afin de garantir l'égalité de traitement des opérateurs économiques, il y a lieu de veiller à une application technique cohérente desdites procédures. La meilleure manière d'atteindre cet objectif serait probablement d'assurer une coordination et une coopération appropriées entre les organismes notifiés.

(54) La surveillance du marché est un outil essentiel pour assurer l'application correcte et uniforme de la législation de l'Union. Il convient dès lors de mettre en place le cadre juridique dans lequel la surveillance du marché pourra être effectuée de manière appropriée. Les règles relatives à la surveillance du marché de l'Union et au contrôle des produits entrant sur le marché de l'Union prévues par le règlement (UE) 2019/1020 du Parlement européen et du Conseil[20] s'appliquent aux produits comportant des éléments numériques couverts par le présent règlement.

(55) Conformément au règlement (UE) 2019/1020, les autorités de surveillance du marché sont chargées de la surveillance du marché sur le territoire de l'État membre concerné. Le présent règlement ne devrait pas empêcher les États membres de choisir les autorités compétentes pour l'accomplissement de ces tâches. Chaque État membre devrait désigner une ou plusieurs autorités de surveillance du marché sur son territoire. Les États membres peuvent choisir de désigner toute autorité existante ou nouvelle pour agir en qualité d'autorité de surveillance du marché, y compris les autorités nationales compétentes visées à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] ou les autorités nationales de certification de cybersécurité désignées conformément à l'article 58 du règlement (UE) 2019/881. Les opérateurs économiques devraient coopérer pleinement avec les autorités de surveillance du marché et les autres autorités compétentes. Chaque État membre devrait communiquer à la Commission ainsi qu'aux autres États membres le nom de ses autorités de surveillance du marché et les domaines de compétence de chacune de ces autorités et veiller à ce qu'elles disposent des ressources et compétences nécessaires pour effectuer les tâches de surveillance qui leur incombent en vertu du présent règlement. Conformément à l'article 10, paragraphes 2 et 3, du règlement (UE) 2019/1020, chaque État membre devrait désigner un bureau de liaison unique chargé, entre autres, de représenter la position coordonnée des autorités de surveillance du marché et de contribuer à la coopération entre les autorités de surveillance du marché des différents États membres.

(56) Il convient de créer un groupe de coopération administrative (ADCO) spécifique pour l'application uniforme du présent règlement, conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. Cet ADCO devrait être composé de représentants des autorités de surveillance du marché nationales et, si nécessaire, de représentants des bureaux de liaison uniques. La Commission devrait soutenir et encourager la coopération entre les autorités de surveillance du marché par l'intermédiaire du réseau de l'Union pour la conformité des produits, institué sur la base de l'article 29 du règlement (UE) 2019/1020 et composé de représentants de chaque État membre, dont un représentant de chaque bureau de liaison unique visé à l'article 10 du règlement (UE) 2019/1020 et un expert national facultatif, les présidents

[20] Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011 (JO L 169 du 25.6.2019, p. 1).

des ADCO et des représentants de la Commission. La Commission devrait participer aux réunions du réseau, de ses sous-groupes et de l'ADCO concerné. Elle devrait également assister cet ADCO au moyen d'un secrétariat exécutif qui lui fournirait une assistance technique et logistique.

(57) Afin de garantir des mesures opportunes, proportionnées et efficaces en ce qui concerne les produits comportant des éléments numériques présentant un risque de cybersécurité important, il convient de prévoir une procédure de sauvegarde de l'Union en vertu de laquelle les parties intéressées sont informées des mesures qu'il est prévu de prendre à l'égard de ces produits. Cette procédure de sauvegarde devrait également permettre aux autorités de surveillance du marché, en coopération avec les opérateurs économiques concernés, d'agir, le cas échéant, à un stade plus précoce. Lorsqu'il y a accord entre les États membres et la Commission quant au bien-fondé d'une mesure prise par un État membre, une intervention de la Commission ne devrait plus être nécessaire, sauf dans les cas où la non-conformité peut être attribuée aux insuffisances d'une norme harmonisée.

(58) Dans certains cas, un produit comportant des éléments numériques conforme au présent règlement peut néanmoins présenter un risque de cybersécurité important ou présenter un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services offerts au moyen d'un système d'information électronique par des entités essentielles du type visé à l'[annexe I de la directive XXX/XXXX (SRI 2)] ou pour d'autres aspects de la protection de l'intérêt public. Il est donc nécessaire d'établir des règles permettant d'atténuer ces risques. En conséquence, les autorités de surveillance du marché devraient prendre des mesures pour demander à l'opérateur économique de veiller à ce que le produit ne présente plus ce risque, de le rappeler ou de le retirer, en fonction du risque. Dès qu'une autorité de surveillance du marché restreint ou interdit ainsi la libre circulation d'un produit, l'État membre devrait immédiatement informer la Commission et les autres États membres des mesures provisoires prises, en justifiant sa décision. Lorsqu'une autorité de surveillance du marché adopte de telles mesures à l'encontre de produits présentant un risque, la Commission devrait entamer sans retard des consultations avec les États membres et le ou les opérateurs économiques concernés et évaluer la mesure nationale. En fonction des résultats de cette évaluation, la Commission devrait décider si la mesure nationale est justifiée ou non. La Commission devrait adresser sa décision à tous les États membres et la communiquer immédiatement à ceux-ci ainsi qu'à l'opérateur ou aux opérateurs économiques concernés. Si la mesure est jugée justifiée, la Commission peut également envisager d'adopter des propositions de révision de la législation de l'Union concernée.

(59) Pour les produits comportant des éléments numériques présentant un risque de cybersécurité important, et lorsqu'il y a lieu de croire que ces produits ne sont pas conformes au présent règlement, ou pour les produits qui sont conformes au présent règlement, mais présentent d'autres risques importants, tels que des risques pour la santé ou la sécurité des personnes, les droits fondamentaux ou la fourniture de services par des entités essentielles du type visé à l'[annexe I de la directive XXX/XXXX (SRI 2)], la Commission peut demander à l'ENISA de procéder à une évaluation. Sur la base de cette évaluation, la Commission peut adopter, au moyen d'actes d'exécution, des mesures correctives ou restrictives au niveau de l'Union, y compris ordonner le retrait du marché ou le rappel des produits concernés, dans un délai raisonnable, proportionné à la nature du risque. La Commission ne peut recourir à une

telle intervention que dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur, et uniquement lorsqu'aucune mesure efficace n'a été prise par les autorités de surveillance pour remédier à la situation. De telles circonstances exceptionnelles peuvent être des situations d'urgence dans lesquelles, par exemple, un produit non conforme est largement mis à disposition par le fabricant dans plusieurs États membres, utilisé également dans des secteurs clés par des entités relevant du champ d'application de la [directive XXX/XXXX (SRI 2)], alors qu'il contient des vulnérabilités connues qui sont exploitées par des acteurs malveillants et pour lesquelles le fabricant ne met pas de correctifs à disposition. La Commission ne peut intervenir dans de telles situations d'urgence que pour la durée des circonstances exceptionnelles et si le non-respect du présent règlement ou les risques importants présentés persistent.

(60) Lorsqu'il existe des indices de non-respect du présent règlement dans plusieurs États membres, les autorités de surveillance du marché devraient pouvoir mener des activités conjointes avec d'autres autorités, en vue de vérifier la conformité et d'identifier les risques de cybersécurité des produits comportant des éléments numériques.

(61) Les actions de contrôle coordonnées simultanées (opérations «coup de balai») sont des mesures d'application spécifiques prises par les autorités de surveillance du marché qui peuvent renforcer davantage la sécurité des produits. Ces «coups de balai» devraient avoir lieu, en particulier, lorsque les tendances du marché, les plaintes des consommateurs ou d'autres indications suggèrent que certaines catégories de produits présentent souvent des risques de cybersécurité. L'ENISA devrait soumettre aux autorités de surveillance du marché des propositions concernant des catégories de produits pour lesquelles des actions simultanées pourraient être organisées, sur la base, entre autres, des notifications de vulnérabilités de produits et d'incidents qu'elle reçoit.

(62) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité en ce qui concerne les mises à jour de la liste des produits critiques figurant à l'annexe III et de préciser les définitions de ces catégories de produits. Il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article pour lui permettre de répertorier les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui atteignent un niveau de protection identique à celui du présent règlement, en précisant si une limitation ou une exclusion du champ d'application du présent règlement serait nécessaire ainsi que la portée de cette limitation, le cas échéant. Il convient également de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article en ce qui concerne la possibilité de rendre obligatoire la certification de certains produits hautement critiques comportant des éléments numériques sur la base des critères de criticité énoncés dans le présent règlement, ainsi que de préciser le contenu minimal de la déclaration UE de conformité; et de compléter les éléments à inclure dans la documentation technique. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux

légiférer»[21]. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

(63) Afin de garantir des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission, afin qu'elle puisse: spécifier le format et les éléments de la nomenclature des logiciels; préciser davantage le type d'informations, le format et la procédure des notifications relatives aux vulnérabilités activement exploitées et aux incidents soumises à l'ENISA par les fabricants; spécifier les schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 qui peuvent être utilisés pour démontrer la conformité aux exigences essentielles ou à des parties de celles-ci énoncées à l'annexe I du présent règlement; adopter des spécifications communes en ce qui concerne les exigences essentielles énoncées à l'annexe I; établir des spécifications techniques pour les pictogrammes ou toute autre marque liée à la sécurité des produits comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation; décider de mesures correctives ou restrictives au niveau de l'Union dans des circonstances exceptionnelles qui justifient une intervention immédiate afin de préserver le bon fonctionnement du marché intérieur. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[22].

(64) Afin de garantir une coopération constructive et en toute confiance entre les autorités de surveillance du marché au niveau de l'Union et au niveau national, toutes les parties intervenant dans l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans le cadre de l'exécution de leurs tâches.

(65) Afin de garantir une application efficace des obligations prévues par le présent règlement, chaque autorité de surveillance du marché devrait avoir le pouvoir d'imposer ou de demander l'imposition d'amendes administratives. Il convient donc d'établir des niveaux maximaux pour les amendes administratives à prévoir dans les législations nationales en cas de non-respect des obligations énoncées dans le présent règlement. Pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et, au minimum, celles explicitement établies dans le présent règlement, y compris la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour des infractions similaires. De telles caractéristiques peuvent être soit aggravantes, dans des situations où l'infraction commise par le même opérateur persiste sur le territoire d'autres États membres que celui où une amende administrative a déjà été infligée, soit atténuantes, en veillant à ce que toute autre amende administrative envisagée par une autre autorité de surveillance du marché pour le même opérateur économique ou le même type d'infraction tienne déjà compte, avec d'autres circonstances spécifiques pertinentes, d'une sanction imposée dans d'autres États membres et de son montant. Dans tous ces

---

21 JO L 123 du 12.5.2016, p. 1.

22 Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

cas, l'amende administrative cumulative que les autorités de surveillance du marché de plusieurs États membres pourraient infliger au même opérateur économique pour le même type d'infraction devrait être conforme au principe de proportionnalité.

(66) Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité compétente devrait tenir compte, lorsqu'elle examine le montant approprié pour l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives.

(67) Dans ses rapports avec les pays tiers, l'UE s'efforce de favoriser le commerce international des produits réglementés. Un large éventail de mesures peut être appliqué afin de faciliter le commerce, dont plusieurs instruments juridiques tels que les accords de reconnaissance mutuelle (ARM) bilatéraux (intergouvernementaux) sur l'évaluation de la conformité et le marquage des produits réglementés. Les accords de reconnaissance mutuelle sont conclus entre l'Union et les pays tiers bénéficiant d'un niveau de développement technique comparable et poursuivant une approche compatible en matière d'évaluation de la conformité. Ces accords se fondent sur l'acceptation mutuelle des certificats, des marques de conformité et des rapports d'essai délivrés par les organismes d'évaluation de la conformité de l'une des deux parties conformément à la législation de l'autre partie. Actuellement, des ARM sont en place pour plusieurs pays. Les accords sont conclus dans un certain nombre de secteurs spécifiques pouvant varier selon les pays. Afin de faciliter davantage le commerce et reconnaissant que les chaînes d'approvisionnement de produits comportant des éléments numériques sont mondiales, des ARM concernant l'évaluation de la conformité peuvent être conclus pour les produits régis par le présent règlement par l'Union conformément à l'article 218 du TFUE. La coopération avec les pays partenaires est également importante pour renforcer la cyberrésilience à l'échelle mondiale, car à long terme, celle-ci contribuera à renforcer le cadre de cybersécurité tant à l'intérieur qu'à l'extérieur de l'UE.

(68) Le présent règlement devrait être réexaminé périodiquement par la Commission, en consultation avec les parties intéressées, notamment en vue de déterminer s'il est nécessaire de le modifier pour tenir compte de l'évolution de la société, de la situation politique, des technologies ou de la situation des marchés.

(69) Il convient d'accorder un délai suffisant aux opérateurs économiques afin qu'ils s'adaptent aux exigences du présent règlement. Le présent règlement devrait s'appliquer [24 mois] à compter de son entrée en vigueur, à l'exception des obligations de signalement concernant les vulnérabilités activement exploitées et les incidents, qui devraient s'appliquer [12 mois] à compter de son entrée en vigueur.

(70) Étant donné que l'objectif du présent règlement ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(71) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[23] et a rendu un avis le [...],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

Le présent règlement établit:

(a) les règles relatives à la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;

(b) les exigences essentielles relatives à la conception, au développement et à la production de produits comportant des éléments numériques, et les obligations qui incombent aux opérateurs économiques en ce qui concerne ces produits eu égard à la cybersécurité;

(c) les exigences essentielles relatives aux processus de gestion des vulnérabilités mis en place par les fabricants pour garantir la cybersécurité des produits comportant des éléments numériques tout au long du cycle de vie, et les obligations incombant aux opérateurs économiques en ce qui concerne ces processus;

(d) les règles relatives à la surveillance du marché et au contrôle de l'application des règles et exigences susmentionnées.

Article 2

Champ d'application

1. Le présent règlement s'applique aux produits comportant des éléments numériques dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau.

2. Le présent règlement ne s'applique pas aux produits comportant des éléments numériques auxquels s'appliquent les actes de l'Union suivants:

   (a) règlement (UE) 2017/745;

   (b) règlement (UE) 2017/746;

   (c) règlement (UE) 2019/2144.

3. Le présent règlement ne s'applique pas aux produits comportant des éléments numériques qui ont été certifiés conformément au règlement (UE) 2018/1139.

[23] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

4. L’application du présent règlement à des produits comportant des éléments numériques qui relèvent d’autres règles de l’Union fixant des exigences qui couvrent tout ou partie des risques auxquels s'appliquent les exigences essentielles énoncées à l’annexe I peut être limitée ou exclue lorsque:

   (a) cette limitation ou cette exclusion est compatible avec le cadre réglementaire général applicable à ces produits;

   (b) les règles sectorielles assurent un niveau de protection identique à celui prévu par le présent règlement.

