UNION EUROPÉENNE

LE PARLEMENT EUROPÉEN **LE CONSEIL**

Bruxelles, le 25 septembre 2024
(OR. en)

2022/0272(COD) **PE-CONS 100/23**

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience)

RÈGLEMENT (UE) 2024/...
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du ...

concernant des exigences de cybersécurité horizontales
pour les produits comportant des éléments numériques
et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020
et la directive (UE) 2020/1828 (règlement sur la cyberrésilience)

(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],

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire[2],

---

1 JO C 100 du 16.3.2023, p. 101.

2 Position du Parlement européen du 12 mars 2024 (non encore parue au Journal officiel) et décision du Conseil du ….

considérant ce qui suit:

(1) La cybersécurité est l'un des grands enjeux de l'Union. Le nombre et la diversité des dispositifs connectés ne cesseront d'augmenter dans les prochaines années. Les cyberattaques sont une question d'intérêt public, car elles ont des conséquences très importantes non seulement sur l'économie de l'Union, mais également sur la démocratie ainsi que sur la sécurité des consommateurs et sur la santé. Il est dès lors nécessaire de renforcer l'approche de l'Union en matière de cybersécurité, d'aborder la cyberrésilience au niveau de l'Union et d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme concernant les exigences essentielles 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 sécurisés comportant des éléments numériques 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, en améliorant par exemple la transparence concernant la période d'assistance pour les produits comportant des éléments numériques mis à disposition sur le marché.

(3) Le droit pertinent de l'Union 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 chaîne d'approvisionnement numérique. Toutefois, le droit existant de l'Union relatif à la cybersécurité, dont le règlement (UE) 2019/881 du Parlement européen et du Conseil[3] et la directive (UE) 2022/2555 du Parlement européen et du Conseil[4], ne couvre pas directement les exigences contraignantes en matière de sécurité des produits comportant des éléments numériques.

---

[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) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

[4] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

(4) Bien que le droit 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 et aux organisations pour se conformer à un certain nombre d'exigences et d'obligations pour des types de produits similaires. La cybersécurité de ces produits revêt une dimension transfrontière particulièrement forte, étant donné que les produits comportant des éléments numériques fabriqués dans un État membre ou un pays tiers 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 afin d'assurer un cadre réglementaire harmonisé et de garantir la sécurité juridique aux utilisateurs, aux organisations et aux entreprises, dont les microentreprises et les petites et moyennes entreprises telles que définies à l'annexe de la recommandation 2003/361/CE de la Commission[5]. Le paysage réglementaire de l'Union devrait être harmonisé en introduisant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques. Il convient en outre de garantir, dans l'ensemble de l'Union, la sécurité juridique des opérateurs économiques et des utilisateurs, ainsi qu'une meilleure harmonisation du marché intérieur et la proportionnalité pour les microentreprises et les petites et moyennes entreprises, en créant des conditions plus viables pour les opérateurs économiques désireux de pénétrer sur le marché de l'Union.

---

[5] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

(5) En ce qui concerne les microentreprises et les petites et moyennes entreprises, les dispositions de l'annexe de la recommandation 2003/361/CE de la Commission devraient être appliquées dans leur intégralité pour déterminer la catégorie dont relève une entreprise. Par conséquent, lors du calcul des effectifs et des seuils financiers définissant les catégories d'entreprises, les dispositions de l'article 6 de l'annexe de la recommandation 2003/361/CE de la Commission relatives à la détermination des données de l'entreprise eu égard à certains types d'entreprises, telles que les entreprises partenaires ou liées, devraient également s'appliquer.

(6) Il convient que la Commission fournisse des orientations afin d'aider les opérateurs économiques, en particulier les microentreprises et les petites et moyennes entreprises, à appliquer le présent règlement. Ces orientations devraient couvrir, entre autres, le champ d'application du présent règlement, en particulier la notion de "traitement de données à distance" et ses implications pour les développeurs de logiciels libres et ouverts, l'application des critères employés pour définir la période d'assistance pour les produits comportant des éléments numériques, l'interaction entre le présent règlement et d'autres actes législatifs de l'Union ainsi que la notion de modification substantielle.

(7) Au niveau de l'Union, divers documents programmatiques et politiques, tels que la communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, datée du 16 décembre 2020 et intitulée "La stratégie de cybersécurité de l'Union pour la décennie numérique", les conclusions du Conseil du 2 décembre 2020 sur la cybersécurité des dispositifs connectés et du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne ou encore la résolution du Parlement européen du 10 juin 2021sur la stratégie de cybersécurité de l'Union pour la décennie numérique[6], 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 tiers introduisent des mesures pour réglementer cette question de leur propre initiative. Dans le rapport final de la conférence sur l'avenir de l'Europe, les citoyens ont préconisé de "renforcer le rôle de l'Union dans la lutte contre les menaces de cybersécurité". Afin de permettre à l'Union de jouer un rôle de premier plan sur la scène internationale dans le domaine de la cybersécurité, il importe d'établir un cadre réglementaire ambitieux.

(8) 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 essentielles de cybersécurité, axées sur l'objectif et technologiquement neutres pour ces produits, qui s'appliquent horizontalement.

---

[6] JO C 67 du 8.2.2022, p. 81.

(9) 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 comportant des éléments numériques soient conçus et développés conformément aux exigences essentielles de cybersécurité prévues par le présent règlement. Cette obligation concerne 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 cybermenaces 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 comportant des éléments numériques qui ne sont connectés qu'indirectement à d'autres dispositifs ou réseaux.

(10) L'établissement d'exigences de cybersécurité des produits comportant des éléments numériques aux fins de leur mise sur le marché vise à renforcer la cybersécurité de ces produits, tant pour les consommateurs que pour les entreprises. Ces exigences garantiront, en outre, que la cybersécurité est intégrée à tous les stades des chaînes d'approvisionnement, rendant ainsi plus sûrs les produits finaux comportant des éléments numériques et leurs composants. 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 ou les systèmes de surveillance pour bébé. Les produits de consommation comportant des éléments numériques qui sont catégorisés, en vertu du présent règlement, comme des produits importants comportant des éléments numériques présentent un risque de cybersécurité plus élevé car leur fonction comporte un risque important d'effets néfastes du fait de leur intensité et de leur capacité à perturber, contrôler ou endommager un grand nombre d'autres produits ou à porter atteinte à la santé, à la sécurité ou à la sûreté de leurs utilisateurs; aussi ces produits devraient-ils faire l'objet d'une procédure plus stricte d'évaluation de la conformité. Cela s'applique aux produits tels que les produits domestiques intelligents comportant des fonctionnalités de sécurité, y compris les serrures intelligentes, les systèmes de surveillances pour bébés et les systèmes d'alarme, les jouets connectés ou les dispositifs portables personnels de santé. En outre, les procédures d'évaluation de la conformité plus strictes auxquelles sont soumis les produits comportant des éléments numériques qui sont catégorisés, en vertu du présent règlement, comme produits critiques ou importants comportant des éléments numériques contribueront à prévenir les répercussions négatives que l'exploitation de vulnérabilités pourrait avoir sur les consommateurs.

(11) Le présent règlement vise à garantir un niveau élevé de cybersécurité des produits comportant des éléments numériques et de leurs solutions intégrées de traitement de données à distance. Ces solutions de traitement de données à distance devraient être définies comme le traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant du produit comportant des éléments numériques concerné ou au nom de celui-ci, et dont l'absence empêcherait le produit d'exécuter l'une de ses fonctions. Grâce à cette approche, les produits concernés sont sécurisés dans leur intégralité et de façon adéquate par leur fabricant, que les données soient traitées ou stockées localement, sur l'appareil de l'utilisateur, ou à distance, par le fabricant. Cependant, le traitement ou le stockage des données à distance ne relèvent du champ d'application du présent règlement que s'ils sont nécessaires à l'exécution des fonctions d'un produit comportant des éléments numériques. Le traitement ou le stockage à distance comprend les cas où une application mobile a besoin d'accéder à une interface de programmation d'application ou à une base de données fournie par l'intermédiaire d'un service développé par le fabricant. Dans cette situation, le service constitue une solution de traitement de données à distance et relève donc du champ d'application du présent règlement. Par conséquent, les exigences relatives aux solutions de traitement de données à distance qui relèvent du champ d'application du présent règlement ne comportent pas de mesures techniques, opérationnelles ou organisationnelles visant à gérer les risques qui pèsent sur la sécurité des réseaux et systèmes d'information d'un fabricant dans leur ensemble.

(12) Les solutions en nuage ne constituent des solutions de traitement de données à distance au sens du présent règlement que si elles répondent à la définition énoncée dans ce dernier. Par exemple, les fonctionnalités en nuage fournies par un fabricant d'appareils domestiques intelligents qui permettent aux utilisateurs de contrôler l'appareil à distance relèvent du champ d'application du présent règlement. À l'inverse, les sites internet qui ne supportent pas la fonctionnalité d'un produit comportant des éléments numériques ou les services en nuage qui ne sont pas conçus et développés sous la responsabilité du fabricant d'un produit comportant des éléments numériques ne relèvent pas du champ d'application du présent règlement. La directive (UE) 2022/2555 s'applique aux services d'informatique en nuage et aux modèles de services en nuage, tels que les logiciels service (SaaS), les plates-formes services (PaaS) et les infrastructures services (IaaS). Les entités qui fournissent des services d'informatique en nuage dans l'Union et qui répondent à la définition des moyennes entreprises énoncée à l'article 2 de l'annexe à la recommandation 2003/361/CE de la Commission, ou qui dépassent les plafonds applicables aux moyennes entreprises prévus au paragraphe 1 dudit article, relèvent du champ d'application de cette directive.

(13) Conformément à l'objectif du présent règlement consistant à éliminer les obstacles à la libre circulation des produits comportant des éléments numériques, les États membres ne devraient pas empêcher, pour les aspects relevant du présent règlement, la mise à disposition sur le marché de produits comportant des éléments numériques conformes au présent règlement. Par conséquent, en ce qui concerne les questions harmonisées par le présent règlement, les États membres ne peuvent pas imposer d'exigences de cybersécurité supplémentaires pour la mise à disposition sur le marché de produits comportant des éléments numériques. Cependant, toute entité, qu'elle soit publique ou privée, peut imposer des exigences, en plus de celles prévues par le présent règlement, pour l'achat de produits comportant des éléments numériques ou leur utilisation à des fins qui lui sont propres, et peut donc choisir d'utiliser des produits comportant des éléments numériques répondant à des exigences de cybersécurité plus strictes ou plus spécifiques que celles qui s'appliquent à la mise à disposition sur le marché en vertu du présent règlement. Sans préjudice des directives 2014/24/UE[7] et 2014/25/UE[8] du Parlement européen et du Conseil, les États membres devraient veiller, lorsqu'ils achètent des produits comportant des éléments numériques qui doivent respecter les exigences essentielles de cybersécurité prévues par le présent règlement, y compris celles relatives à la gestion des vulnérabilités, à ce qu'il soit tenu compte de ces exigences, ainsi que de la capacité du fabricant à appliquer des mesures de cybersécurité et à gérer les cybermenaces de façon efficace, lors des procédures de passation de marchés.