   La Commission est habilitée à adopter des actes délégués conformément à l’article 50 pour modifier le présent règlement aux fins de préciser si une telle limitation ou exclusion est nécessaire, les produits et règles concernés, ainsi que la portée de la limitation, le cas échéant.

5. Le présent règlement ne s’applique pas aux produits comportant des éléments numériques qui sont développés exclusivement à des fins de sécurité nationale ou à des fins militaires, ni aux produits spécifiquement conçus pour traiter des informations classifiées.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

(1) «produit comportant des éléments numériques»: tout produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels destinées à être mis sur le marché séparément;

(2) «traitement de données à distance»: tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant ou sous la responsabilité de ce dernier, et dont l’absence empêcherait le produit comportant des éléments numériques d’exécuter une de ses fonctions;

(3) «produit critique comportant des éléments numériques»: un produit comportant des éléments numériques, qui présente un risque de cybersécurité selon les critères énoncés à l’article 6, paragraphe 2, et dont la fonctionnalité de base est définie à l’annexe III;

(4) «produit hautement critique comportant des éléments numériques»: un produit comportant des éléments numériques, qui présente un risque de cybersécurité selon les critères énoncés à l’article 6, paragraphe 5;

(5) «technologie opérationnelle»: des systèmes ou dispositifs numériques programmables qui interagissent avec l’environnement physique ou gèrent des dispositifs qui interagissent avec l’environnement physique;

(6) «logiciel»: la partie d’un système d’information électronique qui consiste en un code informatique;

(7) «matériel informatique»: un système d’information électronique physique, ou des parties de celui-ci, capable de traiter, de stocker ou de transmettre des données numériques;

(8) «composant»: un logiciel ou du matériel destiné à être intégré dans un système d’information électronique;

(9) «système d'information électronique»: tout système, y compris des équipements électriques ou électroniques, capable de traiter, de stocker ou de transmettre des données numériques;

(10) «connexion logique»: une représentation virtuelle d'une connexion de données mise en œuvre au moyen d'une interface logicielle;

(11) «connexion physique»: toute connexion entre des systèmes d'information électroniques ou des composants mis en œuvre par des moyens physiques, y compris par des interfaces électriques ou mécaniques, des fils ou des ondes radio;

(12) «connexion indirecte»: une connexion à un dispositif ou à un réseau, qui n'est pas établie directement, mais plutôt dans le cadre d'un système plus vaste qui peut être directement connecté à ce dispositif ou à ce réseau;

(13) «privilège»: un droit d'accès accordé à des utilisateurs ou à des programmes particuliers pour effectuer des opérations liées à la sécurité au sein d'un système d'information électronique;

(14) «privilège élevé»: un droit d'accès accordé à des utilisateurs ou à des programmes particuliers pour effectuer un ensemble étendu d'opérations liées à la sécurité au sein d'un système d'information électronique et qui, s'il était utilisé de manière abusive ou compromis, pourrait permettre à un acteur malveillant d'accéder plus largement aux ressources d'un système ou d'une organisation;

(15) «point terminal»: tout dispositif connecté à un réseau et servant de point d'entrée à ce réseau;

(16) «ressources de mise en réseau ou de calcul»: des données ou des fonctionnalités matérielles ou logicielles accessibles soit localement, soit par l'intermédiaire d'un réseau ou d'un autre dispositif connecté;

(17) «opérateur économique», le fabricant, le mandataire, l'importateur, le distributeur ou toute autre personne physique ou morale soumise aux obligations prévues par le présent règlement;

(18) «fabricant»: toute personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;

(19) «mandataire»: toute personne physique ou morale établie dans l'Union ayant reçu mandat écrit d'un fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées;

(20) «importateur»: toute personne physique ou morale établie dans l'Union qui met sur le marché un produit comportant des éléments numériques, lequel porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union;

(21) «distributeur»: toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit comportant des éléments numériques à disposition sur le marché de l'Union sans altérer ses propriétés;

(22) «mise sur le marché»: la première mise à disposition d'un produit comportant des éléments numériques sur le marché de l'Union;

(23) «mise à disposition sur le marché»: toute fourniture d'un produit comportant des éléments numériques destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

(24) «utilisation prévue»: l'utilisation à laquelle un produit comportant des éléments numériques est destiné par le fabricant, y compris le contexte et les conditions spécifiques d'utilisation, telles que précisées dans les informations communiquées par le fabricant dans la notice d'utilisation, les indications publicitaires ou de vente, ainsi que dans la documentation technique;

(25) «utilisation raisonnablement prévisible»: une utilisation qui n'est pas nécessairement celle qui est prévue par le fabricant et qui figure dans la notice d'utilisation, les indications publicitaires ou de vente, ainsi que dans la documentation technique, mais qui est susceptible de résulter d'un comportement humain raisonnablement prévisible, d'opérations techniques ou d'interactions;

(26) «mauvaise utilisation raisonnablement prévisible»: l'utilisation d'un produit comportant des éléments numériques d'une manière qui n'est pas conforme à son utilisation prévue, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction avec d'autres systèmes;

(27) «autorité notifiante»: l'autorité nationale chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle;

(28) «évaluation de la conformité»: le processus qui permet de vérifier si les exigences essentielles énoncées à l'annexe I ont été respectées;

(29) «organisme d'évaluation de la conformité»: un organisme au sens de l'article 2, point 13), du règlement (CE) nº 765/2008;

(30) «organisme notifié»: un organisme d'évaluation de la conformité désigné en application de l'article 33 du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents;

(31) «modification substantielle»: une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, section 1, ou entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué;

(32) «marquage CE»: un marquage par lequel un fabricant indique qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I et à toute autre législation de l'Union applicable harmonisant les conditions de commercialisation des produits (ci-après dénommée «législation d'harmonisation de l'Union») qui en prévoit l'apposition;

(33) «autorité de surveillance du marché»: une autorité au sens de l'article 3, point 4, du règlement (UE) 2019/1020;

(34) «norme harmonisée»: une norme harmonisée au sens de l'article 2, point 1) c), du règlement (UE) nº 1025/2012;

(35) «risque de cybersécurité»: un risque au sens de l'article [X] de la directive [directive XXX/XXXX (SRI 2)];

(36) «risque de cybersécurité important »: un risque de cybersécurité qui, en raison de ses caractéristiques techniques, peut être présumé hautement susceptible de donner lieu à un incident pouvant avoir un impact négatif grave, notamment en causant une perte ou une perturbation matérielle ou immatérielle considérable;

(37) «nomenclature des logiciels»: un document officiel contenant les détails et les relations avec la chaîne d'approvisionnement des différents composants utilisés dans la fabrication d'un produit comportant des éléments numériques;

(38) «vulnérabilité»: une vulnérabilité au sens de l'article [X] de la directive [directive XXX/XXXX (SRI 2)];

(39) «vulnérabilité activement exploitée»: une vulnérabilité pour laquelle il existe des preuves fiables qu'un code malveillant a été exécuté par un acteur sur un système sans l'autorisation du propriétaire du système;

(40) «données à caractère personnel»: des données à caractère personnel au sens de l'article 4, point 1, du règlement (UE) 2016/679.

Article 4

Libre circulation

6. Les États membres n'empêchent pas, pour les aspects relevant du présent règlement, la mise à disposition sur le marché de produits comportant des éléments numériques conformes au présent règlement.

7. Lors de foires commerciales, d'expositions, de démonstrations ou d'événements similaires, les États membres n'empêchent pas la présentation et l'utilisation d'un produit comportant des éléments numériques non conforme au présent règlement.

8. Les États membres n'empêchent pas la mise à disposition de logiciels inachevés qui ne sont pas conformes au présent règlement, à condition que le logiciel ne soit mis à disposition que pour une durée limitée nécessaire à des fins d'essai et qu'une marque visible indique clairement que le logiciel n'est pas conforme au présent règlement et qu'il ne sera pas disponible sur le marché à d'autres fins que les essais.

Article 5

Exigences applicables aux produits comportant des éléments numériques

Les produits comportant des éléments numériques ne sont mis à disposition sur le marché que

(1) s'ils satisfont aux exigences essentielles énoncées à l'annexe I, section 1, à condition qu'ils soient correctement installés, entretenus, utilisés conformément à l'utilisation prévue ou dans des conditions raisonnablement prévisibles et, le cas échéant, mis à jour, et

(2) si les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2.

Article 6

Produits critiques comportant des éléments numériques

1. Les produits comportant des éléments numériques relevant d'une catégorie qui figure à l'annexe III sont considérés comme des produits critiques comportant des éléments numériques. Les produits dont la fonctionnalité de base est celle d'une catégorie

énumérée à l'annexe III du présent règlement sont considérés comme relevant de cette catégorie. Les catégories de produits critiques comportant des éléments numériques sont réparties entre les classes I et II, comme indiqué à l'annexe III, en fonction du niveau de risque de cybersécurité lié à ces produits.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour modifier l'annexe III en ajoutant une nouvelle catégorie à la liste des catégories de produits critiques comportant des éléments numériques ou en retirant une catégorie existante de cette liste. Lorsqu'elle évalue la nécessité de modifier la liste figurant à l'annexe III, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits comportant des éléments numériques. Pour déterminer le niveau de risque de cybersécurité, un ou plusieurs des critères suivants sont pris en compte:

   (a) la fonctionnalité liée à la cybersécurité du produit comportant des éléments numériques, et le fait que le produit comportant des éléments numériques possède ou non au moins l'un des attributs suivants:

      (i) il est conçu pour fonctionner avec un privilège élevé ou pour gérer des privilèges;

      (ii) il dispose d'un accès direct ou privilégié à des ressources de mise en réseau ou de calcul;

      (iii) il est conçu pour contrôler l'accès aux données ou à la technologie opérationnelle;

      (iv) il exécute des fonctions essentielles pour la confiance, en particulier des fonctions de sécurité telles que le contrôle du réseau, la sécurité des points terminaux et la protection du réseau;

   (b) l'utilisation prévue dans des environnements sensibles, y compris dans des environnements industriels ou par des entités essentielles du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)];

   (c) la finalité prévue de l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel;

   (d) l'ampleur potentielle d'une incidence négative, notamment en ce qui concerne son intensité et sa capacité d'affecter plusieurs personnes;

   (e) la mesure dans laquelle l'utilisation de produits comportant des éléments numériques a déjà causé une perte ou une perturbation matérielle ou immatérielle ou a suscité des préoccupations importantes quant à la matérialisation de cette incidence négative.

3. La Commission est habilitée à adopter un acte délégué conformément à l'article 50 afin de compléter le présent règlement en précisant les définitions des catégories de produits relevant des classes I et II figurant à l'annexe III. L'acte délégué est adopté [dans un délai de 12 mois à compter de l'entrée en vigueur du présent règlement].

4. Les produits critiques comportant des éléments numériques sont soumis aux procédures d'évaluation de la conformité visées à l'article 24, paragraphes 2 et 3.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement en précisant les catégories de produits hautement critiques comportant des éléments numériques pour lesquels les fabricants sont tenus d'obtenir un certificat de cybersécurité européen dans le cadre

d'un schéma européen de certification de cybersécurité en vertu du règlement (UE) 2019/881 afin de démontrer la conformité aux exigences essentielles énoncées à l'annexe I, ou à des parties de ces exigences. Lorsqu'elle détermine ces catégories de produits hautement critiques comportant des éléments numériques, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits comportant des éléments numériques, à la lumière d'un ou de plusieurs des critères énumérés au paragraphe 2, ainsi que d'une évaluation visant à déterminer si cette catégorie de produits est:

(a) utilisée par les entités essentielles du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)], nécessaire à leur activité ou susceptible d'avoir une importance future pour les activités de ces entités;

(b) pertinente pour la résilience de l'ensemble de la chaîne d'approvisionnement des produits comportant des éléments numériques face à des événements perturbateurs.

Article 7

Sécurité générale des produits

Par dérogation à l'article 2, paragraphe 1, troisième alinéa, point b), du règlement [règlement relatif à la sécurité générale des produits], lorsque les produits comportant des éléments numériques ne sont pas soumis à des exigences spécifiques prévues dans d'autres actes faisant partie de la législation d'harmonisation de l'Union au sens de [l'article 3, point 25), du règlement relatif à la sécurité générale des produits], le chapitre III, section 1, les chapitres V et VII, et les chapitres IX à XI du règlement [règlement sur la sécurité générale des produits], s'appliquent à ces produits en ce qui concerne les risques pour la sécurité qui ne sont pas couverts par le présent règlement.

Article 8

Systèmes d'IA à haut risque

1. Les produits comportant des éléments numériques classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [législation sur l'IA] qui relèvent du champ d'application du présent règlement et satisfont aux exigences essentielles énoncées à l'annexe I, section 1, du présent règlement sont, lorsque les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2, réputés conformes aux exigences de cybersécurité énoncées à l'article [article 15] du règlement [législation sur l'IA], sans préjudice des autres exigences en matière d'exactitude et de robustesse figurant à l'article susmentionné, et dans la mesure où le niveau de protection requis par ces exigences est démontré par la déclaration UE de conformité délivrée en vertu du présent règlement.

2. Pour les produits et les exigences de cybersécurité visés au paragraphe 1, la procédure d'évaluation de la conformité pertinente prévue à l'article [article 43] du règlement [législation sur l'IA] s'applique. Aux fins de cette évaluation, les organismes notifiés qui sont habilités à contrôler la conformité des systèmes d'IA à haut risque au titre du règlement [législation sur l'IA] sont également habilités à contrôler la conformité des systèmes d'IA à haut risque entrant dans le champ d'application du présent règlement aux exigences énoncées à l'annexe I du présent règlement, à condition que la conformité de ces organismes notifiés aux exigences

énoncées à l'article 29 du présent règlement ait été évaluée dans le cadre de la procédure de notification prévue par le règlement [législation sur l'IA].

3. Par dérogation au paragraphe 2, les produits critiques comportant des éléments numériques énumérés à l'annexe III du présent règlement, qui doivent faire l'objet des procédures d'évaluation de la conformité prévues par l'article 24, paragraphe 2, points a) et b), et à l'article 24, paragraphe 3, points a) et b) du présent règlement, et qui sont également classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [législation sur l'IA] et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne prévue à l'annexe [VI] du règlement [législation sur l'IA], sont soumis aux procédures d'évaluation de la conformité requises par le présent règlement en ce qui concerne les exigences essentielles du présent règlement.

Article 9

Machines et produits connexes

Les machines et produits connexes relevant du champ d'application du règlement [proposition de règlement sur les machines et produits connexes] qui sont des produits comportant des éléments numériques au sens du présent règlement et pour lesquels une déclaration UE de conformité a été délivrée sur la base du présent règlement sont réputés conformes aux exigences essentielles de santé et de sécurité énoncées à l'annexe [annexe III, sections 1.1.9 et 1.2.1] du règlement [proposition de règlement sur les machines et produits connexes], en ce qui concerne la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de commande, et dans la mesure où le niveau de protection requis par ces exigences est démontré dans la déclaration UE de conformité délivrée en vertu du présent règlement.

CHAPITRE II

OBLIGATIONS INCOMBANT AUX OPÉRATEURS ÉCONOMIQUES

Article 10

Obligations incombant aux fabricants

1. Le fabricant s'assure, lorsqu'il met sur le marché un produit comportant des éléments numériques, que celui-ci a été conçu, développé et fabriqué conformément aux exigences essentielles énoncées à l'annexe I, section 1.

2. Aux fins du respect de l'obligation énoncée au paragraphe 1, le fabricant procède à une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques et tient compte des résultats de cette évaluation au cours des phases de planification, de conception, de développement, de production, de livraison et de maintenance du produit comportant des éléments numériques, en vue de réduire au minimum les risques de cybersécurité, de prévenir les incidents de sécurité et de réduire au minimum les conséquences de ces derniers, notamment en ce qui concerne la santé et la sécurité des utilisateurs.

3. Lorsqu'il met sur le marché un produit comportant des éléments numériques, le fabricant inclut une évaluation des risques de cybersécurité dans la documentation technique prévue à l'article 23 et à l'annexe V. Pour les produits comportant des éléments numériques mentionnés à l'article 8 et à l'article 24, paragraphe 4, qui

relèvent aussi d'autres actes législatifs de l'Union, l'évaluation des risques de cybersécurité peut faire partie de l'évaluation des risques prévue par ces actes de l'Union. Lorsque certaines exigences essentielles ne sont pas applicables au produit comportant des éléments numériques commercialisé, le fabricant fait figurer une justification claire dans cette documentation.

4. Aux fins du respect de l'obligation énoncée au paragraphe 1, le fabricant fait preuve de la diligence nécessaire lorsqu'il intègre dans des produits comportant des éléments numériques des composants obtenus auprès de tiers. Il veille à ce que ces composants ne compromettent pas la sécurité du produit comportant des éléments numériques.

5. Le fabricant documente systématiquement, d'une manière proportionnée à la nature et à l'ampleur des risques de cybersécurité, les aspects pertinents pour la cybersécurité concernant le produit comportant des éléments numériques, y compris les vulnérabilités dont il a connaissance et toute information pertinente fournie par des tiers, et, le cas échéant, met à jour l'évaluation des risques du produit.

6. Lorsqu'il met sur le marché un produit comportant des éléments numériques, et pendant la durée de vie prévue du produit ou pendant une période de cinq ans à compter de la mise sur le marché de celui-ci, la plus courte des deux durées étant retenue, le fabricant veille à ce que les vulnérabilités de ce produit soient gérées efficacement et conformément aux exigences essentielles énoncées à l'annexe I, section 2.

   Le fabricant dispose de politiques et de procédures appropriées, notamment les politiques de divulgation coordonnée des vulnérabilités mentionnées à l'annexe I, section 2, point 5), pour traiter et corriger les vulnérabilités potentielles du produit comportant des éléments numériques signalées par des sources internes ou externes.

7. Avant de mettre sur le marché un produit comportant des éléments numériques, le fabricant établit la documentation technique visée à l'article 23.

   Il applique ou fait appliquer les procédures d'évaluation de la conformité choisies visées à l'article 24.

   Lorsqu'il a été démontré, au moyen de cette procédure d'évaluation de la conformité, que le produit comportant des éléments numériques est conforme aux exigences essentielles énoncées à l'annexe I, section 1, et que les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2, le fabricant établit la déclaration UE de conformité conformément à l'article 20 et appose le marquage CE conformément à l'article 22.

8. Le fabricant tient la documentation technique et la déclaration UE de conformité, le cas échéant, à la disposition des autorités de surveillance du marché pendant une durée de dix ans après la mise sur le marché du produit comportant des éléments numériques.

9. Le fabricant veille à ce que des procédures soient en place pour que la conformité des produits comportant des éléments numériques produits en série reste assurée. Le fabricant tient dûment compte des modifications du processus de développement et de production ou de la conception ou des caractéristiques du produit comportant des éléments numériques, ainsi que des modifications des normes harmonisées, des schémas européens de certification de cybersécurité ou des spécifications techniques visées à l'article 19 au regard desquelles la conformité du produit comportant des éléments numériques est déclarée ou en application desquelles sa conformité est vérifiée.

10. Le fabricant veille à ce que les produits comportant des éléments numériques soient accompagnés des informations et des instructions énoncées à l'annexe II, sous forme électronique ou physique. Ces informations et instructions sont rédigées dans une langue aisément compréhensible par les utilisateurs. Elles sont claires, compréhensibles, intelligibles et lisibles. Elles permettent une installation, un fonctionnement et une utilisation sécurisés des produits comportant des éléments numériques.

11. Le fabricant fournit la déclaration UE de conformité avec le produit comportant des éléments numériques ou inclut dans les instructions et informations énoncées à l'annexe II l'adresse internet à laquelle la déclaration UE de conformité est accessible.

12. Dès la mise sur le marché et pendant la durée de vie prévue d'un produit comportant des éléments numériques ou pendant une période de cinq ans après sa mise sur le marché, la durée la plus courte étant retenue, le fabricant qui considère ou a des raisons de croire que le produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus du fabricant en conformité, ou pour procéder à leur retrait ou à leur rappel, selon le cas.

13. Sur requête motivée d'une autorité de surveillance du marché, le fabricant communique à cette dernière, dans une langue aisément compréhensible par celle-ci, toutes les informations et tous les documents, sur support papier ou par voie électronique, nécessaires pour démontrer la conformité du produit comportant des éléments numériques et des processus mis en place par le fabricant aux exigences essentielles énoncées à l'annexe I. Il coopère avec ladite autorité, à la demande de cette dernière, concernant toute mesure prise pour éliminer les risques de cybersécurité présentés par le produit comportant des éléments numériques qu'il a mis sur le marché.

14. Un fabricant qui cesse ses activités et qui, de ce fait, n'est pas en mesure de se conformer aux obligations énoncées dans le présent règlement informe les autorités de surveillance du marché concernées de cette situation avant que cette cessation ne prenne effet, ainsi que, par tout moyen disponible et dans la mesure du possible, les utilisateurs des produits comportant des éléments numériques mis sur le marché concernés.

15. La Commission peut, au moyen d'actes d'exécution, préciser le format et les éléments de la nomenclature des logiciels prévue à l'annexe I, section 2, point 1). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

Article 11

Obligations en matière de communication d'informations incombant aux fabricants

1. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance, toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques. La notification contient des précisions concernant cette vulnérabilité et, le cas échéant, toute mesure prise pour y remédier ou en atténuer les effets. Dès réception de cette

notification, l'ENISA la transmet, sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, au CSIRT désigné aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article [X] de la directive [XXX/XXXX (SRI2)] des États membres concernés et informe l'autorité de surveillance du marché de la vulnérabilité notifiée.

2. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance, tout incident ayant un impact sur la sécurité du produit comportant des éléments numériques. L'ENISA transmet sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, les notifications au point de contact unique désigné conformément à l'article [article X] de la directive [XXX/XXXX (SRI 2)] des États membres concernés et informe l'autorité de surveillance du marché des incidents notifiés. La notification d'incident comprend des informations sur la gravité et l'impact de l'incident et, le cas échéant, indique si le fabricant soupçonne des actes illicites ou malveillants d'être à l'origine de l'incident ou s'il considère que ce dernier a des répercussions transfrontières.

3. L'ENISA soumet au réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe) institué par l'article [l'article X] de la directive [la directive XXX/XXXX (SRI2)] les informations notifiées conformément aux paragraphes 1 et 2 si elles sont pertinentes pour la gestion coordonnée au niveau opérationnel des incidents et crises de cybersécurité majeurs.

4. Dans les meilleurs délais après avoir pris connaissance de l'incident, le fabricant informe les utilisateurs du produit comportant des éléments numériques de cet incident et, le cas échéant, des mesures correctives que l'utilisateur peut mettre en place pour en atténuer l'impact.

5. La Commission peut, au moyen d'actes d'exécution, préciser plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

6. Sur la base des notifications reçues conformément aux paragraphes 1 et 2, l'ENISA élabore un rapport technique bisannuel sur les tendances émergentes en ce qui concerne les risques de cybersécurité dans les produits comportant des éléments numériques et le soumet au groupe de coopération visé à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)]. Le premier rapport de ce type est présenté dans les 24 mois suivant le début de l'application des obligations prévues aux paragraphes 1 et 2.

7. Lorsqu'il identifie une vulnérabilité dans un composant, y compris un composant *open source*, qui est intégré au produit comportant des éléments numériques, le fabricant signale la vulnérabilité à la personne ou à l'entité qui assure la maintenance du composant.

Article 12

Mandataires

1. Un fabricant peut désigner, par mandat écrit, un mandataire.

2. Les obligations énoncées à l'article 10, paragraphes 1 à 7, premier alinéa et à l'article 10, paragraphe 9, ne font pas partie du mandat confié au mandataire.

3. Le mandataire exécute les tâches spécifiées dans le mandat qu'il reçoit du fabricant. Le mandat autorise au minimum le mandataire:

(a) à tenir à la disposition des autorités de surveillance du marché la déclaration UE de conformité mentionnée à l'article 20 et la documentation technique mentionnée à l'article 23 pendant dix ans à partir de la mise sur le marché du produit comportant des éléments numériques;

(b) sur requête motivée d'une autorité de surveillance du marché, à communiquer à cette dernière toutes les informations et tous les documents nécessaires pour démontrer la conformité du produit comportant des éléments numériques;

(c) à coopérer avec les autorités de surveillance du marché, à leur demande, concernant toute mesure adoptée pour éliminer les risques présentés par un produit comportant des éléments numériques relevant du mandat confié au mandataire.

Article 13

Obligations incombant aux importateurs

1. Un importateur ne met sur le marché que des produits comportant des éléments numériques conformes aux exigences essentielles énoncées à l'annexe I, section 1, et lorsque les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2.

2. Avant de mettre sur le marché un produit comportant des éléments numériques, l'importateur veille à ce que:

(a) les procédures appropriées d'évaluation de la conformité mentionnées à l'article 24 aient été menées à bien par le fabricant;

(b) le fabricant ait établi la documentation technique;

(c) le produit comportant des éléments numériques porte le marquage CE mentionné à l'article 22 et soit accompagné des informations et de la notice d'utilisation mentionnées à l'annexe II.

3. Lorsqu'un importateur considère ou a des raisons de croire qu'un produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I, il ne met pas le produit sur le marché tant que ce produit ou les processus mis en place par le fabricant n'ont pas été mis en conformité avec les exigences essentielles énoncées à l'annexe I. En outre, lorsque le produit comportant des éléments numériques présente un risque de cybersécurité important, l'importateur en informe le fabricant et les autorités de surveillance du marché.

4. L'importateur indique son nom, sa raison sociale ou sa marque déposée et les adresses postale et électronique auxquelles il peut être contacté sur le produit comportant des éléments numériques ou, lorsque cela n'est pas possible, sur l'emballage ou dans un document accompagnant le produit comportant des éléments numériques. Les coordonnées sont indiquées dans une langue aisément compréhensible par les utilisateurs et les autorités de surveillance du marché.

5. L'importateur veille à ce que le produit comportant des éléments numériques soit accompagné des instructions et informations prévues à l'annexe II, rédigées dans une langue aisément compréhensible par les utilisateurs.

6. Tout importateur qui considère ou a des raisons de croire qu'un produit comportant des éléments numériques, qu'il a mis sur le marché, ou bien les processus mis en place par son fabricant, ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus mis en place par son fabricant en conformité avec les exigences essentielles énoncées à l'annexe I, ou pour procéder au retrait ou au rappel du produit, si nécessaire.

   Lorsqu'il décèle une vulnérabilité du produit comportant des éléments numériques, l'importateur en informe le fabricant dans les meilleurs délais. En outre, si le produit comportant des éléments numériques présente un risque de cybersécurité important, l'importateur en informe immédiatement les autorités de surveillance du marché des États membres dans lesquels il a mis ce produit à disposition sur le marché, en fournissant des précisions, notamment, sur la non-conformité et toute mesure corrective adoptée.

7. Pendant dix ans à partir de la mise sur le marché du produit comportant des éléments numériques, l'importateur tient à la disposition des autorités de surveillance du marché une copie de la déclaration UE de conformité et s'assure que la documentation technique peut être fournie à ces autorités, sur demande.

8. Sur requête motivée d'une autorité de surveillance du marché, l'importateur communique à cette dernière toutes les informations et tous les documents nécessaires, sur support papier ou par voie électronique, pour démontrer la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, section 1, ainsi que la conformité des processus mis en place par le fabricant aux exigences essentielles énoncées à l'annexe I, section 2, dans une langue aisément compréhensible par cette autorité. Il coopère avec cette autorité, à la demande de cette dernière, concernant toute mesure prise en vue d'éliminer les risques de cybersécurité présentés par le produit comportant des éléments numériques qu'il a mis sur le marché.

9. Lorsque l'importateur d'un produit comportant des éléments numériques a connaissance du fait que le fabricant de ce produit a cessé ses activités et, de ce fait, n'est pas en mesure de se conformer aux obligations énoncées dans le présent règlement, l'importateur informe les autorités de surveillance du marché concernées de cette situation, ainsi que, par tout moyen disponible et dans la mesure du possible, les utilisateurs des produits concernés comportant des éléments numériques mis sur le marché.

Article 14

Obligations des distributeurs

1. Lorsqu'il met un produit comportant des éléments numériques à disposition sur le marché, le distributeur agit avec la diligence requise en ce qui concerne les exigences du présent règlement.

2. Avant de mettre un produit comportant des éléments numériques à disposition sur le marché, le distributeur vérifie que:

   (a) le produit comportant des éléments numériques porte le marquage CE;

(b) le fabricant et l'importateur se sont conformés aux obligations énoncées, respectivement, à l'article 10, paragraphes 10 et 11, et à l'article 13, paragraphe 4.

3. Lorsqu'un distributeur considère ou a des raisons de croire qu'un produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I, il ne met pas le produit comportant des éléments numériques à disposition sur le marché tant que ce produit ou les processus mis en place par le fabricant n'ont pas été mis en conformité. En outre, lorsque le produit comportant des éléments numériques présente un risque de cybersécurité important, le distributeur en informe le fabricant et les autorités de surveillance du marché.

4. Tout distributeur sachant ou ayant des raisons de croire qu'un produit comportant des éléments numériques, qu'il a mis à disposition sur le marché, ou bien les processus mis en place par son fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I veille à ce que soient prises les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus mis en place par son fabricant en conformité, ou pour retirer ou rappeler le produit, si nécessaire.