---

7 Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

8 Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et abrogeant la directive 2004/17/CE (JO L 94 du 28.3.2014, p. 243).

En outre, la directive (UE) 2022/2555 établit des mesures de gestion des risques en matière de cybersécurité applicables aux entités essentielles et importantes visées à l'article 3 de ladite directive. Ces mesures pourraient entraîner des mesures de sécurité de la chaîne d'approvisionnement nécessitant l'utilisation, par ces entités, de produits comportant des éléments numériques qui répondent à des exigences de cybersécurité plus strictes que celles prévues par le présent règlement. Conformément à la directive (UE) 2022/2555 et dans le respect de son principe d'harmonisation minimale, les États membres peuvent donc imposer des exigences de cybersécurité supplémentaires applicables à l'utilisation de produits TIC par des entités essentielles ou importantes au titre de ladite directive afin d'assurer un niveau plus élevé de cybersécurité, à condition que ces exigences soient compatibles avec les obligations des États membres prévues par le droit de l'Union. Les facteurs non techniques liés aux produits comportant des éléments numériques et aux fabricants de ces derniers peuvent compter parmi les questions qui ne sont pas régies par le présent règlement. Les États membres peuvent donc adopter des mesures nationales, y compris des restrictions applicables aux produits comportant des éléments numériques ou aux fournisseurs de ces produits, qui tiennent compte de facteurs non techniques. Les mesures nationales liées à ces facteurs sont nécessaires pour respecter le droit de l'Union.

(14) Le présent règlement devrait être sans préjudice de la responsabilité des États membres de préserver la sécurité nationale, conformément au droit de l'Union. Les États membres devraient être en mesure de soumettre à des mesures supplémentaires les produits comportant des éléments numériques achetés ou utilisés à des fins de sécurité nationale ou de défense, à condition que ces mesures soient conformes aux obligations des États membres prévues par le droit de l'Union.

(15) Le présent règlement ne s'applique aux opérateurs économiques qu'en ce qui concerne les produits comportant des éléments numériques mis à disposition sur le marché, donc fournis pour être distribués ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale. La fourniture dans le cadre d'une activité commerciale peut être caractérisée non seulement par le prix facturé pour un produit comportant des éléments numériques, mais également par le prix des services d'assistance technique lorsqu'il ne sert pas uniquement à récupérer les coûts réels, par une intention de monétisation, par exemple par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, par l'exigence, comme condition à l'utilisation, du traitement des données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel, ou par l'acceptation de dons supérieurs aux coûts associés à la conception, au développement et à la fourniture d'un produit comportant des éléments numériques. Le fait d'accepter des dons sans intention lucrative ne devrait pas être considéré comme constitutif d'une activité commerciale.

(16) Aux fins du présent règlement, les produits comportant des éléments numériques fournis dans le cadre d'une prestation de service pour laquelle une rétribution est perçue à la seule fin de récupérer les coûts réels directement liés au fonctionnement de ce service, comme ce peut être le cas de certains produits comportant des éléments numériques fournis par des entités de l'administration publique, ne devraient pas être considérés pour cette seule raison comme constituant une activité commerciale. En outre, les produits comportant des éléments numériques qui sont développés ou modifiés par une entité de l'administration publique exclusivement pour son propre usage ne devraient pas être considérés comme mis à disposition sur le marché au sens du présent règlement.

(17) Les logiciels et données qui sont partagés de manière ouverte, auxquels les utilisateurs peuvent librement accéder et qu'ils peuvent librement utiliser, modifier et redistribuer, dans une version modifiée ou non, peuvent contribuer à la recherche et à l'innovation sur le marché. Pour favoriser le développement et le déploiement de logiciels libres et ouverts, en particulier par les microentreprises et les petites et moyennes entreprises, y compris les jeunes pousses, par les personnes physiques, par les organisations à but non lucratif et par les instituts de recherche universitaires, l'application du présent règlement aux produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts fournis pour être distribués ou utilisés dans le cadre d'une activité commerciale devrait tenir compte de la nature des différents modèles de développement de logiciels distribués et développés sous licences logicielles libres et ouvertes.

(18) On entend par "logiciel libre et ouvert" un logiciel dont le code source est partagé de manière ouverte et dont la licence prévoit tous les droits pour qu'il soit librement accessible, utilisable, modifiable et redistribuable. Les logiciels libres et ouverts sont développés, entretenus et distribués de façon ouverte, y compris par l'intermédiaire de plates-formes en ligne. En ce qui concerne les opérateurs économiques auxquels s'applique le présent règlement, seuls les logiciels libres et ouverts mis à disposition sur le marché, donc fournis pour être distribués ou utilisés dans le cadre d'une activité commerciale, devraient relever du champ d'application du présent règlement. Les seules circonstances dans lesquelles le produit comportant des éléments numériques a été développé ou la manière dont le développement a été financé ne devraient donc pas être prises en considération au moment de déterminer si l'activité en question est de nature commerciale ou non. Plus précisément, aux fins du présent règlement et en ce qui concerne les opérateurs économiques auxquels il s'applique, afin de garantir la distinction claire entre les phases de développement et de fourniture, la fourniture de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui ne sont pas monétisés par leur fabricant ne devrait pas être considérée comme une activité commerciale. En outre, la fourniture de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts, destinés à être intégrés par d'autres fabricants à leurs propres produits comportant des éléments numériques, ne devrait être considérée comme une mise à disposition sur le marché que si le composant est monétisé par son fabricant d'origine. Par exemple, le simple fait qu'un fabricant verse un soutien financier à un logiciel libre comportant des éléments numériques ou qu'il contribue au développement d'un tel produit ne devrait pas en soi suffire à déterminer que cette activité est de nature commerciale.

En outre, les mises à jour régulières de ce logiciel ne devraient pas permettre à elles seules de conclure qu'un produit comportant des éléments numériques est fourni dans le cadre d'une activité commerciale. Enfin, aux fins du présent règlement, le développement par des organisations à but non lucratif de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne devrait pas être considéré comme une activité commerciale, pour autant que l'organisation concernée soit constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs. Le présent règlement ne s'applique pas aux personnes physiques ou morales qui contribuent, sous forme de code source, à des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne relevant pas de leur responsabilité.

(19) Étant donné l'importance que revêtent, en matière de cybersécurité, de nombreux produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui sont publiés mais ne sont pas mis à disposition sur le marché au sens du présent règlement, les personnes morales qui apportent un soutien prolongé au développement de tels produits destinés à des activités commerciales et qui jouent un rôle de premier plan en veillant à la viabilité de ces produits (intendants de logiciels ouverts) devraient être soumises à un régime réglementaire allégé et sur mesure. Figurent parmi les intendants de logiciels ouverts certaines fondations et les entités qui développent et publient des logiciels libres et ouverts dans un cadre commercial, y compris les entités à but non lucratif. Le régime réglementaire devrait tenir compte de leur nature particulière et de leur compatibilité avec le type d'obligations qui leur incombent. Ce régime ne devrait concerner que les produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts et dont la finalité est commerciale, par exemple ceux qui sont destinés à être intégrés à des services commerciaux ou à des produits comportant des éléments numériques monétisés. Aux fins de ce régime réglementaire, l'intention d'intégration à des produits comportant des éléments numériques monétisés couvre les cas où le fabricant qui intègre un composant dans ses propres produits comportant des éléments numériques contribue régulièrement au développement de ce composant ou apporte une assistance financière régulière afin d'assurer la pérennité d'un logiciel. Le fait d'apporter un soutien prolongé au développement d'un produit comportant des éléments numériques comprend, sans s'y limiter, l'hébergement et la gestion de plates-formes collaboratives de développement de logiciels, l'hébergement de code source ou d'un logiciel, l'administration ou la gestion de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ainsi que le pilotage du développement de ces produits. Étant donné que le régime réglementaire allégé et sur mesure n'impose pas aux intendants de logiciels ouverts les mêmes obligations que celles qui incombent aux fabricants en vertu du présent règlement, les intendants de logiciels ouverts ne devraient pas être autorisés à apposer le marquage CE aux produits comportant des éléments numériques dont ils soutiennent le développement.

(20) Le seul fait d'héberger des produits comportant des éléments numériques sur des dépôts ouverts, y compris par l'intermédiaire de progiciels ou de plates-formes collaboratives, ne constitue pas en soi la mise à disposition sur le marché d'un produit comportant des éléments numériques. Les fournisseurs de ces services ne devraient être considérés comme des distributeurs que s'ils mettent ces logiciels à disposition sur le marché, donc s'ils les fournissent pour qu'ils soient distribués ou utilisés sur le marché de l'Union dans le cadre d'une activité commerciale.

(21) Afin de soutenir et de faciliter l'application du devoir de diligence raisonnable par les fabricants qui intègrent à leurs produits comportant des éléments numériques des composants logiciels libres et ouverts qui ne sont pas soumis aux exigences essentielles de cybersécurité énoncées dans le présent règlement, la Commission devrait être en mesure de mettre en place des programmes volontaires d'attestation de sécurité, soit par voie d'un acte délégué complétant le présent règlement, soit en demandant, en vertu de l'article 48 du règlement (UE) 2019/881, un schéma européen de certification de cybersécurité qui tienne compte des spécificités des modèles de développement des logiciels libres et ouverts. Les programmes d'attestation de sécurité devraient être conçus de sorte que non seulement les personnes physiques ou morales qui développent un produit comportant des éléments numériques répondant aux critères d'un logiciel libre et ouvert ou qui participent à son développement, mais aussi des tiers, tels que les fabricants qui intègrent ces produits à leurs propres produits comportant des éléments numériques, les utilisateurs ou les administrations publiques de l'Union ou des États membres, puissent être à l'initiative d'une attestation de sécurité ou la financer.

(22) Au vu des objectifs en matière de cybersécurité que fixe le présent règlement et afin d'améliorer l'appréciation de la situation qu'ont les États membres concernant la dépendance de l'Union à l'égard des composants logiciels, en particulier les composants potentiellement libres et ouverts, un groupe de coopération administrative (ADCO) spécifique, institué par le présent règlement, devrait pouvoir décider d'enclencher conjointement une évaluation des dépendances de l'Union. Il convient que les autorités de surveillance du marché puissent exiger des fabricants de produits comportant des éléments numériques appartenant aux catégories déterminées par l'ADCO qu'ils présentent la nomenclature des logiciels qu'ils ont établie en vertu du présent règlement. Afin de préserver la confidentialité des nomenclatures des logiciels, les autorités de surveillance du marché devraient transmettre à l'ADCO les informations pertinentes relatives aux dépendances de façon agrégée et anonymisée.

(23) La bonne application du présent règlement dépendra également de la disponibilité des compétences appropriées en matière de cybersécurité. Au niveau de l'Union, la pénurie de main-d'œuvre qualifiée en cybersécurité dans l'Union et la nécessité d'y remédier à titre de priorité, dans le secteur tant public que privé, ont été reconnues dans divers documents programmatiques et politiques, dont la communication de la Commission du 18 avril 2023 intitulée "Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE" et les conclusions du Conseil du 22 mai 2023 sur la politique de cyberdéfense de l'UE. Aux fins de la bonne application du présent règlement, les États membres devraient veiller à ce que les autorités de surveillance du marché et les organismes d'évaluation de la conformité disposent des ressources appropriées afin d'employer le personnel nécessaire aux tâches qui leur incombent en vertu du présent règlement. Ces mesures devraient favoriser la mobilité des effectifs dans le domaine de la cybersécurité et des parcours professionnels associés et contribuer à rendre la main-d'œuvre de ce domaine plus résiliente et inclusive, y compris pour ce qui est de l'équilibre entre les hommes et les femmes. Par conséquent, les États membres devraient prendre des mesures garantissant que les tâches susmentionnées sont menées à bien par des professionnels formés disposant des compétences nécessaires dans le domaine de la cybersécurité. De même, il convient que le fabricant veille à ce que son personnel dispose des compétences nécessaires pour respecter les obligations qui leur incombent en vertu du présent règlement. Les États membres et la Commission, conformément à leurs prérogatives et compétences ainsi qu'aux tâches particulières qui leur reviennent en vertu du présent règlement, devraient prendre des mesures visant à soutenir les fabricants et en particulier les microentreprises et les petites et moyennes entreprises, dont les jeunes pousses, y compris dans des domaines tels que le développement de compétences, aux fins du respect des obligations qui leur incombent en vertu du présent règlement. En outre, puisque la directive (UE) 2022/2555 exige d'eux qu'ils adoptent, dans le cadre de leurs stratégies nationales en matière de cybersécurité, des mesures de politique publique qui encouragent et développent la formation et les compétences dans le domaine de la cybersécurité, les États membres peuvent également envisager, lors de l'adoption de ces stratégies, de pourvoir aux besoins de compétences en matière de cybersécurité qui découlent du présent règlement, y compris les besoins de renforcement des compétences et de reconversion professionnelle.

(24) Un internet sécurisé est indispensable au fonctionnement des infrastructures critiques et à la société dans son ensemble. La directive (UE) 2022/2555 vise à garantir un niveau élevé de cybersécurité des services fournis par des entités essentielles et importantes visées à son article 3, y compris les fournisseurs d'infrastructures numériques qui soutiennent les fonctions essentielles de l'internet ouvert, assurent l'accès à l'internet et fournissent 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 (UE) 2022/2555, 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.

(25) Le règlement (UE) 2017/745 du Parlement européen et du Conseil[9] établit des règles relatives aux dispositifs médicaux et le règlement (UE) 2017/746 du Parlement européen et du Conseil[10] définit des règles relatives aux dispositifs médicaux de diagnostic in vitro. Ces 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. 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.

---

9 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) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1).

10 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).

(26) Les produits comportant des éléments numériques qui sont développés ou modifiés exclusivement à des fins de sécurité nationale ou de défense ou les produits spécifiquement conçus pour traiter des informations classifiées ne relèvent pas du champ d'application du présent règlement. Les États membres sont invités à veiller à ce que ces produits bénéficient d'un niveau de protection analogue, voire supérieur, à celui appliqué aux produits relevant du champ d'application du présent règlement.

(27) Le règlement (UE) 2019/2144 du Parlement européen et du Conseil[11] établit des exigences pour la réception par type des véhicules, ainsi que de leurs systèmes et composants, et introduit certaines exigences 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 risques de cybersécurité 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, notamment le règlement ONU n° 155 – Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité, et prévoit des procédures spécifiques d'évaluation de la conformité.

---

[11] 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) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

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 comprennent des obligations de protection contre les menaces relatives à la sécurité de l'information. Le processus de certification prévu par le règlement (UE) 2018/1139 garantit le niveau d'assurance visé par le présent règlement. 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 devraient donc pas être soumis aux exigences essentielles de cybersécurité et aux procédures d'évaluation de la conformité énoncées dans le présent règlement.

[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) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

(28) 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 de cybersécurité énoncées dans 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 de cybersécurité énoncées dans le 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 au moins identique à celui prévu par le présent règlement. La Commission devrait être habilitée à adopter des actes délégués pour compléter le présent règlement en identifiant de tels produits et règles. Pour ce qui est du droit de l'Union en vigueur auquel cette limitation ou exclusion devrait s'appliquer, le présent règlement prévoit des dispositions spécifiques visant à clarifier sa relation avec ce droit de l'Union.

(29) Afin de garantir que les produits comportant des éléments numériques mis à disposition sur le marché pourront être réparés de manière efficace et que leur durabilité pourra être prolongée, il convient de prévoir une dérogation pour les pièces de rechange. Cette dérogation devrait concerner à la fois les pièces de rechange destinées à réparer des produits anciens ayant été mis à disposition avant la date d'application du présent règlement et les pièces de rechange qui ont déjà fait l'objet d'une procédure d'évaluation de la conformité en application du présent règlement.

(30) Le règlement délégué (UE) 2022/30 de la Commission[13] précise que plusieurs des exigences essentielles énoncées à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE du Parlement européen et du Conseil[14], qui portent sur les dommages au réseau et la mauvaise utilisation des ressources du réseau, sur les données à caractère personnel et la vie privée ainsi que sur la fraude, s'appliquent à certains équipements radio. La décision d'exécution C(2022) 5637 de la Commission du 5 août 2022 relative à une demande de normalisation adressée au Comité européen de normalisation et au Comité européen de normalisation électrotechnique fixe des exigences pour l'élaboration de normes spécifiques précisant la manière dont ces trois exigences essentielles doivent être traitées. Les exigences essentielles de cybersécurité énoncées dans 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 de cybersécurité 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, lorsque 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 lors de l'élaboration et du développement de normes harmonisées visant à faciliter la mise en œuvre du présent règlement. Au cours de la période transitoire pour l'application du présent règlement, la Commission devrait fournir des orientations aux fabricants soumis à la fois au présent règlement et au règlement délégué (UE) 2022/30, afin de faciliter la démonstration du respect de ces deux règlements.

---

13 Règlement délégué (UE) 2022/30 de la Commission du 29 octobre 2021 complétant la directive 2014/53/UE du Parlement européen et du Conseil en ce qui concerne l'application des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de cette directive (JO L 7 du 12.1.2022, p. 6).

14 Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).

(31) La directive (UE) 2024/... du Parlement européen et du Conseil[15+] 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.

---

15 Directive (UE) 2024/... du Parlement européen et du Conseil du ... sur ... (JO L, ..., ELI: ...).

+ JO: veuillez insérer dans le corps du texte le numéro de la directive qui figure dans le document (2022/0302 (COD)) et insérer dans la note de bas de page le numéro, la date, l'intitulé et la référence au JO de ladite directive.

(32) Le présent règlement devrait s'appliquer sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil[16], et notamment de ses dispositions concernant 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 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 de cybersécurité prévues par 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.

---

[16] 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).

(33) Dans la mesure où leurs produits relèvent du champ d'application du présent règlement, les fournisseurs de portefeuilles européens d'identité numérique visés à l'article 5 *bis*, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil[17] devraient se conformer à la fois aux exigences essentielles de cybersécurité horizontales énoncées dans le présent règlement et aux exigences de sécurité spécifiques énoncées à l'article 5 *bis* du règlement (UE) n° 910/2014. Afin de faciliter la conformité, les fournisseurs de portefeuilles devraient pouvoir démontrer la conformité des portefeuilles européens d'identité numérique aux exigences énoncées respectivement dans le présent règlement et dans le règlement (UE) n° 910/2014 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 voie d'actes délégués, une présomption de conformité pour le présent règlement, dans la mesure où le certificat, ou des parties de celui-ci, couvre ces exigences.

---

[17] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

(34) Lorsqu'il intègre des composants obtenus auprès de tiers à des produits comportant des éléments numériques au cours de la phase de conception et de développement, le fabricant devrait, pour que les produits soient conçus, développés et produits conformément aux exigences essentielles de cybersécurité énoncées dans le présent règlement, faire preuve de diligence raisonnable concernant ces composants, y compris les composants logiciels libres et ouverts qui n'ont pas été mis à disposition sur le marché. Le niveau approprié de diligence raisonnable dépend de la nature et du niveau du risque de cybersécurité associé à un composant donné et devrait, à cette fin, tenir compte d'une ou de plusieurs des mesures suivantes: vérifier, le cas échéant, que le fabricant d'un composant a démontré se conformer au présent règlement, y compris en s'assurant que le composant porte déjà le marquage CE; vérifier qu'un composant fait régulièrement l'objet de mises à jour de sécurité, par exemple en consultant l'historique de ses mises à jour de sécurité; vérifier qu'un composant est exempt des vulnérabilités enregistrées dans la base de données européenne des vulnérabilités créée en vertu de l'article 12, paragraphe 2, de la directive (UE) 2022/2555 ou dans d'autres bases de données publiques; réaliser des essais de sécurité supplémentaires. Les obligations en matière de gestion des vulnérabilités énoncées dans le présent règlement, que le fabricant doit respecter lors de la mise sur le marché d'un produit comportant des éléments numériques puis pendant la période d'assistance, s'appliquent aux produits comportant des éléments numériques dans leur entièreté, y compris à tous les composants intégrés. Lorsque, dans l'exercice de sa diligence raisonnable, le fabricant du produit comportant des éléments numériques décèle une vulnérabilité dans un composant, y compris un composant libre et ouvert, il devrait en informer la personne ou l'entité qui fabrique le composant ou en assure l'entretien, s'attaquer et remédier à la vulnérabilité et, le cas échéant, fournir à la personne ou à l'entité le correctif de sécurité appliqué.

(35) Immédiatement après la période transitoire pour l'application du présent règlement, le fabricant d'un produit comportant des éléments numériques qui intègre un ou plusieurs composants obtenus auprès de tiers qui relèvent également du présent règlement pourrait ne pas être en mesure de vérifier, dans le cadre de son obligation de diligence raisonnable, que les fabricants de ces composants ont démontré qu'ils se conforment au présent règlement en s'assurant, par exemple, que le composant porte déjà le marquage CE. Cette situation pourrait se présenter lorsque des composants ont été intégrés avant que le présent règlement ne s'applique à leur fabricant. Dans ce cas, un fabricant qui intègre de tels composants devrait faire preuve de diligence raisonnable par d'autres moyens.