   Lorsqu'il décèle une vulnérabilité du produit comportant des éléments numériques, le distributeur en informe le fabricant dans les meilleurs délais. En outre, si le produit comportant des éléments numériques présente un risque de cybersécurité important, le distributeur en informe immédiatement les autorités de surveillance du marché des États membres dans lesquels il a mis ce produit à disposition sur le marché, en fournissant des précisions, notamment, sur la non-conformité et toute mesure corrective adoptée.

5. Sur requête motivée d'une autorité de surveillance du marché, le distributeur communique à cette dernière toutes les informations et tous les documents nécessaires, sur support papier ou par voie électronique, pour démontrer la conformité du produit comportant des éléments numériques et des processus mis en place par son fabricant avec les exigences essentielles énoncées à l'annexe I dans une langue aisément compréhensible par cette autorité. Il coopère avec cette autorité, à sa demande, à toute mesure prise en vue d'éliminer les risques de cybersécurité présentés par le produit comportant des éléments numériques qu'il a mis à disposition sur le marché.

6. Lorsque le distributeur d'un produit comportant des éléments numériques apprend que le fabricant de ce produit a cessé ses activités et, de ce fait, n'est pas en mesure de se conformer aux obligations énoncées dans le présent règlement, le distributeur informe les autorités de surveillance du marché concernées de cette situation, ainsi que, par tout moyen disponible et dans la mesure du possible, les utilisateurs des produits concernés comportant des éléments numériques mis sur le marché.

Article 15

Cas dans lesquels les obligations des fabricants s'appliquent aux importateurs et aux distributeurs

Un importateur ou un distributeur est considéré comme un fabricant aux fins du présent règlement et est soumis aux obligations incombant au fabricant au titre de l'article 10 et de l'article 11, paragraphes 1, 2, 4 et 7, lorsque cet importateur ou ce distributeur met un produit

comportant des éléments numériques sur le marché sous son propre nom ou sa propre marque, ou lorsqu'il apporte une modification substantielle à un produit comportant des éléments numériques déjà mis sur le marché.

Article 16

Autres cas dans lesquels les obligations des fabricants s'appliquent

Une personne physique ou morale, autre que le fabricant, l'importateur ou le distributeur, qui apporte une modification substantielle à un produit comportant des éléments numériques est considérée comme un fabricant aux fins du présent règlement.

Cette personne est soumise aux obligations incombant au fabricant énoncées à l'article 10 et à l'article 11, paragraphes 1, 2, 4 et 7, en ce qui concerne la partie du produit sur laquelle porte la modification substantielle, ou en ce qui concerne l'ensemble du produit si la modification substantielle a une incidence sur la cybersécurité du produit comportant des éléments numériques dans son ensemble.

Article 17

Identification des opérateurs économiques

1. Sur demande et lorsque les informations sont disponibles, l'opérateur économique fournit aux autorités de surveillance du marché les informations suivantes:

   (a) le nom et l'adresse de tout opérateur économique qui lui a fourni un produit comportant des éléments numériques;

   (b) le nom et l'adresse de tout opérateur économique auquel il a fourni un produit comportant des éléments numériques.

2. L'opérateur économique est en mesure de communiquer les informations visées au paragraphe 1 pendant dix ans à compter de la date à laquelle le produit comportant des éléments numériques lui a été fourni et pendant dix ans à compter de la date à laquelle il l'a fourni.

CHAPITRE III

CONFORMITE DU PRODUIT COMPORTANT DES ELEMENTS NUMERIQUES

Article 18

Présomption de conformité

1. Le produit comportant des éléments numériques et les processus mis en place par le fabricant qui sont conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences essentielles qui sont couvertes par ces normes ou parties de ces normes et qui sont énoncées à l'annexe I.

2. Le produit comportant des éléments numériques et les processus mis en place par le fabricant qui sont conformes aux spécifications communes visées à l'article 19 sont présumés conformes aux exigences essentielles énoncées à l'annexe I, dans la mesure où celles-ci sont couvertes par ces spécifications communes.

3. Le produit comportant des éléments numériques et les processus mis en place par le fabricant pour lesquels une déclaration de conformité de l'UE ou un certificat de cybersécurité européen ont été délivrés dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881 et spécifié conformément au paragraphe 4 sont présumés conformes aux exigences essentielles énoncées à l'annexe I, dans la mesure où celles-ci sont couvertes par la déclaration de conformité de l'UE ou le certificat de cybersécurité européen, ou des parties de ceux-ci.

4. La Commission est habilitée, au moyen d'actes d'exécution, à préciser les schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 qui peuvent être utilisés afin de démontrer la conformité avec les exigences essentielles énoncées à l'annexe I, ou avec des parties de ces exigences. En outre, le cas échéant, la Commission précise si un certificat de cybersécurité délivré au titre de tels schémas supprime l'obligation d'un fabricant de procéder à une évaluation de la conformité par un tiers pour les exigences correspondantes, comme indiqué à l'article 24, paragraphe 2, points a) et b), et paragraphe 3, points a) et b). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

Article 19

Spécifications communes

Lorsque les normes harmonisées visées à l'article 18 n'existent pas ou lorsque la Commission estime que les normes harmonisées pertinentes sont insuffisantes pour satisfaire aux exigences du présent règlement ou pour répondre à la demande de normalisation de la Commission, ou lorsque la procédure de normalisation rencontre des retards excessifs ou lorsqu'aucune organisation européenne de normalisation n'a accepté la demande de normes harmonisées de la Commission, la Commission est habilitée, au moyen d'actes d'exécution, à adopter des spécifications communes en ce qui concerne les exigences essentielles énoncées à l'annexe I. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

Article 20

Déclaration UE de conformité

1. La déclaration UE de conformité est établie par le fabricant conformément à l'article 10, paragraphe 7, et atteste que le respect des exigences essentielles applicables énoncées à l'annexe I a été démontré.

2. La déclaration UE de conformité est établie selon le modèle figurant à l'annexe IV et contient les éléments précisés dans les procédures d'évaluation de la conformité applicables prévues à l'annexe VI. Cette déclaration est constamment mise à jour. Elle est disponible dans la ou les langues requises par l'État membre dans lequel le produit comportant des éléments numériques est mis sur le marché ou mis à disposition.

3. Lorsqu'un produit comportant des éléments numériques relève de plusieurs actes de l'Union imposant une déclaration UE de conformité, une seule déclaration UE de conformité est établie pour l'ensemble de ces actes. Cette déclaration mentionne les titres des actes de l'Union concernés, ainsi que les références de leur publication.

4. En établissant la déclaration UE de conformité, le fabricant assume la responsabilité de la conformité du produit.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement aux fins d'ajouter des éléments au contenu minimal de la déclaration UE de conformité prévu à l'annexe IV afin de tenir compte des progrès techniques.

Article 21

Principes généraux du marquage CE

Le marquage CE tel que défini à l'article 3, paragraphe 32, est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) nº 765/2008.

Article 22

Règles et conditions d'apposition du marquage CE

1. Le marquage CE est apposé de manière visible, lisible et indélébile sur le produit comportant des éléments numériques. Lorsque la nature du produit comportant des éléments numériques ne le permet pas ou ne le justifie pas, il est apposé sur son emballage et sur la déclaration UE de conformité mentionnée à l'article 20 qui accompagne le produit comportant des éléments numériques. Pour les produits comportant des éléments numériques qui se présentent sous la forme d'un logiciel, le marquage CE est apposé soit sur la déclaration UE de conformité mentionnée à l'article 20, soit sur le site web qui accompagne le logiciel.

2. En raison de la nature du produit comportant des éléments numériques, la hauteur du marquage CE apposé sur le produit comportant des éléments numériques peut être inférieure à 5 mm, à condition qu'il reste visible et lisible.

3. Le marquage CE est apposé avant que le produit comportant des éléments numériques ne soit mis sur le marché. Il peut être suivi d'un pictogramme ou de tout autre marquage indiquant un risque ou un usage particulier énoncés dans les actes d'exécution visés au paragraphe 6.

4. Le marquage CE est suivi du numéro d'identification de l'organisme notifié, lorsque cet organisme participe à la procédure d'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) visée à l'article 24.

   Le numéro d'identification de l'organisme notifié est apposé par l'organisme lui-même ou, sur instruction de celui-ci, par le fabricant ou le mandataire du fabricant.

5. Les États membres s'appuient sur les mécanismes existants pour assurer la bonne application du régime régissant le marquage CE et prennent les mesures nécessaires en cas d'usage abusif de ce marquage. Lorsque le produit comportant des éléments numériques relève d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, le marquage CE indique que le produit satisfait également aux exigences de ces autres actes législatifs.

6. La Commission peut, au moyen d'actes d'exécution, définir des spécifications techniques pour les pictogrammes ou tout autre marquage en lien avec la sécurité du produit comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

Article 23

Documentation technique

1. La documentation technique réunit l'ensemble des informations ou des précisions utiles concernant les moyens employés par le fabricant pour garantir la conformité du produit comportant des éléments numériques et des processus mis en place par le fabricant aux exigences essentielles énoncées à l'annexe I. Elle contient, au minimum, les éléments énumérés à l'annexe V.

2. La documentation technique est établie avant que le produit comportant des éléments numériques ne soit mis sur le marché et fait l'objet de mises à jour régulières, le cas échéant, pendant la durée de vie prévue du produit ou pendant une période de cinq ans après la mise sur le marché d'un produit comportant des éléments numériques, la durée la plus courte étant retenue.

3. Pour les produits comportant des éléments numériques mentionnés à l'article 8 et à l'article 24, paragraphe 4, qui relèvent aussi d'autres actes législatifs de l'Union, une seule documentation technique est établie, contenant les informations visées à l'annexe V du présent règlement ainsi que les informations requises en vertu de ces actes de l'Union.

4. La documentation technique et la correspondance se rapportant à toute procédure d'évaluation de la conformité sont rédigées dans une langue officielle de l'État membre dans lequel est établi l'organisme notifié ou dans une langue acceptée par celui-ci.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement aux fins d'inclure les éléments requis dans la documentation technique figurant à l'annexe V pour tenir compte des progrès techniques ainsi que des évolutions rencontrées dans le processus de mise en œuvre du présent règlement.

Article 24

Procédures d'évaluation de la conformité pour les produits comportant des éléments numériques

1. Le fabricant effectue une évaluation de la conformité du produit comportant des éléments numériques et des processus mis en place par le fabricant pour déterminer si les exigences essentielles énoncées à l'annexe I sont respectées. Le fabricant ou le mandataire du fabricant démontre la conformité avec les exigences essentielles en suivant l'une des procédures suivantes:

   (a) la procédure de contrôle interne (module A) visée à l'annexe VI; ou

   (b) la procédure d'examen UE de type (module B) prévue à l'annexe VI, suivie de la conformité au type «UE» sur la base du contrôle interne de la production (module C), prévue à l'annexe VI; ou

   (c) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VI.

2. Lorsque, lors de l'évaluation de la conformité du produit critique comportant des éléments numériques relevant de la classe I figurant à l'annexe III et des processus mis en place par son fabricant avec les exigences essentielles énoncées à l'annexe I, le fabricant ou le mandataire du fabricant n'a pas appliqué ou n'a appliqué qu'en

partie des normes harmonisées, des spécifications communes ou des schémas européens de certification de cybersécurité visés à l'article 18, ou lorsque ces normes harmonisées, spécifications communes ou schémas européens de certification de cybersécurité n'existent pas, le produit comportant des éléments numériques concerné et les processus mis en place par le fabricant sont soumis, pour ce qui a trait à ces exigences essentielles, à l'une des procédures suivantes:

(a) la procédure d'examen UE de type (module B) prévue à l'annexe VI, suivie de la conformité au type «UE» sur la base du contrôle interne de la production (module C), prévue à l'annexe VI; ou

(b) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VI.

3. Lorsque le produit est un produit critique comportant des éléments numériques relevant de la classe II figurant à l'annexe III, le fabricant ou le mandataire du fabricant démontre la conformité avec les exigences essentielles énoncées à l'annexe I en suivant l'une des procédures suivantes:

(a) la procédure d'examen UE de type (module B) prévue à l'annexe VI, suivie de la conformité au type «UE» sur la base du contrôle interne de la production (module C), prévue à l'annexe VI; ou

(b) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VI.

4. Le fabricant de produits comportant des éléments numériques qui sont classés comme systèmes de DME relevant du champ d'application du règlement [règlement relatif à l'espace européen des données de santé] démontre la conformité avec les exigences essentielles énoncées à l'annexe I du présent règlement en suivant la procédure d'évaluation de la conformité pertinente prévue par le règlement [chapitre III du règlement relatif à l'espace européen des données de santé].

5. Les organismes notifiés tiennent compte des intérêts et besoins spécifiques des petites et moyennes entreprises (PME) lorsqu'ils fixent les redevances imposées pour les procédures d'évaluation de la conformité, et les réduisent proportionnellement auxdits intérêts et besoins spécifiques.

CHAPITRE IV

NOTIFICATION DES ORGANISMES D'ÉVALUATION DE LA CONFORMITÉ

Article 25

Notification

Les États membres notifient à la Commission et aux autres États membres les organismes d'évaluation de la conformité autorisés à procéder à l'évaluation de la conformité conformément au présent règlement.

Article 26

Autorités notifiantes

1. Les États membres désignent une autorité notifiante responsable de la mise en place et de l'application des procédures nécessaires à l'évaluation et à la notification des

organismes d'évaluation de la conformité ainsi qu'au contrôle des organismes notifiés, y compris le respect de l'article 31.

2. Les États membres peuvent décider que l'évaluation et le contrôle visés au paragraphe 1 sont effectués par un organisme d'accréditation national au sens du règlement (CE) nº 765/2008 et conformément à ses dispositions.

Article 27

Exigences concernant les autorités notifiantes

1. Une autorité notifiante est établie de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité.

2. Une autorité notifiante est organisée et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités.

3. Une autorité notifiante est organisée de telle sorte que chaque décision concernant la notification d'un organisme d'évaluation de la conformité est prise par des personnes compétentes différentes de celles qui ont réalisé l'évaluation.

4. Une autorité notifiante ne propose ni ne fournit aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle.

5. Une autorité notifiante garantit la confidentialité des informations qu'elle obtient.

6. Une autorité notifiante dispose d'un personnel compétent en nombre suffisant pour la bonne exécution de ses tâches.

Article 28

Obligation des autorités notifiantes en matière d'information

1. Les États membres informent la Commission de leurs procédures concernant l'évaluation et la notification des organismes d'évaluation de la conformité ainsi que le contrôle des organismes notifiés, et de toute modification en la matière.

2. La Commission rend publiques ces informations.

Article 29

Exigences concernant les organismes notifiés

1. Aux fins de la notification, un organisme d'évaluation de la conformité répond aux exigences définies aux paragraphes 2 à 12.

2. Un organisme d'évaluation de la conformité est constitué en vertu du droit national et possède la personnalité juridique.

3. Un organisme d'évaluation de la conformité est un organisme tiers indépendant de l'organisation ou du produit qu'il évalue.

Un organisme appartenant à une association d'entreprises ou à une fédération professionnelle qui représente des entreprises participant à la conception, au développement, à la production, à la fourniture, à l'assemblage, à l'utilisation ou à l'entretien des produits comportant des éléments numériques qu'il évalue peut, pour autant que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées, être considéré comme satisfaisant à cette condition.

4. Un organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargés d'exécuter les tâches d'évaluation de la conformité ne peuvent être le concepteur, le développeur, le fabricant, le fournisseur, l'installateur, l'acheteur, le propriétaire, l'utilisateur ou le responsable de l'entretien des produits comportant des éléments numériques qu'ils évaluent, ni le mandataire d'aucune de ces parties. Cela n'exclut pas l'utilisation de produits évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité, ou l'utilisation de ces produits à des fins personnelles.

   Un organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargés d'exécuter les tâches d'évaluation de la conformité n'interviennent pas directement dans la conception, le développement, la production, la commercialisation, l'installation, l'utilisation ou l'entretien de ces produits ou ne représentent pas les parties engagées dans ces activités. Ils ne participent à aucune activité qui peut entrer en conflit avec l'indépendance de leur jugement ou l'intégrité des activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela vaut en particulier pour les services de conseil.

   Les organismes d'évaluation de la conformité veillent à ce que les activités de leurs filiales ou sous-traitants n'aient pas d'incidence sur la confidentialité, l'objectivité ou l'impartialité de leurs activités d'évaluation de la conformité.

5. Les organismes d'évaluation de la conformité et leur personnel accomplissent les activités d'évaluation de la conformité avec la plus haute intégrité professionnelle et la compétence technique requise dans le domaine spécifique et sont à l'abri de toute pression ou incitation, notamment d'ordre financier, susceptible d'influencer leur jugement ou les résultats de leurs activités d'évaluation de la conformité, en particulier de la part de personnes ou de groupes de personnes intéressés par ces résultats.

6. Un organisme d'évaluation de la conformité est capable d'exécuter toutes les tâches d'évaluation de la conformité visées à l'annexe VI et pour lesquelles il a été notifié, que ces tâches soient exécutées par lui-même ou en son nom et sous sa responsabilité.

   En toutes circonstances et pour chaque procédure d'évaluation de la conformité et tout type ou toute catégorie de produits comportant des éléments numériques pour lesquels il a été notifié, l'organisme d'évaluation de la conformité dispose à suffisance:

   (a) du personnel requis ayant les connaissances techniques et l'expérience suffisante et appropriée pour exécuter les tâches d'évaluation de la conformité;

   (b) de descriptions des procédures utilisées pour évaluer la conformité, garantissant la transparence et la capacité de reproduction de ces procédures. L'organisme dispose de politiques et de procédures appropriées faisant la distinction entre les tâches qu'il exécute en tant qu'organisme notifié et d'autres activités;

   (c) de procédures pour accomplir ses activités qui tiennent dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit en question et de la nature en masse, ou série, du processus de production.

Il dispose des moyens nécessaires à la bonne exécution des tâches techniques et administratives liées aux activités d'évaluation de la conformité et a accès à tous les équipements ou installations nécessaires.

7. Le personnel chargé de l'exécution des activités d'évaluation de la conformité possède:

   (a) une solide formation technique et professionnelle correspondant à l'ensemble des activités d'évaluation de la conformité pour lesquelles l'organisme d'évaluation de la conformité a été notifié;

   (b) une connaissance satisfaisante des exigences applicables aux évaluations qu'il effectue et l'autorité nécessaire pour effectuer ces évaluations;

   (c) une connaissance et une compréhension adéquates des exigences essentielles, des normes harmonisées applicables ainsi que des dispositions pertinentes de la législation d'harmonisation de l'Union et de ses actes d'exécution;

   (d) l'aptitude à rédiger les attestations, procès-verbaux et rapports qui constituent la matérialisation des évaluations effectuées.

8. L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs et du personnel effectuant l'évaluation est garantie.

   La rémunération des cadres supérieurs et du personnel chargé de l'évaluation au sein d'un organisme d'évaluation de la conformité ne dépend ni du nombre d'évaluations effectuées, ni de leurs résultats.

9. Les organismes d'évaluation de la conformité souscrivent une assurance couvrant leur responsabilité civile, à moins que cette responsabilité ne soit couverte par l'État sur la base du droit national ou que l'évaluation de la conformité ne soit effectuée sous la responsabilité directe de l'État membre.

10. Le personnel d'un organisme d'évaluation de la conformité est lié par le secret professionnel pour toutes les informations dont il prend connaissance dans l'exercice de ses fonctions dans le cadre de l'annexe VI ou de toute disposition de droit national lui donnant effet, sauf à l'égard des autorités de surveillance du marché de l'État membre où il exerce ses activités. Les droits de propriété sont protégés. L'organisme d'évaluation de la conformité dispose de procédures documentées garantissant le respect du présent paragraphe.

11. Les organismes d'évaluation de la conformité participent aux activités de normalisation pertinentes et aux activités du groupe de coordination des organismes notifiés établi en vertu de l'article 40, ou veillent à ce que leur personnel d'évaluation en soit informé, et appliquent comme lignes directrices les décisions et les documents administratifs résultant du travail de ce groupe.

12. Les organismes d'évaluation de la conformité agissent conformément à un ensemble de conditions cohérentes, justes et raisonnables, notamment en tenant compte des intérêts des PME pour ce qui est des redevances.

Article 30

Présomption de conformité des organismes notifiés

Lorsqu'un organisme d'évaluation de la conformité démontre sa conformité avec les critères fixés dans les normes harmonisées concernées, ou dans des parties de ces normes, dont les références ont été publiées au *Journal officiel de l'Union européenne*, il est présumé répondre

aux exigences énoncées à l'article 29 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

Article 31

Filiales et sous-traitants des organismes notifiés

1. Lorsqu'un organisme notifié sous-traite des tâches spécifiques dans le cadre de l'évaluation de la conformité ou a recours à une filiale, il s'assure que le sous-traitant ou la filiale répond aux exigences définies à l'article 29 et informe l'autorité notifiante en conséquence.
2. Les organismes notifiés assument l'entière responsabilité des tâches accomplies par les sous-traitants ou filiales, quel que soit leur lieu d'établissement.
3. Des activités ne peuvent être sous-traitées ou réalisées par une filiale qu'avec l'accord du fabricant.
4. Les organismes notifiés tiennent à la disposition de l'autorité notifiante les documents pertinents concernant l'évaluation des qualifications du sous-traitant ou de la filiale et le travail exécuté par celui-ci ou celle-ci en vertu du présent règlement.

Article 32

Demande de notification

1. Un organisme d'évaluation de la conformité soumet une demande de notification à l'autorité notifiante de l'État membre dans lequel il est établi.
2. Cette demande est accompagnée d'une description des activités d'évaluation de la conformité, de la ou des procédures d'évaluation de la conformité et du ou des produits pour lesquels cet organisme se déclare compétent, ainsi que d'un certificat d'accréditation, lorsqu'il existe, délivré par un organisme national d'accréditation, qui atteste que l'organisme d'évaluation de la conformité remplit les exigences définies à l'article 29.
3. Lorsque l'organisme d'évaluation de la conformité ne peut produire le certificat d'accréditation, il présente à l'autorité notifiante toutes les preuves documentaires nécessaires à la vérification, à la reconnaissance et au contrôle régulier de sa conformité avec les exigences définies à l'article 29.

Article 33

Procédure de notification

1. Les autorités notifiantes ne peuvent notifier que les organismes d'évaluation de la conformité qui ont satisfait aux exigences énoncées à l'article 29.
2. L'autorité notifiante notifie la Commission et les autres États membres à l'aide du système d'information NANDO (New Approach Notified and Designated Organisations) mis en place et géré par la Commission.
3. La notification comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et le ou les produits concernés, ainsi que l'attestation de compétence correspondante.
4. Lorsqu'une notification n'est pas fondée sur le certificat d'accréditation visé à l'article 32, paragraphe 2, l'autorité notifiante fournit à la Commission et aux autres

États membres les preuves documentaires qui attestent de la compétence de l'organisme d'évaluation de la conformité et des dispositions en place pour garantir que cet organisme sera régulièrement contrôlé et continuera à satisfaire aux exigences énoncées à l'article 29.

5. L'organisme concerné ne peut effectuer les activités propres à un organisme notifié que si aucune objection n'est émise par la Commission ou les autres États membres dans un délai de deux semaines à compter d'une notification dans laquelle il est fait usage d'un certificat d'accréditation, ou dans un délai de deux mois, s'il n'en est pas fait usage.

   Seul un tel organisme est considéré comme un organisme notifié aux fins du présent règlement.

6. La Commission et les autres États membres sont avertis de toute modification pertinente apportée ultérieurement à la notification.

Article 34

Numéros d'identification et liste des organismes notifiés

1. La Commission attribue un numéro d'identification à chaque organisme notifié.

   Elle attribue un seul numéro, même si l'organisme est notifié au titre de plusieurs actes de l'Union.

2. La Commission rend publique la liste des organismes notifiés au titre du présent règlement et y mentionne les numéros d'identification qui leur ont été attribués et les activités pour lesquelles ils ont été notifiés.

   La Commission veille à ce que cette liste soit tenue à jour.

Article 35

Modifications apportées à la notification

1. Lorsqu'une autorité notifiante a établi ou a été informée qu'un organisme notifié ne répond plus aux exigences énoncées à l'article 29, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la notification à des restrictions, la suspend ou la retire, selon le cas, en fonction de la gravité du non-respect de ces exigences ou du non-acquittement de ces obligations. Elle en informe immédiatement la Commission et les autres États membres.

2. En cas de restriction, de suspension ou de retrait d'une notification, ou lorsque l'organisme notifié a cessé ses activités, l'État membre notifiant prend les mesures qui s'imposent pour faire en sorte que les dossiers dudit organisme soient traités par un autre organisme notifié ou tenus à la disposition des autorités notifiantes et des autorités de surveillance du marché compétentes qui en font la demande.

Article 36

Contestation de la compétence des organismes notifiés

1. La Commission enquête sur tous les cas dans lesquels elle nourrit des doutes ou est avertie de doutes quant à la compétence d'un organisme notifié ou au fait qu'il continue à remplir les exigences qui lui sont applicables et à s'acquitter des responsabilités qui lui incombent.

2. L’État membre notifiant communique à la Commission, sur demande, toutes les informations relatives au fondement de la notification ou au maintien de la compétence de l’organisme concerné.

3. La Commission veille à ce que toutes les informations sensibles obtenues au cours de ses enquêtes soient traitées de manière confidentielle.

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences relatives à sa notification, elle en informe l'État membre notifiant et l'invite à prendre les mesures correctives qui s'imposent, y compris la dénotification si nécessaire.

Article 37

Obligations opérationnelles des organismes notifiés

1. Les organismes notifiés réalisent les évaluations de la conformité dans le respect des procédures d’évaluation de la conformité prévues à l’article 24 et à l’annexe VI.

2. Les évaluations de la conformité sont effectuées de manière proportionnée, en évitant d'imposer des charges inutiles aux opérateurs économiques. Les organismes d’évaluation de la conformité accomplissent leurs activités en tenant dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit en question et de la nature en masse, ou série, du processus de production.

3. Les organismes notifiés respectent toutefois le degré de rigueur et le niveau de protection requis pour la conformité du produit avec les dispositions du présent règlement.

4. Lorsqu'un organisme notifié constate que les exigences définies dans l’annexe I ou dans les normes harmonisées correspondantes ou les spécifications communes telles que visées à l’article 19 n'ont pas été remplies par un fabricant, il invite celui-ci à prendre les mesures correctives appropriées et ne délivre pas de certificat de conformité.

5. Lorsque, au cours du contrôle de la conformité faisant suite à la délivrance d’un certificat de conformité, un organisme notifié constate qu’un produit ne respecte plus les exigences définies par le présent règlement, il exige du fabricant qu’il prenne les mesures correctrices appropriées et suspend ou retire le certificat si nécessaire.

6. Lorsque des mesures correctives ne sont pas prises ou n’ont pas l’effet requis, l’organisme notifié soumet le certificat à des restrictions, le suspend ou le retire, le cas échéant.

Article 38

Obligation des organismes notifiés en matière d’information

1. Les organismes notifiés communiquent à l’autorité notifiante les éléments suivants:

   (a) tout refus, restriction, suspension ou retrait d'un certificat;

   (b) toute circonstance ayant une incidence sur la portée et les conditions de la notification;

   (c) toute demande d’information reçue des autorités de surveillance du marché concernant des activités d’évaluation de la conformité;

(d) sur demande, les activités d'évaluation de la conformité réalisées dans le cadre de leur notification et toute autre activité réalisée, y compris les activités transfrontières et sous-traitées.

2. Les organismes notifiés fournissent aux autres organismes notifiés au titre du présent règlement qui effectuent des activités similaires d'évaluation de la conformité couvrant les mêmes produits des informations pertinentes sur les questions relatives aux résultats négatifs de l'évaluation de la conformité et, sur demande, aux résultats positifs.

Article 39

Partage d'expérience

La Commission veille à l'organisation du partage d'expérience entre les autorités nationales des États membres responsables de la politique de notification.

Article 40

Coordination des organismes notifiés

1. La Commission veille à ce qu'une coordination et une coopération appropriées s'établissent entre les organismes notifiés et soient dûment encadrées sous la forme d'un groupe transsectoriel d'organismes notifiés.

2. Les États membres veillent à ce que les organismes qu'ils ont notifiés participent aux travaux de ce groupe, directement ou par l'intermédiaire de représentants désignés.

CHAPITRE V

SURVEILLANCE DU MARCHÉ ET CONTRÔLE DE L'APPLICATION DE LA LÉGISLATION

Article 41

Surveillance du marché et contrôle des produits comportant des éléments numériques sur le marché de l'Union

1. Le règlement (UE) 2019/1020 s'applique aux produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement.

2. Chaque État membre désigne une ou plusieurs autorités de surveillance du marché chargées de veiller à la mise en œuvre effective du présent règlement. Les États membres peuvent désigner une autorité existante ou une nouvelle autorité qui agit en tant qu'autorité de surveillance du marché aux fins du présent règlement.

3. Le cas échéant, les autorités de surveillance du marché coopèrent avec les autorités nationales de certification de cybersécurité désignées en vertu de l'article 58 du règlement (UE) 2019/881 et échangent régulièrement des informations. Les autorités de surveillance du marché désignées coopèrent avec l'ENISA en ce qui concerne le contrôle de la mise en œuvre des obligations en matière de communication d'informations prévues à l'article 11 du présent règlement.

4. Le cas échéant, les autorités de surveillance du marché coopèrent avec d'autres autorités de surveillance du marché désignées sur la base d'autres législations

d'harmonisation de l'Union pour d'autres produits et échangent des informations régulièrement.