(36) Le marquage CE devrait être apposé sur les produits comportant des éléments numériques pour indiquer de manière visible, lisible et indélébile 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 prévues par le présent règlement et portent le marquage CE. En outre, lors de foires, d'expositions et de démonstrations ou de manifestations similaires, les États membres ne devraient pas faire obstacle à la présentation ou à l'utilisation d'un produit comportant des éléments numériques non conforme au présent règlement, y compris ses prototypes, pour autant que le produit porte une marque visible indiquant clairement que le produit n'est pas conforme au présent règlement et que, tant que ce sera le cas, il ne sera pas mis à disposition sur le marché.

(37) Afin de garantir que les fabricants puissent mettre à disposition des logiciels à des fins d'essai avant de soumettre leurs produits comportant des éléments numériques 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, à condition que le logiciel inachevé ne soit mis à disposition que pendant le temps nécessaire pour le 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 prévues 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.

(38) 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 de cybersécurité pour ces produits. Ces exigences, y compris celles qui ont trait à la gestion des vulnérabilités, s'appliquent à chaque produit comportant des éléments numériques lors de sa mise sur le marché, qu'il ait été fabriqué individuellement ou produit en série. Par exemple, pour un type de produit, chaque produit comportant des éléments numériques devrait, lors de sa mise sur le marché, avoir reçu individuellement tous les correctifs et mises à jour de sécurité qui existent pour remédier aux problèmes de sécurité pertinents. Lorsque des produits comportant des éléments numériques sont modifiés ultérieurement, par des moyens physiques ou numériques, d'une manière qui n'est pas prévue par le fabricant dans l'évaluation initiale des risques et qui peut impliquer qu'ils ne satisfont plus aux exigences essentielles de cybersécurité pertinentes, la modification devrait être considérée comme substantielle. Par exemple, les réparations pourraient être assimilées à des opérations d'entretien pour autant qu'elles ne modifient pas un produit comportant des éléments numériques 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.

(39) Comme c'est le cas pour les réparations ou modifications physiques, un produit comportant des éléments numériques devrait être considéré comme substantiellement modifié par une modification logicielle lorsque la mise à jour du logiciel modifie l'utilisation prévue de ce produit et que ces modifications n'ont pas été prévues par le fabricant dans l'évaluation initiale des risques, ou lorsque la nature du danger a changé ou que le niveau de risque de cybersécurité a augmenté en raison de la mise à jour du logiciel, et que la version mise à jour est mise à disposition sur le marché. Une mise à jour de sécurité destinée à réduire le niveau de risque de cybersécurité d'un produit comportant des éléments numériques qui ne modifie pas l'utilisation prévue de ce produit n'est pas considérée comme une modification substantielle. Il s'agit généralement des situations où une mise à jour de sécurité ne comporte que des ajustements mineurs du code source. Ce pourrait être le cas, par exemple, d'une mise à jour de sécurité qui remédie à une vulnérabilité connue, y compris en modifiant les fonctions ou les performances d'un produit comportant des éléments numériques dans le seul but de réduire le niveau de risque de cybersécurité. De même, une mise à jour mineure de fonctionnalités, telle qu'une amélioration visuelle ou l'ajout de nouveaux pictogrammes ou de nouvelles langues ou d'un nouvel ensemble de pictogrammes à l'interface utilisateur, ne devrait pas, en règle générale, être considérée comme une modification substantielle. À l'inverse, une mise à jour de caractéristiques qui modifie les fonctions initialement prévues d'un produit comportant des éléments numériques, son type ou ses performances et qui remplit les critères susmentionnés devrait être considérée comme une modification substantielle, étant donné que l'ajout de nouvelles caractéristiques accroît généralement la surface d'attaque et, partant, les risques de cybersécurité. Ce peut être le cas, par exemple, lorsque l'ajout d'un nouvel élément de saisie à une application nécessite que le fabricant procède à une validation adéquate de la saisie. Le fait qu'une mise à jour de caractéristiques soit apportée de façon indépendante ou qu'elle soit combinée à une mise à jour de sécurité n'est pas pertinent pour déterminer si elle constitue une modification substantielle. La Commission devrait publier des orientations sur la manière de déterminer ce qui constitue une modification substantielle.

(40) Compte tenu de la nature itérative du développement de logiciels, un fabricant ayant successivement mis sur le marché plusieurs versions d'un logiciel en raison d'une modification substantielle apportée à ce dernier ne devrait être en mesure de fournir des mises à jour de sécurité pendant la période d'assistance que pour la dernière version du logiciel qu'il a mise sur le marché. Il ne devrait être en mesure de procéder ainsi que si les utilisateurs des versions précédentes concernées du logiciel ont accès gratuitement à la dernière version mise sur le marché et qu'ils n'ont pas à s'acquitter de coûts supplémentaires pour adapter l'environnement matériel ou logiciel dans lequel ils exploitent le produit. Tel pourrait être le cas par exemple, si la mise à jour d'un système d'exploitation de bureau ne nécessite pas de matériel nouveau tel qu'un processeur plus rapide ou de plus grandes capacités de mémoire. Toutefois, pendant la période d'assistance, le fabricant devrait continuer de respecter d'autres exigences relatives à la gestion des vulnérabilités, comme le fait de disposer d'une politique de divulgation coordonnée des vulnérabilités ou d'appliquer des mesures visant à faciliter le partage d'informations relatives à de possibles vulnérabilités pour toutes les versions suivantes du logiciel mis sur le marché qui ont été modifiées de façon substantielle. Il convient que le fabricant ne soit en mesure de fournir des mises à jour mineures de sécurité ou de fonctionnalité qui ne constituent pas une modification substantielle que pour la dernière version ou sous-version d'un logiciel qui n'a pas été modifiée de façon substantielle. Dans le même temps, lorsqu'un produit matériel tel qu'un téléphone intelligent n'est pas compatible avec la version la plus récente du système d'exploitation avec lequel il avait initialement été livré, il convient que le fabricant continue d'apporter des mises à jour de sécurité pendant la période d'assistance, au moins pour la dernière version du système d'exploitation compatible avec ce produit matériel.

(41) Conformément à la notion généralement établie de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, lorsque se produit une modification substantielle de nature à affecter la conformité d'un produit comportant des éléments numériques 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, une modification susceptible d'entraîner une modification substantielle devrait être notifiée à ce dernier.

(42) Lorsqu'un produit comportant des éléments numériques fait l'objet d'une "remise à neuf", d'un "entretien" et d'une "réparation", au sens de l'article 2, points 18), 19) et 20), du règlement (UE) 2024/1781 du Parlement européen et du Conseil[18], cela n'entraîne 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 comportant des éléments numériques par le fabricant pourrait entraîner des modifications dans la conception et le développement de ce produit et donc avoir une incidence sur son utilisation prévue et sa conformité aux exigences énoncées dans le présent règlement.

---

[18] Règlement (UE) 2024/1781 du Parlement européen et du Conseil du 13 juin 2024 établissant un cadre pour la fixation d'exigences en matière d'écoconception pour des produits durables, modifiant la directive (UE) 2020/1828 et le règlement (UE) 2023/1542 et abrogeant la directive 2009/125/CE (JO L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Les produits comportant des éléments numériques devraient être considérés comme importants si l'exploitation de vulnérabilités potentielles dans ces produits peut avoir de graves répercussions en raison, entre autres, de la fonctionnalité liée à la cybersécurité ou d'une fonction qui comporte un risque important d'effets néfastes du fait de leur intensité et leur capacité à perturber, contrôler ou endommager un grand nombre d'autres produits ou à porter atteinte à la santé, à la sécurité ou à la sûreté de leurs utilisateurs par une manipulation directe, par exemple une fonction du système central, notamment la gestion du réseau, le contrôle de la configuration, la virtualisation ou le traitement des données à caractère personnel. En particulier, les vulnérabilités de produits comportant des éléments numériques qui ont une fonctionnalité liée à la cybersécurité, tels que les gestionnaires de démarrage, peuvent provoquer une propagation des problèmes de sécurité tout au long de la chaîne d'approvisionnement. La gravité des répercussions d'un incident peut également augmenter lorsque le produit assure principalement une fonction du système central, y compris la gestion du réseau, le contrôle de la configuration, la virtualisation ou le traitement des données à caractère personnel.

(44) Certaines catégories de produits comportant des éléments numériques devraient être soumises à des procédures d'évaluation de la conformité plus strictes, tout en conservant une approche proportionnée. À cette fin, les produits importants comportant des éléments numériques devraient être divisés en deux catégories, reflétant le niveau de risque de cybersécurité lié à ces catégories de produits. Un incident impliquant des produits importants comportant des éléments numériques qui relèvent de la classe II pourrait avoir des répercussions négatives plus importantes qu'un incident impliquant des produits importants comportant des éléments numériques qui relèvent de la classe I, par exemple en raison de la nature de leur fonction liée à la cybersécurité ou de l'exécution d'une autre fonction qui comporte un risque important d'effets néfastes. À titre indicatif, les produits comportant des éléments numériques qui relèvent de la classe II pourraient assurer soit une fonctionnalité liée à la cybersécurité, soit une autre fonction comportant un risque important d'effets néfastes plus élevé que pour les produits relevant de la classe I, soit ces deux types de fonctions. Par conséquent, les produits importants comportant des éléments numériques qui relèvent de la classe II devraient faire l'objet d'une procédure plus stricte d'évaluation de la conformité.

(45) Par "produits importants comportant des éléments numériques visés dans le présent règlement", on devrait entendre les produits possédant les fonctionnalités essentielles d'une catégorie de produits importants comportant des éléments numériques recensée dans le présent règlement. Par exemple, le présent règlement établit des catégories de produit importants comportant des éléments numériques qui sont définis par leur fonctionnalité de base comme pare-feu ou des systèmes de détection ou de prévention des intrusions de classe II. Par conséquent, les pare-feu et systèmes de détection ou de prévention des intrusions sont soumis à une évaluation de conformité obligatoire par un tiers. Ce n'est pas le cas pour d'autres produits comportant des éléments numériques qui ne sont pas catégorisés comme des produits importants comportant des éléments numériques mais qui peuvent intégrer des pare-feu ou des systèmes de détection ou de prévention des intrusions. La Commission devrait adopter un acte d'exécution pour préciser la description technique des catégories de produits importants comportant des éléments numériques qui relèvent des classes I et II, telles qu'elles figurent dans le présent règlement.