5. Les autorités de surveillance du marché coopèrent, s'il y a lieu, avec les autorités chargées de la surveillance du droit de l'Union en matière de protection des données. Cette coopération consiste notamment à informer ces autorités de toute conclusion pertinente pour l'exercice de leurs compétences, y compris lors de la publication d'orientations et de conseils en vertu du paragraphe 8 du présent article, si ces orientations et conseils concernent le traitement de données à caractère personnel.

   Les autorités chargées de la surveillance du droit de l'Union en matière de protection des données sont habilitées à demander toute documentation rédigée ou tenue à jour en vertu du présent règlement et à y accéder lorsque l'accès à ces documents est nécessaire à l'accomplissement de leurs tâches. Elles informent les autorités de surveillance du marché désignées de l'État membre concerné de toute demande en ce sens.

6. Les États membres veillent à ce que les autorités de surveillance du marché désignées disposent de ressources financières et humaines suffisantes pour mener à bien les tâches qui leur sont confiées en vertu du présent règlement.

7. La Commission facilite les échanges d'expériences entre les autorités de surveillance du marché désignées.

8. Avec le soutien de la Commission, les autorités de surveillance du marché peuvent fournir des orientations et des conseils aux opérateurs économiques sur la mise en œuvre du présent règlement.

9. Chaque année, les autorités de surveillance du marché communiquent à la Commission les résultats des activités de surveillance du marché pertinentes. Les autorités de surveillance du marché désignées communiquent sans retard à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de la concurrence de l'Union.

10. Pour les produits comportant des éléments numériques relevant du champ d'application du présent règlement classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [la législation sur l'IA], les autorités de surveillance du marché désignées aux fins du règlement [la législation sur l'IA] sont les autorités responsables des activités de surveillance du marché requises en vertu du présent règlement. Les autorités de surveillance du marché désignées en vertu du règlement [la législation sur l'IA] coopèrent, le cas échéant, avec les autorités de surveillance du marché désignées en vertu du présent règlement et, en ce qui concerne le contrôle de la mise en œuvre des obligations en matière de communication d'informations prévues à l'article 11, avec l'ENISA. Les autorités de surveillance du marché désignées en vertu du règlement [la législation sur l'IA] informent en particulier les autorités de surveillance du marché désignées en vertu du présent règlement de toute conclusion pertinente pour la réalisation de leurs tâches liées à la mise en œuvre du présent règlement.

11. Un groupe de coopération administrative (ADCO) spécifique est établi pour l'application uniforme du présent règlement, conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. Cet ADCO se compose de

représentants des autorités de surveillance du marché désignées et, si nécessaire, de représentants des bureaux de liaison uniques.

Article 42

Accès aux données et à la documentation

Lorsque cela est nécessaire pour évaluer la conformité des produits comportant des éléments numériques et des processus mis en place par leurs fabricants aux exigences essentielles énoncées à l'annexe I, et sur demande motivée, les autorités de surveillance du marché ont accès aux données requises pour évaluer la conception, le développement, la production et le traitement des vulnérabilités de ces produits, y compris la documentation interne correspondante de l'opérateur économique concerné.

Article 43

Procédure au niveau national concernant les produits comportant des éléments numériques qui présentent un risque de cybersécurité important

1. Lorsque l'autorité de surveillance du marché d'un État membre a des raisons suffisantes de considérer qu'un produit comportant des éléments numériques, y compris son traitement des vulnérabilités, présente un risque de cybersécurité important, elle procède à une évaluation de la conformité de ce produit avec l'ensemble des exigences énoncées dans le présent règlement. Les opérateurs économiques concernés coopèrent comme il se doit avec l'autorité de surveillance du marché.

   Si, au cours de cette évaluation, l'autorité de surveillance du marché constate que le produit comportant des éléments numériques ne respecte pas les exigences énoncées dans le présent règlement, elle invite sans tarder l'opérateur économique en cause à prendre toutes les mesures correctives appropriées pour mettre le produit en conformité avec ces exigences, le retirer du marché ou le rappeler dans un délai raisonnable, proportionné à la nature du risque, qu'elle prescrit.

   L'autorité de surveillance du marché informe l'organisme notifié concerné en conséquence. L'article 18 du règlement (UE) 2019/1020 s'applique aux mesures correctives appropriées.

2. Lorsque l'autorité de surveillance du marché considère que la non-conformité n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres des résultats de l'évaluation et des mesures qu'elle a exigées de l'opérateur.

3. Le fabricant s'assure que toutes les mesures correctives appropriées sont prises pour tous les produits comportant des éléments numériques concernés qu'il a mis à disposition sur le marché dans toute l'Union.

4. Lorsque le fabricant d'un produit comportant des éléments numériques ne prend pas les mesures correctives adéquates dans le délai visé au paragraphe 1, deuxième alinéa, l'autorité de surveillance du marché adopte toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du produit sur son marché national ou pour procéder à son retrait de ce marché ou à son rappel.

   L'autorité informe sans retard la Commission et les autres États membres de ces mesures.

5. Les informations visées au paragraphe 4 contiennent toutes les précisions disponibles, notamment en ce qui concerne les données nécessaires pour identifier les produits comportant des éléments numériques non conformes, l'origine du produit comportant des éléments numériques, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales adoptées et les arguments avancés par l'opérateur concerné. En particulier, l'autorité de surveillance du marché indique si la non-conformité découle d'une ou plusieurs des causes suivantes:

   (a) la non-conformité du produit ou des processus mis en place par le fabricant avec les exigences essentielles énoncées à l'annexe I;

   (b) des lacunes dans les normes harmonisées, les systèmes de certification de cybersécurité ou les spécifications communes visés à l'article 18.

6. Les autorités de surveillance du marché des États membres autres que l'autorité de surveillance du marché de l'État membre qui a entamé la procédure informent sans retard la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du produit concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

7. Lorsque, dans les trois mois suivant la réception des informations mentionnées au paragraphe 4, aucune objection n'a été émise par un État membre ou par la Commission à l'encontre d'une mesure provisoire prise par un État membre, cette mesure est réputée justifiée. Cette disposition est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020.

8. Les autorités de surveillance du marché de tous les États membres veillent à ce que les mesures restrictives appropriées, comme le retrait de leur marché, soient prises sans retard à l'égard du produit concerné.

Article 44

Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 43, paragraphe 4, un État membre soulève des objections à l'encontre d'une mesure prise par un autre État membre ou que la Commission estime que cette mesure est contraire à la législation de l'Union, la Commission entame sans tarder des consultations avec l'État membre et le ou les opérateurs économiques concernés et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission décide si la mesure nationale est justifiée ou non dans un délai de neuf mois suivant la notification visée à l'article 43, paragraphe 4, et communique sa décision à l'État membre concerné.

2. Si la mesure nationale est jugée justifiée, tous les États membres prennent les mesures nécessaires pour s'assurer du retrait du produit comportant des éléments numériques non conforme de leur marché et ils en informent la Commission. Si la mesure nationale est jugée injustifiée, l'État membre concerné la retire.

3. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du produit comportant des éléments numériques est imputée à des lacunes dans les normes

harmonisées, la Commission applique la procédure prévue à l'article 10 du règlement (UE) nº 1025/2012.

4. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du produit comportant des éléments numériques est imputée à des lacunes dans un schéma européen de certification de cybersécurité visé à l'article 18, la Commission examine s'il y a lieu de modifier ou d'abroger l'acte d'exécution visé à l'article 18, paragraphe 4, qui précise la présomption de conformité concernant ce schéma de certification.

5. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du produit comportant des éléments numériques est imputée à des lacunes dans les spécifications communes visées à l'article 19, la Commission examine s'il y a lieu de modifier ou d'abroger l'acte d'exécution visé à l'article 19 qui établit ces spécifications communes.

Article 45

Procédure au niveau de l'UE concernant les produits comportant des éléments numériques qui présentent un risque de cybersécurité important

1. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par l'ENISA, qu'un produit comportant des éléments numériques présentant un risque de cybersécurité important n'est pas conforme aux exigences énoncées dans le présent règlement, elle peut demander aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43.

2. Dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des raisons suffisantes de considérer que le produit visé au paragraphe 1 demeure non conforme aux exigences énoncées dans le présent règlement et qu'aucune mesure effective n'a été prise par les autorités de surveillance du marché concernées, la Commission peut demander à l'ENISA de procéder à une évaluation de la conformité. La Commission en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

3. Se fondant sur l'évaluation de l'ENISA, la Commission peut décider qu'une mesure corrective ou restrictive est nécessaire au niveau de l'Union. À cette fin, elle consulte sans tarder les États membres concernés et le ou les opérateurs économiques concernés.

4. Sur la base de la consultation visée au paragraphe 3, la Commission peut adopter des actes d'exécution afin de décider de mesures correctives ou restrictives au niveau de l'Union, y compris ordonner le retrait du marché du produit ou le rappeler, dans un délai raisonnable, proportionné à la nature du risque. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

5. La Commission communique immédiatement à l'opérateur ou aux opérateurs économiques concernés la décision visée au paragraphe 4. Les États membres exécutent les actes visés au paragraphe 4 sans tarder et en informent la Commission.

6. Les paragraphes 2 à 5 sont applicables pendant la durée de la situation exceptionnelle qui a justifié l'intervention de la Commission et aussi longtemps que le produit concerné n'est pas mis en conformité avec le présent règlement.

Article 46

Produits conformes comportant des éléments numériques qui présentent un risque de cybersécurité important

1. Lorsque, après avoir réalisé une évaluation au titre de l'article 43, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant soient conformes au présent règlement, ils présentent un risque de cybersécurité important ainsi qu'un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, pour la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services proposés au moyen d'un système d'information électronique par des entités essentielles du type visé à [l'annexe I de la directive XXX/XXXX (NIS2)] ou pour d'autres aspects de la protection de l'intérêt public, elle exige de l'opérateur concerné qu'il prenne toutes les mesures appropriées pour faire en sorte qu'une fois mis sur le marché, le produit comportant des éléments numériques et les processus mis en place par le fabricant concerné ne présentent plus ce risque, pour retirer ledit produit du marché ou pour le rappeler dans un délai raisonnable, proportionné à la nature du risque.

2. Le fabricant ou les autres opérateurs concernés s'assurent que des mesures correctives sont prises pour tous les produits comportant des éléments numériques concernés qu'ils ont mis à disposition sur le marché dans toute l'Union dans le délai établi par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

3. L'État membre informe immédiatement la Commission et les autres États membres des mesures prises en application du paragraphe 1. Ces informations comprennent toutes les précisions disponibles, notamment les données nécessaires pour identifier les produits comportant des éléments numériques concernés, leur origine et leur chaîne d'approvisionnement, la nature du risque couru, ainsi que la nature et la durée des mesures nationales adoptées.

4. La Commission entame sans retard des consultations avec les États membres et l'opérateur économique en cause et évalue les mesures nationales prises. En fonction des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, si nécessaire, propose des mesures appropriées.

5. La Commission communique sa décision aux États membres.

6. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par l'ENISA, qu'un produit comportant des éléments numériques, bien que conforme au présent règlement, présente les risques visés au paragraphe 1, elle peut demander aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43 et aux paragraphes 1, 2 et 3 du présent article.

7. Dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des raisons suffisantes de considérer que le produit visé au paragraphe 6 continue

de présenter les risques visés au paragraphe 1 et qu'aucune mesure effective n'a été prise par les autorités nationales de surveillance du marché concernées, la Commission peut demander à l'ENISA de procéder à une évaluation des risques présentés par ledit produit et en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

8. Se fondant sur l'évaluation de l'ENISA visée au paragraphe 7, la Commission peut décider qu'une mesure corrective ou restrictive est nécessaire au niveau de l'Union. À cette fin, elle consulte sans tarder les États membres concernés et le ou les opérateurs concernés.

9. Sur la base de la consultation visée au paragraphe 8, la Commission peut adopter des actes d'exécution afin de décider de mesures correctives ou restrictives au niveau de l'Union, y compris ordonner le retrait du marché du produit ou le rappeler, dans un délai raisonnable, proportionné à la nature du risque. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

10. La Commission communique immédiatement à l'opérateur ou aux opérateurs concernés la décision visée au paragraphe 9. Les États membres exécutent ces actes sans tarder et en informent la Commission.

11. Les paragraphes 6 à 10 sont applicables pendant la durée de la situation exceptionnelle qui a justifié l'intervention de la Commission et aussi longtemps que le produit concerné continue de présenter les risques visés au paragraphe 1.

Article 47

Non-conformité formelle

1. Lorsque l'autorité de surveillance du marché d'un État membre fait l'une des constatations ci-après, elle invite le fabricant concerné à mettre un terme à la non-conformité en question:

   (a) le marquage de conformité a été apposé en violation des articles 21 et 22;

   (b) le marquage de conformité n'a pas été apposé;

   (c) la déclaration UE de conformité n'a pas été établie;

   (d) la déclaration UE de conformité n'a pas été établie correctement;

   (e) le numéro d'identification de l'organisme notifié, qui participe à la procédure d'évaluation de la conformité, le cas échéant, n'a pas été apposé.

   (f) la documentation technique n'est pas disponible ou n'est pas complète.

2. Si la non-conformité visée au paragraphe 1 persiste, l'État membre concerné prend toutes les mesures appropriées pour restreindre ou interdire la mise à disposition du produit comportant des éléments numériques sur le marché ou pour faire en sorte que le produit soit rappelé ou retiré du marché.

Article 48

Activités conjointes des autorités de surveillance du marché

1. Les autorités de surveillance du marché peuvent convenir avec d'autres autorités compétentes de mener des activités conjointes visant à garantir la cybersécurité et la

protection des consommateurs en ce qui concerne des produits spécifiques comportant des éléments numériques mis sur le marché ou mis à disposition sur le marché, en particulier des produits dont il est souvent constaté qu'ils présentent des risques de cybersécurité.

2. La Commission ou l'ENISA peuvent proposer des activités conjointes de contrôle du respect du présent règlement à mener par les autorités de surveillance du marché sur la base d'indications ou d'informations relatives à une non-conformité potentielle, dans plusieurs États membres, de produits relevant du champ d'application du présent règlement, aux exigences fixées par ce dernier.

3. Les autorités de surveillance du marché et la Commission, le cas échéant, veillent à ce que l'accord portant sur la réalisation d'activités conjointes n'engendre pas de concurrence déloyale entre les opérateurs économiques et n'influe pas négativement sur l'objectivité, l'indépendance et l'impartialité des parties à l'accord.

4. Une autorité de surveillance du marché peut utiliser toutes les informations issues des activités menées dans le cadre des enquêtes qu'elle entreprend.

5. L'autorité de surveillance du marché concernée et la Commission, le cas échéant, mettent à la disposition du public l'accord sur les activités conjointes, y compris le nom des parties concernées.

Article 49

Opérations «coup de balai»

1. Les autorités de surveillance du marché peuvent décider de mener des actions de contrôle coordonnées et simultanées (opérations «coup de balai») concernant certains produits ou catégories de produits comportant des éléments numériques afin de vérifier le respect du présent règlement ou de détecter des infractions à celui-ci.