(46) Les catégories de produits critiques comportant des éléments numériques énoncées dans le présent règlement ont une fonctionnalité liée à la cybersécurité et remplissent une fonction qui comporte un risque important d'effets néfastes quant à son intensité et à sa capacité à perturber, contrôler ou endommager un grand nombre d'autres produits avec éléments numériques par le biais d'une manipulation directe. En outre, ces catégories de produits comportant des éléments numériques sont considérées comme des dépendances critiques pour les entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555. Les catégories de produits critiques comportant des éléments numériques figurant en annexe du présent règlement, en raison de leur criticité, reposent déjà largement sur diverses formes de certification et relèvent également du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) défini dans le règlement d'exécution (UE) 2024/482 de la Commission[19]. Par conséquent, afin d'assurer, dans l'Union, une protection adéquate commune sur le plan de la cybersécurité des produits critiques comportant des éléments numériques, il pourrait être approprié et proportionné de soumettre ces catégories de produits, par voie d'un acte délégué, à une certification européenne de cybersécurité obligatoire lorsqu'un schéma européen de certification de cybersécurité pertinent couvrant ces produits est déjà en place et qu'une évaluation des effets potentiels sur le marché de la certification obligatoire envisagée a été réalisée par la Commission. Cette évaluation devrait tenir compte à la fois de l'offre et de la demande, et y compris de l'existence d'une demande, de la part des États membres et des utilisateurs pour les produits comportant des éléments numériques concernés, qui soit suffisante pour exiger une certification européenne de cybersécurité, ainsi que les finalités pour lesquelles les produits comportant des éléments numériques sont destinés à être utilisés, y compris la dépendance critique à leur égard des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555. L'évaluation devrait également analyser les effets potentiels de la certification obligatoire sur la disponibilité de ces produits sur le marché intérieur, ainsi que les capacités et l'état de préparation des États membres pour la mise en œuvre des schémas européens de certification de cybersécurité.

---

19 Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Les actes délégués exigeant une certification européenne de cybersécurité obligatoire devraient déterminer les produits comportant des éléments numériques qui ont la fonctionnalité essentielle d'une catégorie de produits critiques comportant des éléments numériques définie dans le présent règlement et qui doivent faire l'objet d'une certification obligatoire, ainsi que le niveau d'assurance requis, lequel devrait être au moins "substantiel". Le niveau d'assurance requis doit être proportionnel au niveau de risque de cybersécurité associé au produit comportant des éléments numériques. Par exemple, lorsque le produit comportant des éléments numériques possède les fonctionnalités essentielles d'une catégorie de produits critiques comportant des éléments numériques définie dans le présent règlement et qu'il est destiné à être utilisé dans un environnement sensible ou critique, comme les produits destinés à être utilisés par des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555, il peut nécessiter le niveau d'assurance le plus élevé.

(48) Afin d'assurer, dans l'Union, une protection adéquate commune sur le plan de la cybersécurité des produits comportant des éléments numériques qui ont les fonctionnalités essentielles d'une catégorie de produits critiques comportant des éléments numériques définie dans le présent règlement, il convient également de conférer à la Commission le pouvoir d'adopter des actes délégués pour modifier le présent règlement en y ajoutant ou en en retirant des catégories de produits critiques comportant des éléments numériques pour lesquels les fabricants pourraient être tenus d'obtenir un certificat européen de cybersécurité dans le cadre d'un schéma européen de certification de cybersécurité en application du règlement (UE) 2019/881 afin de démontrer leur conformité avec le présent règlement. Une nouvelle catégorie de produits critiques comportant des éléments numériques peut être ajoutée à ces catégories s'il existe une dépendance critique à leur égard d'entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555 ou, s'ils sont touchés par des incidents ou contiennent des vulnérabilités exploitées, si cela pourrait entraîner des perturbations pour les chaînes d'approvisionnement critiques. Lorsqu'elle évalue la nécessité d'ajouter ou de retirer des catégories de produits critiques comportant des éléments numériques par voie d'un acte délégué, la Commission devrait pouvoir tenir compte du fait que les États membres ont recensé, au niveau national, les produits comportant des éléments numériques qui jouent un rôle critique pour la résilience des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555 et qui sont de plus en plus confrontés à des cyberattaques dans la chaîne d'approvisionnement, avec des effets perturbateurs potentiels graves. Il convient par ailleurs que la Commission puisse tenir compte des résultats des évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22 de la directive (UE) 2022/2555.

(49) La Commission devrait veiller à ce qu'un large éventail de parties prenantes soit consulté de manière structurée et régulière lors de l'élaboration des mesures de mise en œuvre du présent règlement. Cela devrait être particulièrement le cas lorsque la Commission évalue la nécessité d'actualiser les listes des catégories de produits importants ou critiques comportant des éléments numériques. Le cas échéant, les fabricants devraient être consultés et leurs avis pris en compte afin d'analyser les risques de cybersécurité ainsi que l'équilibre entre les coûts et les avantages de la désignation de ces catégories de produits comme importants ou critiques.

(50) 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 toujours liés à la cybersécurité mais qui peuvent être la conséquence d'une atteinte à la sécurité. Ces risques devraient continuer à être réglementés par des actes législatifs d'harmonisation de l'Union autres que le présent règlement. Si aucune législation d'harmonisation de l'Union autre que le présent règlement ne leur est applicable, ils devraient être soumis au règlement (UE) 2023/988 du Parlement européen et du Conseil[20]. Par conséquent, compte tenu du caractère ciblé du présent règlement, par dérogation à l'article 2, paragraphe 1, troisième alinéa, point b), du règlement (UE) 2023/988, le chapitre III, section 1, les chapitres V et VII, et les chapitres IX à XI du règlement (UE) 2023/988 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 prévues par une législation d'harmonisation de l'Union autre que le présent règlement au sens de l'article 3, point 27), du règlement (UE) 2023/988.

---

[20] Règlement (UE) 2023/988 du Parlement européen et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits, modifiant le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil et la directive (UE) 2020/1828 du Parlement européen et du Conseil, et abrogeant la directive 2001/95/CE du Parlement européen et du Conseil et la directive 87/357/CEE du Conseil (JO L 135 du 23.5.2023, p. 1).

(51) Les produits comportant des éléments numériques classés comme systèmes d'IA à haut risque conformément à l'article 6 du règlement (UE) 2024/1689 du Parlement européen et du Conseil[21] qui relèvent du champ d'application du présent règlement devraient satisfaire aux exigences essentielles de cybersécurité énoncées dans celui-ci. Lorsque ces systèmes d'IA à haut risque satisfont aux exigences essentielles de cybersécurité énoncées dans le présent règlement, ils devraient être réputés respecter les exigences de cybersécurité énoncées à l'article article 15 du règlement (UE) 2024/1689, 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. À cette fin, l'évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques classés comme système d'IA à haut risque en vertu du règlement (UE) 2024/1689 qui doit être prise en compte pendant les phases de planification, de conception, de développement, de production, de livraison et de maintenance de ce produit, comme l'exige le présent règlement, devrait tenir compte des risques pour la cyberrésilience d'un système d'IA en cas de tentatives par des tiers non autorisés de modifier son utilisation, son comportement ou ses performances, y compris les vulnérabilités propres à l'IA telles que l'empoisonnement des données ou les attaques adversaires, ainsi que, le cas échéant, les risques pour les droits fondamentaux, conformément au règlement (UE) 2024/1689. En ce qui concerne les procédures d'évaluation de la conformité relatives aux exigences essentielles de cybersécurité d'un produit comportant des éléments numériques qui entre dans le champ d'application du présent règlement et classé comme système d'IA à haut risque, l'article 43 du règlement (UE) 2024/1689 devrait de manière générale s'appliquer en lieu et place des dispositions pertinentes du présent règlement.

---

[21] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Toutefois, l'application de cette règle ne devrait pas entraîner de réduction du niveau d'assurance nécessaire pour les produits importants ou critiques comportant des éléments numériques visés dans 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 (UE) 2024/1689 et sont également considérés comme des produits importants ou critiques comportant des éléments numériques visés dans le 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 (UE) 2024/1689 devraient être soumis aux procédures d'évaluation de la conformité prévues par le présent règlement en ce qui concerne les exigences essentielles de cybersécurité énoncées dans celui-ci. Dans ce cas, pour tous les autres aspects couverts par le règlement (UE) 2024/1689, les dispositions pertinentes relatives à l'évaluation de la conformité fondée sur le contrôle interne énoncées à l'annexe VI de ce règlement devraient s'appliquer.

(52) Afin d'améliorer la sécurité des produits comportant des éléments numériques mis sur le marché intérieur, il est nécessaire d'établir des exigences essentielles de cybersécurité applicables à ces produits. Ces exigences essentielles de cybersécurité ne devraient pas porter atteinte aux évaluations coordonnées au niveau de l'Union des risques de sécurité portant sur les chaînes d'approvisionnement critiques et prévues à l'article 22 de la directive (UE) 2022/2555, 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 de la Commission[22], dans l'évaluation coordonnée par l'Union de la cybersécurité des réseaux 5G et dans la boîte à outils de l'Union sur la cybersécurité 5G convenue par le groupe de coopération institué en vertu de l'article 14 de la directive (UE) 2022/2555.

[22] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 sur la cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

(53) Les fabricants de produits relevant du champ d'application du règlement (UE) 2023/1230 du Parlement européen et du Conseil[23] qui sont également des produits comportant des éléments numériques au sens du présent règlement devraient satisfaire à la fois aux exigences essentielles de cybersécurité énoncées dans le présent règlement et aux exigences essentielles de santé et de sécurité énoncées dans le règlement (UE) 2023/1230. Les exigences essentielles de cybersécurité énoncées dans le présent règlement et certaines exigences essentielles énoncées dans le règlement (UE) 2023/1230 pourraient porter sur des risques similaires en matière de cybersécurité. Par conséquent, le respect des exigences essentielles de cybersécurité énoncées dans le présent règlement pourrait faciliter le respect des exigences essentielles qui s'appliquent également à certains risques de cybersécurité énoncés dans le règlement (UE) 2023/1230, et en particulier celles concernant la protection contre la corruption et la sécurité et la fiabilité des systèmes de contrôle énoncées aux sections 1.1.9 et 1.2.1 de l'annexe III de ce règlement. Ces synergies doivent être démontrées par le fabricant, qui doit par exemple appliquer, le cas échéant, des normes harmonisées ou d'autres spécifications techniques répondant aux exigences essentielles de cybersécurité pertinentes, à la suite d'une évaluation des risques liés à la cybersécurité. Le fabricant doit également suivre les procédures d'évaluation de la conformité applicables définies dans le présent règlement et dans le règlement (UE) 2023/1230. La Commission et les organismes européens de normalisation, dans le cadre des travaux préparatoires soutenant la mise en œuvre du présent règlement et du règlement (UE) 2023/1230, ainsi que des processus de normalisation connexes, devraient promouvoir la cohérence dans la manière d'évaluer les risques liés à la cybersécurité et dans la manière de couvrir ces risques par des normes harmonisées en ce qui concerne les exigences essentielles pertinentes.

---

[23] Règlement (UE) 2023/1230 du Parlement européen et du Conseil du 14 juin 2023 sur les machines, abrogeant la directive 2006/42/CE du Parlement européen et du Conseil et la directive 73/361/CEE du Conseil (JO L 165 du 29.6.2023, p. 1).

En particulier, la Commission et les organismes européens de normalisation devraient tenir compte du présent règlement dans la préparation et l'élaboration de normes harmonisées visant à faciliter la mise en œuvre du règlement (UE) 2023/1230 en ce qui concerne notamment les aspects de la cybersécurité liés à la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de contrôle énoncés aux sections 1.1.9 et 1.2.1 de l'annexe III de ce règlement. La Commission devrait fournir des orientations pour aider les fabricants relevant du présent règlement mais aussi du règlement (UE) 2023/1230, en particulier pour leur permettre de démontrer plus facilement qu'ils respectent les exigences essentielles pertinentes énoncées dans le présent règlement et dans le règlement (UE) 2023/1230.

(54) Afin de garantir la sécurité des produits comportant des éléments numériques au moment de leur mise sur le marché et pendant la période d'utilisation prévue du produit comportant des éléments numériques, il est nécessaire de définir des exigences essentielles de cybersécurité relatives à la gestion de la vulnérabilité et des exigences essentielles de cybersécurité concernant les propriétés des produits comportant des éléments numériques. Les fabricants devraient se conformer à toutes les exigences essentielles de cybersécurité relatives à la gestion des vulnérabilités tout au long de la période d'assistance, mais ils devraient en outre déterminer les autres exigences essentielles liées aux propriétés du produit pertinentes pour le type de produit comportant des éléments numériques 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 pertinents et les exigences essentielles de cybersécurité pertinentes, de mettre à disposition leurs produits comportant des éléments numériques sans vulnérabilité exploitable connue susceptible d'avoir des répercussions sur la sécurité de ces produits et d'appliquer de manière appropriée des normes harmonisées, des spécifications communes ou des normes européennes ou internationales appropriées.

(55) Lorsque certaines exigences essentielles de cybersécurité ne sont pas applicables à un produit comportant des éléments numériques, le fabricant doit faire figurer une justification claire dans l'évaluation des risques de cybersécurité figurant dans la documentation technique. Cela pourrait être le cas lorsqu'une exigence essentielle de cybersécurité est incompatible avec la nature d'un produit comportant des éléments numériques. Par exemple, la destination d'un produit comportant des éléments numériques peut exiger du fabricant qu'il respecte des normes d'interopérabilité largement reconnues, même si ses dispositifs de sécurité ne sont plus considérés comme étant à la pointe de la technologie. De même, d'autres législations de l'Union exigent des fabricants qu'ils appliquent des exigences spécifiques en matière d'interopérabilité. Lorsqu'une exigence essentielle de cybersécurité ne s'applique pas à un produit comportant des éléments numériques, mais que le fabricant a détecté des risques de cybersécurité en rapport avec ladite exigence essentielle de cybersécurité, il doit prendre des mesures pour faire face à ces risques par d'autres moyens, par exemple en limitant la destination du produit à des environnements de confiance ou en informant les utilisateurs de ces risques.

(56) L'une des mesures les plus importantes que les utilisateurs doivent prendre pour protéger leurs produits comportant des éléments numériques contre les cyberattaques est d'installer les dernières mises à jour de sécurité disponibles dès que possible. Les fabricants doivent donc concevoir leurs produits et mettre en place des procédures de sorte que les produits comportant des éléments numériques comprennent des fonctions automatiques de notification, de distribution, de téléchargement et d'installation des mises à jour de sécurité, en particulier dans le cas des produits de consommation. Ils devraient également offrir la possibilité d'approuver le téléchargement et l'installation des mises à jour de sécurité en tant qu'étape finale. Les utilisateurs doivent garder la possibilité de désactiver les mises à jour automatiques, grâce à un dispositif clair et facile à utiliser, accompagné d'instructions claires sur la manière dont les utilisateurs peuvent renoncer à ces mises à jour. Les exigences relatives aux mises à jour automatiques énoncées dans une annexe du présent règlement ne s'appliquent pas aux produits dont les éléments numériques sont principalement destinés à être intégrés en tant que composants dans d'autres produits. Elles ne s'appliquent pas non plus aux produits comportant des éléments numériques pour lesquels les utilisateurs ne s'attendent pas raisonnablement à des mises à jour automatiques, y compris les produits comportant des éléments numériques destinés à être utilisés dans des réseaux TIC professionnels, et en particulier dans des environnements critiques et industriels où une mise à jour automatique pourrait perturber les opérations. Qu'un produit comportant des éléments numériques soit conçu pour recevoir des mises à jour automatiques ou non, son fabricant doit informer les utilisateurs des vulnérabilités et mettre à disposition des mises à jour de sécurité sans retard. Lorsqu'un produit comportant des éléments numériques est doté d'une interface utilisateur ou de moyens techniques similaires permettant une interaction directe avec ses utilisateurs, le fabricant doit utiliser ces caractéristiques pour informer les utilisateurs que leur produit comportant des éléments numériques est arrivé au terme de la période d'assistance. Les notifications doivent être limitées à ce qui est nécessaire pour garantir la réception effective de ces informations et ne doivent pas avoir de répercussions négatives sur l'expérience de l'utilisateur du produit comportant des éléments numériques.

(57) Afin d'améliorer la transparence des processus de traitement des vulnérabilités et de garantir que les utilisateurs ne sont pas obligés d'installer de nouvelles mises à jour de fonctionnalités dans le seul but de recevoir les dernières mises à jour de sécurité, les fabricants doivent veiller, lorsque cela est techniquement possible, à ce que les nouvelles mises à jour de sécurité soient fournies séparément des mises à jour de fonctionnalités.

(58) La communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 20 juin 2023 intitulée "Stratégie européenne de sécurité économique" indique que l'Union doit optimiser les avantages de son ouverture économique tout en réduisant à leur minimum les risques liés aux dépendances économiques à l'égard des fournisseurs à haut risque, grâce à un cadre stratégique commun pour la sécurité économique de l'Union. Les dépendances à l'égard de fournisseurs à haut risque de produits comportant des éléments numériques peuvent représenter un risque stratégique auquel il faut s'attaquer au niveau de l'Union, en particulier lorsque les produits comportant des éléments numériques sont destinés à être utilisés par des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555. Ces risques peuvent être liés, sans pour autant s'y limiter, à la juridiction dont relève le fabricant, aux caractéristiques de son actionnariat et aux liens de contrôle qui le rattachent au gouvernement d'un pays tiers où il est établi, en particulier si le pays tiers se livre à des activités d'espionnage économique ou à un comportement irresponsable de l'État dans le cyberespace et que sa législation autorise un accès arbitraire aux opérations ou aux données de l'entreprise de quelque nature qu'elles soient, y compris les données commercialement sensibles, et peut imposer des obligations à des fins de renseignement sans garde-fous démocratiques ni mécanisme de contrôle ni procédure régulière ni droit de recours auprès d'une cour ou d'un tribunal indépendant. Lorsqu'elles déterminent l'importance d'un risque de cybersécurité au sens du présent règlement, la Commission et les autorités de surveillance du marché, conformément aux responsabilités qui leur incombent en vertu du présent règlement, devraient également tenir compte des facteurs de risque non techniques, en particulier ceux établis à la suite des évaluations coordonnées au niveau de l'Union des risques de sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22 de la directive (UE) 2022/2555.

(59) Afin de garantir la sécurité des produits comportant des éléments numériques après leur mise sur le marché, les fabricants doivent déterminer une période d'assistance qui doit correspondre à la durée d'utilisation prévue du produit comportant des éléments numériques. Pour déterminer la période d'assistance, le fabricant devrait notamment tenir compte des attentes raisonnables de l'utilisateur, de la nature du produit, ainsi que du droit de l'Union applicable à la durée de vie des produits comportant des éléments numériques. Les fabricants devraient également être en mesure de prendre en compte d'autres facteurs pertinents. Les critères doivent être appliqués de manière à garantir la proportionnalité de la durée de la période d'assistance. Sur demande, un fabricant doit fournir aux autorités de surveillance du marché les informations prises en compte pour déterminer la durée de la période d'assistance d'un produit comportant des éléments numériques.

(60) La période d'assistance pendant laquelle le fabricant garantit le traitement efficace des vulnérabilités ne doit pas être inférieure à cinq ans, sauf si la durée de vie du produit comportant des éléments numériques est inférieure à cinq ans, auquel cas le fabricant doit assurer le traitement des vulnérabilités pendant ladite durée. Dans les cas des produits comportant des éléments numériques dont on peut raisonnablement s'attendre à ce qu'ils soient utilisés pendant plus de cinq ans, comme c'est souvent le cas pour les composants matériels tels que les cartes mères ou les microprocesseurs, les dispositifs de réseau tels que les routeurs, les modems ou les commutateurs, ainsi que les logiciels tels que les systèmes d'exploitation ou les outils d'édition vidéo, les fabricants devraient en conséquence prévoir des périodes d'assistance plus longues. En particulier, les produits comportant des éléments numériques destinés à être utilisés dans des environnements industriels, tels que les systèmes de contrôle industriels, sont souvent utilisés pendant des périodes beaucoup plus longues. Un fabricant ne devrait pouvoir définir une période d'assistance inférieure à cinq ans que si cela est justifié par la nature du produit comportant des éléments numériques concerné et s'il est prévu que ce produit soit utilisé pendant moins de cinq ans, auquel cas la période d'assistance devrait correspondre à la durée d'utilisation prévue. Par exemple, la durée de vie d'une application de recherche des contacts destinée à être utilisée pendant une pandémie pourrait être limitée à la durée de la pandémie. En outre, certaines applications logicielles ne peuvent par nature être mises à disposition que sous la forme d'un abonnement, en particulier lorsque l'application devient indisponible pour l'utilisateur et n'est donc plus utilisable à l'expiration de l'abonnement.

(61) Lorsque les produits comportant des éléments numériques arrivent au terme de leur période d'assistance, afin de garantir que les vulnérabilités peuvent être traitées après la fin de la période d'assistance, les fabricants devraient envisager de divulguer le code source de ces produits comportant des éléments numériques soit à d'autres entreprises qui s'engagent à étendre la fourniture de services de traitement des vulnérabilités, soit au public. Lorsque les fabricants communiquent le code source à d'autres entreprises, ils doivent pouvoir protéger la propriété du produit comportant des éléments numériques et empêcher la diffusion du code source au public, par exemple au moyen d'accords contractuels.

(62) Afin de garantir que les fabricants de l'Union déterminent des périodes d'assistance similaires pour des produits comparables comportant des éléments numériques, l'ADCO devrait publier des statistiques sur les périodes d'assistance moyennes déterminées par les fabricants pour des catégories de produits comportant des éléments numériques et publier des orientations indiquant les périodes d'assistance appropriées pour ces catégories. En outre, afin de garantir une approche harmonisée dans l'ensemble du marché intérieur, la Commission devrait pouvoir adopter des actes délégués pour spécifier des périodes d'assistance minimales pour des catégories de produits spécifiques lorsque les données fournies par les autorités de surveillance du marché semblent indiquer que les périodes d'assistance déterminées par les fabricants ne sont pas systématiquement conformes aux critères de détermination des périodes d'assistance établis dans le présent règlement ou que les fabricants de différents États membres déterminent de manière injustifiée des périodes d'assistance différentes.