2. Sauf accord contraire des autorités de surveillance du marché participantes, les opérations «coup de balai» sont coordonnées par la Commission. Le coordonnateur de l'opération «coup de balai» peut, s'il y a lieu, publier les résultats agrégés de l'opération.

3. L'ENISA peut identifier, dans l'exécution de ses tâches, y compris sur la base des notifications reçues conformément à l'article 11, paragraphes 1 et 2, des catégories de produits pour lesquelles des opérations «coup de balai» peuvent être organisées. La proposition d'opération «coup de balai» est soumise au coordonnateur potentiel visé au paragraphe 2 pour examen par les autorités de surveillance du marché.

4. Lorsqu'elles mènent des opérations «coup de balai», les autorités de surveillance du marché participantes peuvent faire usage des pouvoirs d'enquête prévus aux articles 41 à 47, ainsi que des autres pouvoirs qui leur sont conférés par le droit national.

5. Les autorités de surveillance du marché peuvent inviter des fonctionnaires de la Commission et d'autres personnes les accompagnant habilitées par la Commission à participer aux opérations «coup de balai».

CHAPITRE VI

POUVOIRS DÉLÉGUÉS ET PROCÉDURE DE COMITÉ

Article 50

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 2, paragraphe 4, à l'article 6, paragraphe 2, à l'article 6, paragraphe 3, à l'article 6, paragraphe 5, à l'article 20, paragraphe 5, et à l'article 23, paragraphe 5, est conféré à la Commission.

3. La délégation de pouvoir visée à l'article 2, paragraphe 4, à l'article 6, paragraphe 2, à l'article 6, paragraphe 3, à l'article 6, paragraphe 5, à l'article 20, paragraphe 5, et à l'article 23, paragraphe 5, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant d'adopter un acte délégué, la Commission consulte les experts désignés par chaque État membre conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu de l'article 2, paragraphe 4, de l'article 6, paragraphe 2, de l'article 6, paragraphe 3, de l'article 6, paragraphe 5, de l'article 20, paragraphe 5, et de l'article 23, paragraphe 5, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil, ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 51

Procédure de comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai pour émettre un avis, le président du comité le décide ou un membre du comité le demande.

CHAPITRE VII

CONFIDENTIALITÉ ET SANCTIONS

Article 52

Confidentialité

1. Toutes les parties associées à l'application du présent règlement respectent la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier:

   (a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil[24];

   (b) l'application effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits;

   (c) les intérêts en matière de sécurité nationale et publique;

   (d) l'intégrité des procédures pénales ou administratives.

2. Sans préjudice du paragraphe 1, les informations échangées à titre confidentiel entre les autorités de surveillance du marché et entre celles-ci, d'une part, et la Commission, d'autre part, ne sont pas divulguées sans l'accord préalable de l'autorité de surveillance du marché dont elles émanent.

3. Les paragraphes 1 et 2 sont sans effet sur les droits et obligations de la Commission, des États membres et des organismes notifiés en matière d'échange d'informations et de diffusion de mises en garde et sur les obligations d'information incombant aux personnes concernées en vertu du droit pénal des États membres.

4. La Commission et les États membres peuvent échanger, si nécessaire, des informations sensibles avec les autorités compétentes de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de protection approprié.

Article 53

Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement par les opérateurs économiques et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions prévues sont effectives, proportionnées et dissuasives.

2. Les États membres informent la Commission, sans retard, du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

---

[24] Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

3. La non-conformité avec les exigences de cybersécurité établies à l'annexe I et avec les obligations énoncées aux articles 10 et 11 fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 2,5 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

4. La non-conformité avec toute autre obligation au titre du présent règlement fait l'objet d'amendes administratives pouvant aller jusqu'à 10 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés et aux autorités de surveillance du marché en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 5 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

6. Pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et il est dûment tenu compte des éléments suivants:

   (a) la nature, la gravité et la durée de l'infraction et de ses conséquences;

   (b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour une infraction similaire;

   (c) la taille et la part de marché de l'opérateur qui commet l'infraction.

7. Les autorités de surveillance du marché qui appliquent des amendes administratives communiquent ces informations aux autorités de surveillance du marché des autres États membres au moyen du système d'information et de communication visé à l'article 34 du règlement (UE) 2019/1020.

8. Chaque État membre établit les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

9. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes sont imposées par les juridictions nationales compétentes ou d'autres organismes, en fonction des compétences établies au niveau national dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

10. Des amendes administratives peuvent être imposées, en fonction des circonstances propres à chaque cas, en plus de toute autre mesure corrective ou restrictive appliquée par les autorités de surveillance du marché pour la même infraction.

CHAPITRE VIII

DISPOSITIONS TRANSITOIRES ET FINALES

Article 54

Modification du règlement (UE) 2019/1020

À l'annexe I du règlement (CE) n° 2019/1020, le point suivant est ajouté:

«71. [Règlement XXX] [législation sur la cyberrésilience]».

Article 55

Dispositions transitoires

1. Les attestations d'examen UE de type et les décisions d'approbation délivrées en ce qui concerne les exigences de cybersécurité applicables aux produits comportant des éléments numériques qui sont soumis à d'autres législations d'harmonisation de l'Union restent valables jusqu'au [42 mois après la date d'entrée en vigueur du présent règlement], à moins qu'elles n'expirent avant cette date, ou sauf disposition contraire dans toute autre législation de l'Union, auquel cas elles restent valables conformément à cette législation de l'Union.
2. Les produits comportant des éléments numériques qui ont été mis sur le marché avant le [date d'application du présent règlement visée à l'article 57] ne sont soumis aux exigences du présent règlement que si, à compter de cette date, ces produits font l'objet de modifications substantielles de leur conception ou de leur utilisation prévue.
3. Par dérogation au paragraphe 2, les obligations prévues à l'article 11 s'appliquent à tous les produits comportant des éléments numériques relevant du champ d'application du présent règlement qui ont été mis sur le marché avant le [date d'application du présent règlement visée à l'article 57].

Article 56

Évaluation et réexamen

Au plus tard le [36 mois après la date d'application du présent règlement] et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Les rapports sont publiés.

Article 57

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du [24 mois après la date d'entrée en vigueur du présent règlement]. Cependant, l'article 11 s'applique à compter du [12 mois après la date d'entrée en vigueur du présent règlement].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. La proposition/l'initiative est relative à:

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

1.4.2. Objectif(s) spécifique(s)

1.4.3. Résultat(s) et incidence(s) attendus

1.4.4. Indicateurs de performance

1.5. Justifications de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

1.5.3. Leçons tirées d'expériences similaires

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (législation sur la cyberrésilience)

1.2. Domaine(s) politique(s) concerné(s)

Réseaux de communication, contenu et technologies

1.3. La proposition/l'initiative est relative à:

× **une action nouvelle**

☐ **une action nouvelle faisant suite à un projet pilote/une action préparatoire**[37]

☐ **la prolongation d'une action existante**

☐ **une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

La proposition poursuit deux objectifs principaux visant à assurer le bon fonctionnement du marché intérieur: 1) **créer les conditions pour le développement de produits comportant des éléments numériques sécurisés** en faisant en sorte que les produits matériels et logiciels soient mis sur le marché avec moins de vulnérabilités et que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit; et 2) **créer des conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques**.

1.4.2. Objectif(s) spécifique(s)

Quatre objectifs spécifiques ont été définis pour la proposition: i) faire en sorte que les fabricants améliorent la sécurité des produits comportant des éléments numériques dès la phase de conception et de développement et tout au long du cycle de vie; ii) assurer un cadre cohérent en matière de cybersécurité, en facilitant la mise en conformité pour les producteurs de matériel et de logiciels; iii) améliorer la transparence des propriétés de sécurité des produits comportant des éléments numériques; et iv) permettre aux entreprises et aux consommateurs d'utiliser les produits comportant des éléments numériques en toute sécurité.

Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

[37] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

La proposition présenterait des avantages significatifs pour les différentes parties intéressées. Du point de vue des entreprises, elle permettrait d'éviter l'application de règles de sécurité divergentes aux produits comportant des éléments numériques et de réduire les coûts de conformité à la législation en matière de cybersécurité. Elle entraînerait une réduction du nombre de cyberincidents, des coûts liés à la gestion de ces incidents et des atteintes à la réputation des entreprises. Pour l'ensemble de l'UE, la réduction subséquente des coûts liés aux incidents affectant les entreprises est estimée à quelque 180 à 290 milliards d'EUR par an[38]. Cette option entraînerait une hausse du chiffre d'affaires des entreprises, résultant de l'augmentation de la demande en produits comportant des éléments numériques. Elle permettrait d'améliorer la réputation mondiale des entreprises, avec, à la clé, un accroissement de la demande en dehors de l'UE. Du point de vue des utilisateurs, l'option privilégiée améliorerait la transparence des propriétés de sécurité des produits et faciliterait l'utilisation de produits comportant des éléments numériques. Les consommateurs et les citoyens bénéficieraient également d'une meilleure protection de leurs droits fondamentaux, tels que la vie privée et la protection des données.

Dans le même temps, la proposition se traduirait par des coûts supplémentaires de mise en conformité et d'application pour les entreprises, les organismes notifiés et les autorités publiques, y compris les autorités d'accréditation et de surveillance du marché. Pour les développeurs de logiciels et les fabricants de matériel, elle entraînera des coûts de conformité directs supplémentaires liés aux nouvelles exigences de sécurité, à l'évaluation de la conformité, à la documentation et aux obligations de signalement, portant potentiellement les coûts relatifs à la conformité globaux à quelque 29 milliards d'EUR pour une valeur de marché estimée à 1 485 milliards d'EUR en chiffre d'affaires[39]. Les utilisateurs, y compris les entreprises, les consommateurs et les citoyens, pourraient voir augmenter les produits comportant des éléments numériques. Toutefois, ces coûts sont à considérer dans le contexte des avantages significatifs décrits ci-dessus.

1.4.3. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Afin de vérifier si les fabricants améliorent la sécurité de leurs produits comportant des éléments numériques dès la phase de conception et de développement et tout au long du cycle de vie de ces produits, plusieurs indicateurs pourraient être pris en considération. Il pourrait s'agir, par exemple, du nombre d'incidents significatifs dans l'Union imputables à des vulnérabilités, de la proportion de fabricants de matériel et de logiciels qui suivent un cycle de développement sécurisé systématique, d'une analyse qualitative de la sécurité des produits comportant des éléments numériques, d'une évaluation quantitative et qualitative des bases de données sur les vulnérabilités, de la fréquence des correctifs de sécurité mis à disposition par les fabricants ou du nombre moyen de jours entre la découverte de vulnérabilités et la fourniture de correctifs de sécurité.

---

38 Voir [Document de travail des services de la Commission sur l'analyse d'impact accompagnant le règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques].

39 Voir [Document de travail des services de la Commission sur l'analyse d'impact accompagnant le règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques].

L'absence de législation nationale ciblée et spécifique aux produits en matière de cybersécurité pourrait être un indicateur confirmant l'existence d'un cadre cohérent de cybersécurité .

S'agissant des propriétés de sécurité des produits comportant des éléments numériques, la part de ces produits qui sont expédiés accompagnés d'informations sur lesdites propriétés pourrait être un indicateur de transparence accrue. En outre, la part des produits comportant des éléments numériques fournis avec des instructions pour une utilisation sécurisée pourrait servir d'indicateur pour déterminer si les organisations et les consommateurs sont mis en position d'utiliser les produits en question de manière sûre.

En ce qui concerne le suivi des effets du règlement, plusieurs indicateurs seraient examinés. Ceux-ci seraient évalués par la Commission, le cas échéant avec le soutien de l'ENISA. Selon l'objectif opérationnel à atteindre, ces indicateurs de suivi du succès des exigences horizontales en matière de cybersécurité pourraient être les suivants, par exemple:

Pour évaluer le niveau de cybersécurité des produits comportant des éléments numériques:

- statistiques et analyses qualitatives relatives aux incidents qui touchent les produits comportant des éléments numériques et la manière dont ces incidents ont été gérés. Ces données pourraient être recueillies et évaluées par la Commission, avec le soutien de l'ENISA;

- enregistrements des vulnérabilités connues et analyse de la façon dont elles ont été gérées. Ladite analyse pourrait être réalisée par l'ENISA, à l'aide de la base de données européenne relative aux vulnérabilités établie conformément à la [directive XXX/XXXX (SRI 2)];

- enquêtes auprès des fabricants de matériel et de logiciels pour suivre les progrès accomplis.

Pour évaluer le niveau d'information sur les dispositifs de sécurité, l'assistance en matière de sécurité, la fin de vie et le devoir de diligence: les résultats des enquêtes menées par la Commission, avec le soutien de l'ENISA, auprès des utilisateurs et des entreprises.

Pour évaluer la mise en œuvre, la Commission s'efforcerait de s'assurer que les évaluations de la conformité sont effectivement réalisées. À cette fin, une demande de normalisation sera émise et sa mise en œuvre sera suivie. La Commission vérifiera également la capacité des organismes notifiés et, le cas échéant, des organismes de certification.

S'agissant de l'application, la Commission vérifiera, au moyen des rapports des États membres, qu'aucune initiative nationale ne porte sur des aspects couverts par le règlement.

1.5. Justifications de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Le règlement devrait être pleinement applicable 24 mois après son entrée en vigueur. Toutefois, certains éléments de la structure de gouvernance devraient être en place avant cette date. En particulier, les États membres devraient avoir désigné des

autorités existantes et/ou créé de nouvelles autorités pour accomplir les tâches énoncées dans la législation avant cette date.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

La nature fortement transfrontière de la cybersécurité et le nombre croissant d'incidents ayant des retombées transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs ne peuvent pas être atteints efficacement par les seuls États membres. Compte tenu du caractère mondial des marchés de produits comportant des éléments numériques, les États membres sont confrontés, sur leur territoire, aux mêmes risques pour un même produit. L'émergence d'un cadre fragmenté de règles nationales potentiellement divergentes risque d'entraver la création d'un marché unique ouvert et concurrentiel pour les produits comportant des éléments numériques. Une action commune au niveau de l'UE est donc nécessaire pour accroître le niveau de confiance parmi les utilisateurs et renforcer l'attractivité des produits européens comportant des éléments numériques. Elle profiterait également au marché intérieur en assurant la sécurité juridique et en créant des conditions de concurrence équitables pour les fournisseurs de produits comportant des éléments numériques.