(63) Les fabricants doivent mettre en place un point de contact unique permettant aux utilisateurs d'entrer facilement en contact avec eux, notamment pour communiquer et recevoir des informations sur les vulnérabilités du produit comportant un élément numérique. Ils doivent faire en sorte que le point de contact unique soit facilement joignable par les utilisateurs et indiquer clairement sa disponibilité, en tenant ces informations à jour. Lorsque les fabricants optent pour des outils automatisés, par exemple des boîtes de dialogue, ils doivent également proposer un numéro de téléphone ou d'autres moyens de contact numériques, tels qu'une adresse électronique ou un formulaire de contact. Le point de contact unique ne doit pas dépendre uniquement d'outils automatisés.

(64) Les fabricants devraient mettre à disposition sur le marché leurs produits comportant des éléments numériques dans une configuration sécurisée par défaut et fournir gratuitement des mises à jour de sécurité aux utilisateurs. Les fabricants ne devraient pouvoir s'écarter des exigences essentielles de cybersécurité qu'en ce qui concerne les produits sur mesure adaptés à un usage particulier et destinés à un utilisateur professionnel particulier, et lorsque le fabricant et l'utilisateur sont explicitement convenus d'un autre éventail de conditions contractuelles.

(65) Les fabricants doivent notifier simultanément, via la plateforme unique de signalement, au centre de réponse aux incidents de sécurité informatique (CSIRT) désigné comme coordinateur et à l'ENISA les vulnérabilités activement exploitées contenues dans les produits comportant des éléments numériques, ainsi que les incidents graves ayant des répercussions sur la sécurité de ces produits. Les notifications doivent être transmises au moyen du point terminal de notification électronique d'un CSIRT désigné comme coordinateur et doivent être simultanément mises à la disposition de l'ENISA.

(66) Il convient que les fabricants notifient les vulnérabilités activement exploitées afin que les CSIRT désignés comme coordinateurs, et l'ENISA, aient une bonne vue d'ensemble de ces vulnérabilités et reçoivent les informations nécessaires à l'accomplissement des tâches qui leur incombent en vertu de la directive (UE) 2022/2555 et à l'élévation du niveau global de cybersécurité des entités essentielles et importantes visées à l'article 3 de ladite directive, ainsi qu'afin de garantir le fonctionnement efficace des autorités de surveillance du marché. 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. L'ENISA devrait, en accord avec le fabricant, divulguer les vulnérabilités fixes à la base de données européenne sur les vulnérabilités établie en vertu de l'article 12, paragraphe 2, de la directive (UE) 2022/2555. La base de données européenne sur les vulnérabilités aidera les fabricants à détecter les vulnérabilités exploitables constatées dans leurs produits afin de garantir que les produits mis sur le marché sont sûrs.

(67) Les fabricants devraient également notifier au CSIRT désigné comme coordinateur et à l'ENISA tout incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques. Afin de garantir que les utilisateurs puissent réagir rapidement aux graves incidents ayant des répercussions 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 les répercussions 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 de cybersécurité le justifient, en contactant directement les utilisateurs.

(68) Les vulnérabilités activement exploitées concernent les cas où un fabricant établit qu'une faille de sécurité touchant ses utilisateurs ou toute autre personne physique ou morale résulte de l'utilisation par une personne malveillante d'une faille dans l'un des produits comportant des éléments numériques mis à disposition sur le marché par le fabricant. Il peut s'agir par exemple de vulnérabilités dans les fonctions d'identification et d'authentification d'un produit. Les vulnérabilités qui sont découvertes sans intention malveillante pour les besoins d'essais, d'enquêtes, de correction ou de divulgation de bonne foi afin de renforcer la sécurité ou la sûreté du propriétaire du système et de ses utilisateurs ne devraient pas faire l'objet de notifications obligatoires. Les incidents graves ayant des répercussions sur la sécurité du produit comportant des éléments numériques sont, quant à eux, des situations dans lesquelles un incident de cybersécurité perturbe les processus de développement, de production ou de maintenance du fabricant d'une manière telle qu'il pourrait en résulter un risque accru de cybersécurité pour les utilisateurs ou d'autres personnes. Un tel incident grave pourrait notamment désigner la situation dans laquelle un pirate aurait réussi à introduire un code malveillant dans le canal de diffusion par lequel le fabricant publie ses mises à jour de sécurité à l'intention des utilisateurs.

(69) Pour garantir que les notifications peuvent être diffusées rapidement à tous les CSIRT désignés comme coordinateurs et pour permettre aux fabricants de soumettre une seule notification à chaque étape du processus de notification, l'ENISA doit créer une plateforme unique de signalement avec des points finaux de notification électronique nationaux. Les opérations quotidiennes de la plateforme unique de signalement doivent être administrées par l'ENISA qui en assurera le fonctionnement. Les CSIRT désignés comme coordinateurs doivent informer leurs autorités de surveillance du marché respectives des vulnérabilités ou incidents qui ont été notifiés. La plateforme unique de signalement devrait être conçue de manière à garantir la confidentialité des notifications, en particulier en ce qui concerne les vulnérabilités pour lesquelles une mise à jour de sécurité n'est pas encore disponible. En outre, l'ENISA devrait mettre en place des procédures pour traiter les informations de manière sûre et confidentielle. 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 institué en vertu de l'article 14 de la directive (UE) 2022/2555.

(70) Dans des circonstances exceptionnelles et en particulier à la demande du fabricant, le CSIRT désigné comme coordinateur qui reçoit le premier une notification devrait pouvoir décider de retarder sa diffusion aux autres CSIRT concernés désignés comme coordinateurs via la plateforme unique de signalement, lorsque cela peut être justifié par des motifs ayant trait à la cybersécurité et pour la durée strictement nécessaire. Le CSIRT désigné comme coordinateur doit immédiatement informer l'ENISA de la décision de retarder la diffusion et des raisons de ce retard, ainsi que de la date à laquelle il prévoit de procéder à cette diffusion. La Commission devrait élaborer, par voie d'un acte délégué, des spécifications sur les modalités et conditions d'application des motifs ayant trait à la cybersécurité et devrait coopérer avec le réseau des CSIRT établi en vertu de l'article 15 de la directive (UE) 2022/2555 et l'ENISA pour préparer le projet d'acte délégué. Parmi les exemples de motifs ayant trait à la cybersécurité, figurent une procédure coordonnée de divulgation des vulnérabilités ou bien des situations dans lesquelles un fabricant est censé fournir une mesure d'atténuation à brève échéance et où les risques pour la cybersécurité d'une diffusion immédiate via la plateforme unique de signalement l'emportent sur les avantages qu'elle apporterait. Si le CSIRT désigné comme coordinateur le demande, l'ENISA doit être en mesure de l'aider à faire valoir les motifs liés à la cybersécurité pour retarder la diffusion de la notification sur la base des informations que l'ENISA a reçues de ce CSIRT sur la décision de ne pas diffuser une notification pour lesdits motifs. De plus, dans des circonstances tout à fait exceptionnelles, il y a lieu que l'ENISA ne reçoive pas simultanément tous les détails d'une notification de vulnérabilité activement exploitée.

Ce serait le cas lorsque le fabricant indique dans sa notification que la vulnérabilité notifiée a été activement exploitée par une personne malveillante et que, selon les informations disponibles, elle n'a été exploitée dans aucun autre État membre que celui du CSIRT désigné comme coordinateur auquel le fabricant a notifié la vulnérabilité, lorsque toute nouvelle diffusion immédiate de la vulnérabilité notifiée entraînerait probablement la transmission d'informations dont la divulgation serait contraire aux intérêts essentiels de cet État membre, ou lorsque la vulnérabilité notifiée présente un risque élevé et imminent de cybersécurité du fait de sa diffusion ultérieure. Dans de tels cas, l'ENISA ne recevra simultanément que l'information qu'une notification a été effectuée par le fabricant, des informations générales sur le produit comportant des éléments numériques concerné, l'information sur la nature générale de l'exploitation et l'information sur le fait que ces motifs de sécurité ont été soulevés par le fabricant et que le contenu complet de la notification n'est donc pas divulgué. La notification complète doit alors être mise à la disposition de l'ENISA et d'autres CSIRT désignés comme coordinateurs lorsque le CSIRT désigné comme coordinateur qui reçoit le premier la notification constate que ces motifs de sécurité, en raison de circonstances particulièrement exceptionnelles telles qu'établies dans le présent règlement, ont disparu. Lorsque, sur la base des informations disponibles, l'ENISA considère qu'il existe un risque systémique compromettant la sécurité du marché intérieur, elle doit recommander au CSIRT destinataire de diffuser la notification complète aux autres CSIRT désignés comme coordinateurs et à l'ENISA elle-même.

(71) Lorsque les fabricants notifient une vulnérabilité activement exploitée ou un incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques, ils doivent indiquer la nature sensible qu'ils estiment devoir attribuer à l'information notifiée. Le CSIRT désigné comme coordinateur qui reçoit le premier la notification doit tenir compte de ces informations lorsqu'il évalue si la notification donne lieu à des circonstances exceptionnelles qui justifient de retarder la diffusion de la notification aux autres CSIRT concernés désignés comme coordinateurs, pour des motifs justifiés ayant trait à la cybersécurité. Il doit également tenir compte de ces informations lorsqu'il évalue si la notification d'une vulnérabilité activement exploitée donne lieu à des circonstances particulièrement exceptionnelles qui justifient que la notification complète ne soit pas mise à la disposition de l'ENISA au même moment. Enfin, les CSIRT désignés comme coordinateurs devraient être en mesure de prendre en considération ces informations lorsqu'ils définissent les mesures appropriées pour atténuer les risques découlant de ces vulnérabilités et incidents.

(72) Afin de simplifier la communication des informations requises au titre du présent règlement, compte tenu des autres exigences complémentaires en matière de communication prévues par le droit de l'Union, telles que le règlement (UE) 2016/679, le règlement (UE) 2022/2554 du Parlement européen et du Conseil[24], la directive 2002/58/CE du Parlement européen et du Conseil[25] et la directive (UE) 2022/2555, et afin de réduire la charge administrative pesant sur les entités, les États membres sont incités à étudier la possibilité de mettre en place, au niveau national, des points d'entrée uniques pour lesdites exigences en matière de communication d'informations. L'utilisation de ces points d'entrée uniques nationaux pour la notification des incidents de sécurité au titre du règlement (UE) 2016/679 et de la directive 2002/58/CE ne devrait pas affecter l'application des dispositions du règlement (UE) 2016/679 et de la directive 2002/58/CE, en particulier celles relatives à l'indépendance des autorités qui y sont visées. Lors de la mise en place de la plateforme unique de signalement visée dans le présent règlement, l'ENISA doit prendre en compte la possibilité pour les points finaux nationaux de notification électronique visés dans le présent règlement d'être intégrés dans des points d'entrée uniques nationaux qui peuvent également regrouper d'autres notifications requises par le droit de l'Union.

---

[24] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).