1.5.3. Leçons tirées d'expériences similaires

Le règlement sur la cyberrésilience est le premier règlement en son genre, et le premier à introduire des exigences de cybersécurité pour la mise sur le marché de produits contenant des éléments numériques. Il s'appuie toutefois, pour ce faire, sur la définition du nouveau cadre législatif et sur les enseignements tirés du processus de mise en œuvre de la législation d'harmonisation de l'Union existante pour divers produits, notamment en ce qui concerne la préparation de la mise en œuvre, y compris des aspects tels que la préparation de normes harmonisées.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Le règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques définit de nouvelles exigences de cybersécurité pour tous les produits comportant des éléments numériques mis sur le marché de l'Union, allant au-delà de toutes les exigences prévues par la législation en vigueur. Dans le même temps, la proposition s'appuie sur le cadre existant des dispositions du nouveau cadre législatif. Par conséquent, elle s'appuierait sur les structures et procédures existantes du nouveau cadre législatif, telles que la coopération des organismes notifiés et la surveillance du marché, les modules d'évaluation de la conformité, ou encore l'élaboration de normes harmonisées. La nouvelle proposition s'appuierait également sur certaines structures élaborées conformément à d'autres législations en matière de cybersécurité, telles que la directive 2016/1148 (directive SRI), ou la [directive XXX/XXXX (SRI 2)], et le règlement (UE) 2019/881 (règlement sur la cybersécurité).

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

La gestion des domaines d'action assignés à l'ENISA s'inscrit dans son mandat et ses tâches générales. Ces domaines d'action peuvent nécessiter des profils spécifiques ou de nouvelles affectations, mais ces besoins ne seraient pas significatifs et pourraient être couverts par les ressources existantes de l'ENISA et par la redistribution ou l'association de diverses missions. Par exemple, l'un des principaux domaines d'action assignés à l'ENISA concerne la collecte et le traitement des notifications des fabricants portant sur les vulnérabilités des produits exploitées. En vertu de la [directive XXX/XXXX (SRI 2)], l'ENISA a déjà été chargée d'établir une base de données européenne rassemblant les vulnérabilités connues du public, sur une base volontaire, afin de permettre aux utilisateurs de prendre des mesures d'atténuation appropriées. Les ressources allouées à cette fin pourraient également être utilisées pour les nouvelles missions susmentionnées en lien avec la notification des vulnérabilités des produits. Cela pourrait garantir une utilisation efficace des ressources existantes et créerait également les synergies nécessaires entre ces missions, qui pourraient mieux éclairer les analyses de l'ENISA sur les risques et les menaces en matière de cybersécurité.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **Durée limitée**

– ☐ en vigueur à partir du/de [JJ/MM]AAAA jusqu'au/en [JJ/MM]AAAA

– ☐ Incidence financière de AAAA à AAAA pour les crédits d'engagement et de AAAA à AAAA pour les crédits de paiement.

× **Durée illimitée**

– Mise en œuvre avec une période de montée en puissance à compter de 2025,

– puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[40]

☐ **Gestion directe** par la Commission

– x par ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou des organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☐ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des entités de droit privé investies d'une mission de service public, pour autant qu'elles soient dotées de garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

Le présent règlement assigne certaines actions à l'ENISA, conformément à son mandat existant, et en particulier à l'article 3, paragraphe 2, du règlement (UE) 2019/881 établissant que l'ENISA doit accomplir les tâches qui lui sont assignées par les actes juridiques de

[40] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://ecas.ec.europa.eu/cas/index.html?loginRequestId=ECAS_LR-1668953-ySWYC8rfeTHsCf85fEZI2E7ohdSSOm2BzkFVWlROEGN5NJ9h8y4DYTzzbgiNT9d3mlr5NVsUk11KGFeygCSzVqW-rS0vSrmBGYC95n4fQxJIKm-gBoqEdR0TYsNIawYrXsyypthrmbmNLUtGSoc0uXMgGuSfmwWBcOoNoqcPStZJeiuyD5GGLDMlb7cUoEW340ruW

l'Union qui définissent des mesures de rapprochement des dispositions législatives, réglementaires et administratives des États membres relatives à la cybersécurité. L'ENISA est ainsi notamment chargée de recevoir les notifications des fabricants concernant les vulnérabilités activement exploitées contenues dans les produits comportant des éléments numériques ainsi que les incidents ayant un impact sur la sécurité de ces produits. L'ENISA devrait également transmettre ces notifications aux CSIRT concernés ou, respectivement, au point de contact unique concerné désigné conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] des États membres, et en informer les autorités de surveillance du marché. Sur la base des informations qu'elle recueille, l'ENISA devrait préparer un rapport technique bisannuel sur les tendances émergentes concernant les risques de cybersécurité dans les produits comportant des éléments numériques et le soumettre au groupe de coopération SRI. En outre, compte tenu de son expertise, des informations recueillies et des analyses des menaces, l'ENISA peut soutenir le processus de mise en œuvre du présent règlement en proposant des activités conjointes à mener par les autorités nationales de surveillance du marché sur la base d'indications ou d'informations relatives à une non-conformité potentielle, dans plusieurs États membres, de produits comportant des éléments numériques au présent règlement ou recenser les catégories de produits pour lesquelles des actions de contrôle coordonnées simultanées peuvent être organisées. La Commission peut demander à l'ENISA de procéder à des évaluations portant sur des produits spécifiques dans des circonstances exceptionnelles en relation avec des produits comportant des éléments numériques qui présentent un risque de cybersécurité important et pour lesquels une intervention immédiate est nécessaire afin de préserver le bon fonctionnement du marché intérieur.

Toutes ces missions sont estimées à environ 4,5 ETP sur les ressources existantes de l'ENISA, en s'appuyant déjà sur son expertise et sur les travaux préparatoires qu'elle effectue actuellement, entre autres à l'appui de la mise en œuvre prochaine de la [directive XXX/XXXX (SRI 2)] en vue de laquelle les ressources de l'ENISA ont été étoffées.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Au plus tard 36 mois après la date d'application du présent règlement et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Les rapports sont rendus publics.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

Le présent règlement établit une nouvelle politique en ce qui concerne les exigences harmonisées en matière de cybersécurité applicables aux produits comportant des éléments numériques mis sur le marché intérieur tout au long de leur cycle de vie.

L'acte juridique sera suivi par des demandes adressées par la Commission aux organisations européennes de normalisation pour qu'elles élaborent des normes.

Afin qu'ils soient en mesure d'assumer ces nouvelles tâches, il est nécessaire de doter les services de la Commission des ressources appropriées. On estime que l'application du nouveau règlement nécessite 7 ETP (dont un END) pour couvrir les tâches suivantes:

- préparer la demande de normalisation et/ou les spécifications communes via des actes d'exécution en l'absence de processus de normalisation réussi;
- élaborer un acte délégué [dans un délai de douze mois à compter de l'entrée en vigueur du règlement] précisant les définitions des produits critiques comportant des éléments numériques;
- préparer, le cas échéant, des actes délégués pour la mise à jour de la liste des produits critiques des classes I et II; préciser si une limitation ou une exclusion est nécessaire pour les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui établissent des exigences assurant le même niveau de protection que le présent règlement; rendre obligatoire la certification de certains produits hautement critiques comportant des éléments numériques sur la base des critères énoncés dans le présent règlement; spécifier le contenu minimal de la déclaration UE de conformité et compléter les éléments à inclure dans la documentation technique;
- élaborer, le cas échéant, des actes d'exécution relatifs au format ou aux éléments des signalements obligatoires, à la nomenclature des logiciels, aux spécifications communes ou à l'apposition du marquage CE;
- préparer, le cas échéant, une intervention immédiate en vue d'imposer des mesures correctives ou restrictives dans des circonstances exceptionnelles afin de préserver le bon fonctionnement du marché intérieur, y compris l'élaboration d'un acte d'exécution;
- organiser et coordonner les notifications par les États membres des organismes notifiés et coordonner les organismes notifiés;

– soutenir la coordination des autorités de surveillance des marchés des États membres.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

Afin de garantir que les organismes notifiés et les autorités de surveillance du marché échangent des informations et coopèrent bien, la Commission se chargera de leur coordination. Pour l'expertise technique et commerciale, un groupe d'experts serait créé.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. S'agissant des frais de réunion, compte tenu du faible montant par transaction (par exemple, remboursement des frais de déplacement d'un délégué pour une réunion), les procédures de contrôle types semblent suffisantes. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

Les mesures de prévention des fraudes existantes applicables à la Commission couvriront les crédits supplémentaires nécessaires aux fins du présent règlement.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Schéma

- Nouvelles lignes budgétaires, dont la création est demandée

Sans objet

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

– ☑ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	Numéro	

DG: <…….>			Année **N**[41]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire pour refléter la durée de l'incidence (cf. point 1.6)			**TOTAL**
• Crédits opérationnels										
Ligne budgétaire[42]	Engagements	(1a)								
	Paiements	(2 a)								
Ligne budgétaire	Engagements	(1b)								
	Paiements	(2b)								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[43]										
Ligne budgétaire		(3)								
TOTAL des crédits	Engagements	=1a+1b +3								

41 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

42 Selon la nomenclature budgétaire officielle.

43 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

Pour la DG <…….>	Paiements	=2a+2b +3								

• TOTAL des crédits opérationnels	Engagements	(4)								
	Paiements	(5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)								
TOTAL des crédits pour la RUBRIQUE <….> du cadre financier pluriannuel	Engagements	=4+6								
	Paiements	=5+6								

Si plusieurs rubriques opérationnelles sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

• TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	(4)								
	Paiements	(5)								
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		(6)								
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (Montant de référence)	Engagements	=4+6								
	Paiements	=5+6								

Rubrique du cadre financier pluriannuel	7	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe V des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
DG: CNECT						
• Ressources humaines		1,030	1,030	1,030	1,030	**4,120**
• Autres dépenses administratives		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTAL DG CNECT	Crédits	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

En Mio EUR (à la 3e décimale)

		Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Engagements	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Paiements	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **N**		Année **N+1**		Année **N+2**		Année **N+3**		Insérer autant d'années que nécessaire pour refléter la durée de l'incidence (cf. point 1.6)						**TOTAL**	
	RÉALISATIONS																	
	Type 44	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[45]…																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique n° 1																		
OBJECTIF SPÉCIFIQUE n° 2…																		
- Réalisation																		
Sous-total objectif spécifique nº 2																		
TOTAUX																		

[44] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[45] Tel que décrit au point 1.4.2. «Objectif(s) spécifique(s)…».

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2024**	Année **2025**	Année **2026**	Année **2027**	
RUBRIQUE 7 du cadre financier pluriannuel					
Ressources humaines	1,030	1,030	1,030	1,030	**4,120**
Autres dépenses administratives	0,222	0,222	0,222	0,222	**0,888**
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	1,252	1,252	1,252	1,252	**5,008**
Hors RUBRIQUE 7[46] du cadre financier pluriannuel					
Ressources humaines					
Autres dépenses de nature administrative					
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel					
TOTAL	1,252	1,252	1,252	1,252	**5,008**

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

[46] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.1. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☑ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

		Année **2024**	Année **2025**	Année **2026**	Année **2027**
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		6	6	6	6
20 01 02 03 (délégations)					
01 01 01 01 (recherche indirecte)					
01 01 01 11 (recherche directe)					
Autres lignes budgétaires (à spécifier)					
• Personnel externe (en équivalent temps plein: ETP)[47]					
20 02 01 (AC, END, INT de l'enveloppe globale)		1	1	1	1
20 02 03 (AC, AL, END, INT et JPD dans les délégations)					
XX 01 xx **yy zz** [48]	- au siège				
	- en délégation				
01 01 01 02 (AC, END, INT sur recherche indirecte)					
01 01 01 12 (AC, END, INT sur recherche directe)					
Autres lignes budgétaires (à spécifier)					
TOTAL		**7**	**7**	**7**	**7**

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires 6 ETP x 157 000 EUR/an = 942 000 EUR	Tel que décrit au point 2.2.1.: – préparer la demande de normalisation et/ou les spécifications communes via des actes d'exécution en l'absence de processus de normalisation réussi; – élaborer un acte délégué [dans un délai de douze mois à compter de l'entrée en vigueur du règlement] précisant les définitions des produits critiques comportant des éléments numériques; – préparer, le cas échéant, des actes délégués pour la mise à jour de la liste des produits critiques des classes I et II; préciser si une limitation ou une exclusion est nécessaire pour les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui établissent des exigences assurant le même niveau de protection que le présent règlement; rendre obligatoire la certification de certains produits hautement critiques comportant des éléments numériques sur la base des critères énoncés dans le présent règlement; spécifier le contenu minimal de la déclaration UE de conformité et compléter les éléments à inclure dans la documentation

[47] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[48] Sous-plafond de personnel externe financé sur crédits opérationnels (anciennes lignes «BA»).

	technique; – élaborer, le cas échéant, des actes d'exécution relatifs au format ou aux éléments des signalements obligatoires, à la nomenclature des logiciels, aux spécifications communes ou à l'apposition du marquage CE; – préparer, le cas échéant, une intervention immédiate en vue d'imposer des mesures correctives ou restrictives dans des circonstances exceptionnelles afin de préserver le bon fonctionnement du marché intérieur, y compris l'élaboration d'un acte d'exécution; – organiser et coordonner les notifications par les États membres des organismes notifiés et coordonner les organismes notifiés; – soutenir la coordination des autorités de surveillance des marchés des États membres.
Personnel externe 1 END x 88 000 EUR/an	Tel que décrit au point 2.2.1.: – préparer la demande de normalisation et/ou les spécifications communes via des actes d'exécution en l'absence de processus de normalisation réussi; – élaborer un acte délégué [dans un délai de douze mois à compter de l'entrée en vigueur du règlement] précisant les définitions des produits critiques comportant des éléments numériques; – préparer, le cas échéant, des actes délégués pour la mise à jour de la liste des produits critiques des classes I et II; préciser si une limitation ou une exclusion est nécessaire pour les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui établissent des exigences assurant le même niveau de protection que le présent règlement; rendre obligatoire la certification de certains produits hautement critiques comportant des éléments numériques sur la base des critères énoncés dans le présent règlement; spécifier le contenu minimal de la déclaration UE de conformité et compléter les éléments à inclure dans la documentation technique; – élaborer, le cas échéant, des actes d'exécution relatifs au format ou aux éléments des signalements obligatoires, à la nomenclature des logiciels, aux spécifications communes ou à l'apposition du marquage CE; – préparer, le cas échéant, une intervention immédiate en vue d'imposer des mesures correctives ou restrictives dans des circonstances exceptionnelles afin de préserver le bon fonctionnement du marché intérieur, y compris l'élaboration d'un acte d'exécution; – organiser et coordonner les notifications par les États membres des organismes notifiés et coordonner les organismes notifiés; – soutenir la coordination des autorités de surveillance des marchés des États membres.

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

– x peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Il n'y a pas lieu de procéder à une reprogrammation.

– ☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

-

– ☐ nécessite une révision du CFP.

-

3.2.5. Participation de tiers au financement

La proposition/l'initiative:

– x ne prévoit pas de cofinancement par des tierces parties.

– ☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[49]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

[49] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

– ☐ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a l'incidence financière décrite ci-après:

– ☐ sur les ressources propres

– ☐ sur les autres recettes

– Veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐.

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[50]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes affectées, préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[50] En ce qui concerne les ressources propres traditionnelles (droits de douane et cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.