[25] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO L 201 du 31.7.2002, p. 37).

(73) Lors de la mise en place de la plateforme unique de signalement visée dans le présent règlement et afin de mettre à profit l'expérience acquise, l'ENISA devrait consulter d'autres institutions ou agences de l'Union qui gèrent des plateformes ou des bases de données soumises à de strictes exigences de sécurité, telles que l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice (eu-LISA). L'ENISA devrait également analyser les possibilités de complémentarité avec la base de données européenne sur les vulnérabilités établie en vertu de l'article 12, paragraphe 2, de la directive (UE) 2022/2555.

(74) Les fabricants et autres personnes physiques et morales devraient pouvoir notifier à un CSIRT désigné comme coordinateur ou à l'ENISA, à titre volontaire, toute vulnérabilité contenue dans un produit comportant des éléments numériques, les cybermenaces qui pourraient influer sur le profil de risque d'un produit comportant des éléments numériques, tout incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques ainsi que les incidents évités de justesse qui auraient pu déboucher sur un tel incident.

(75) Les États membres devraient s'efforcer de traiter, dans la mesure du possible, les difficultés auxquelles sont confrontés les experts qui recherchent les vulnérabilités, y compris le risque lié à la responsabilité pénale potentielle, conformément au droit national. Étant donné que les personnes morales et physiques qui recherchent les vulnérabilités pourraient, dans certains États membres, être exposées à une responsabilité pénale et civile, les États membres sont encouragés à adopter des lignes directrices concernant l'absence de poursuites contre les auteurs de recherches en matière de sécurité de l'information et une exemption de responsabilité civile pour leurs activités.

(76) 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 soit directement au fabricant soit indirectement et, sur demande, de manière anonyme, par l'intermédiaire des CSIRT désignés comme coordinateurs aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555. Toute politique de divulgation coordonnée des vulnérabilités par les fabricants 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. En outre, les fabricants devraient également étudier la possibilité de publier leurs politiques de sécurité dans un format lisible par machine. 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. Il s'agit de ce que l'on appelle les programmes dits de "prime aux bogues".

(77) 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 telle nomenclature 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 en particulier aider les fabricants et les utilisateurs à suivre les vulnérabilités et les risques émergents nouvellement apparus en matière de cybersécurité. Il est particulièrement important pour les fabricants de s'assurer que leurs produits comportant des éléments numériques ne contiennent pas de composants vulnérables développés par des tiers. Les fabricants ne devraient pas être tenus de rendre publique la nomenclature des logiciels.

(78) Dans le cadre des nouveaux modèles commerciaux complexes liés aux ventes en ligne, une entreprise exerçant ses activités en ligne peut fournir toute une série de services. Selon la nature des services fournis en rapport avec un produit donné comportant des éléments numériques, la même entité peut relever de différentes catégories de modèles d'entreprise ou d'opérateurs économiques. Lorsqu'une entité fournit uniquement des services d'intermédiation en ligne pour un produit donné comportant des éléments numériques et n'est qu'un fournisseur d'une place de marché en ligne au sens de l'article 3, point 14), du règlement (UE) 2023/988, elle ne peut être considérée comme l'un des types d'opérateurs économiques définis dans le présent règlement. Lorsque la même entité est un fournisseur d'une place de marché en ligne et agit également comme opérateur économique au sens du présent règlement, pour la vente de produits particuliers comportant des éléments numériques, elle devrait être soumise aux obligations prévues par le présent règlement pour ce type d'opérateur économique. Par exemple, si le fournisseur d'une place de marché en ligne distribue également un produit comportant des éléments numériques, il sera alors considéré, en ce qui concerne la vente de ce produit, comme un distributeur. De même, si l'entité en question vend des produits de sa propre marque qui comportent des éléments numériques, elle serait considérée comme un fabricant et devrait donc se conformer aux exigences applicables aux fabricants. En outre, certaines entités peuvent être considérées comme des prestataires de services d'exécution des commandes au sens de l'article 3, point 11), du règlement (UE) 2019/1020 du Parlement européen et du Conseil[26] si elles proposent de tels services. Ces situations devraient être appréciées au cas par cas. Les places de marché en ligne jouant un rôle de premier plan dans le commerce électronique, elles devraient s'efforcer de coopérer avec les autorités de surveillance du marché des États membres pour contribuer à veiller à ce que les produits comportant des éléments numériques qui sont achetés par leur intermédiaire respectent les exigences de cybersécurité prévues par le présent règlement.

---

[26] 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) n° 765/2008 et (UE) n° 305/2011 (JO L 169 du 25.6.2019, p. 1).

(79) Afin de faciliter l'évaluation de la conformité aux exigences prévues 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 de cybersécurité énoncées dans le présent règlement en spécifications techniques détaillées et sont adoptées conformément au règlement (UE) n° 1025/2012 du Parlement européen et du Conseil[27]. Ledit règlement prévoit une procédure pour la formulation d'objections à l'encontre de normes harmonisées lorsque celles-ci ne satisfont pas pleinement aux exigences énoncées dans le présent règlement. Le processus de normalisation devrait garantir une représentation équilibrée des intérêts et la participation effective des parties prenantes de la société civile, y compris des organisations de consommateurs. Les normes internationales qui sont conformes au niveau de protection en matière de cybersécurité visé par les exigences essentielles de cybersécurité prévues par le présent règlement devraient également être prises en compte, afin de faciliter l'élaboration de normes harmonisées et la mise en œuvre du présent règlement, ainsi que la mise en conformité des entreprises, en particulier des microentreprises et des petites et moyennes entreprises, et de celles qui exercent leurs activités à l'échelle mondiale.

---

[27] Règlement (UE) n° 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 n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

(80) L'élaboration en temps utile de normes harmonisées au cours de la période transitoire pour l'application du présent règlement et leur disponibilité avant la date d'application du présent règlement seront particulièrement importantes pour sa mise en œuvre effective. C'est notamment le cas des produits importants comportant des éléments numériques qui relèvent de la classe I. La disponibilité de normes harmonisées permettra aux fabricants de ces produits d'effectuer les évaluations de la conformité selon la procédure de contrôle interne et peut ainsi éviter les goulets d'étranglement et les retards dans les activités des organismes d'évaluation de la conformité.

(81) Le règlement (UE) 2019/881 établit un cadre européen de certification volontaire de cybersécurité pour les produits TIC, les processus TIC et les services TIC. Les schémas européens de certification de cybersécurité offrent un cadre commun de confiance pour les utilisateurs des produits comportant des éléments numériques qui entrent dans le champ d'application du présent règlement. Le présent règlement devrait dès lors créer des synergies avec le règlement (UE) 2019/881. Afin de faciliter l'évaluation de la conformité aux exigences prévues par 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 européen de cybersécurité conformément au règlement (UE) 2019/881 qui a été désigné par la Commission dans un acte d'exécution, sont présumés conformes aux exigences essentielles de cybersécurité énoncées dans le présent règlement pour autant que le certificat européen de cybersécurité 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, y compris lors de l'élaboration du programme de travail glissant de l'Union conformément au règlement (UE) 2019/881. Lorsqu'il est nécessaire d'établir un nouveau schéma régissant les produits comportant des éléments numériques, notamment pour faciliter la mise en conformité avec le présent règlement, la Commission peut demander à l'ENISA d'élaborer des schémas candidats conformément à l'article 48 du règlement (UE) 2019/881. Ces futurs schémas européens de certification de cybersécurité, destinés à couvrir les produits comportant des éléments numériques, devraient tenir compte des exigences essentielles de cybersécurité et des procédures d'évaluation de la conformité énoncées dans le présent règlement et faciliter le respect de celui-ci. Pour les schémas européens de certification de cybersécurité qui entrent en vigueur avant l'entrée en vigueur du présent règlement, des précisions peuvent être nécessaires sur les modalités selon lesquelles la présomption de conformité peut s'appliquer.

Il convient d'habiliter, par voie d'actes délégués, la Commission à préciser dans quelles conditions les schémas européens de certification de cybersécurité peuvent être utilisés pour démontrer la conformité aux exigences essentielles de cybersécurité énoncées dans le présent règlement. En outre, afin d'éviter une charge administrative excessive, il ne devrait y avoir aucune obligation pour les fabricants de faire procéder à une évaluation de conformité par un tiers comme le prévoit le présent règlement pour les exigences correspondantes lorsqu'un certificat européen de cybersécurité a été délivré au titre desdits schémas européens de certification de cybersécurité, au moins au niveau substantiel.

(82) Dès l'entrée en vigueur du règlement d'exécution (UE) 2024/482 relatif aux produits relevant du champ d'application du présent règlement, tels que les modules de sécurité matériels et les microprocesseurs, la Commission devrait être en mesure de préciser, par voie d'un acte délégué, comment la certification EUCC crée une présomption de conformité aux exigences essentielles de cybersécurité énoncées dans le présent règlement ou à certaines de ses parties En outre, cet acte délégué peut définir comment un certificat délivré au titre de la EUCC 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.

(83) Le cadre de normalisation européen en vigueur qui repose sur les principes de la nouvelle approche définie dans la résolution du Conseil du 7 mai 1985 concernant une nouvelle approche en matière d'harmonisation technique et de normalisation et sur le règlement (UE) n° 1025/2012 constitue par défaut le cadre régissant l'élaboration des normes prévoyant la présomption de conformité aux exigences essentielles de cybersécurité pertinentes énoncées dans le présent règlement. Les normes européennes devraient être axées sur le marché et tenir compte de l'intérêt public, ainsi que des objectifs stratégiques clairement énoncés dans la demande que la Commission adresse à une ou plusieurs organisations européennes de normalisation pour qu'elles élaborent des normes harmonisées, dans un délai déterminé et sur la base d'un consensus. Toutefois, en l'absence de références pertinentes à des normes harmonisées, la Commission devrait pouvoir adopter des actes d'exécution établissant des spécifications communes pour les exigences essentielles de cybersécurité énoncées dans le présent règlement, à condition que, ce faisant, elle respecte dûment le rôle et les fonctions des organismes de normalisation, en tant que solution de repli exceptionnelle pour faciliter l'obligation du fabricant de se conformer à ces exigences essentielles de cybersécurité, lorsque le processus de normalisation est bloqué ou lorsqu'il y a des retards dans l'établissement de normes harmonisées appropriées. Si un tel retard est dû à la complexité technique de la norme en question, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes.

(84) Afin d'établir, avec la plus grande efficacité, des spécifications communes applicables aux exigences essentielles de cybersécurité énoncées dans le présent règlement, la Commission devrait associer au processus les parties prenantes concernées.

(85) Par délai raisonnable, en lien avec la publication d'une référence à des normes harmonisées au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012, on entend la période pendant laquelle est attendue la publication au *Journal officiel de l'Union européenne* de la référence à la norme, de son rectificatif ou de sa modification, période qui ne doit pas être supérieure à une année après l'expiration du délai d'élaboration d'une norme européenne fixé conformément au règlement (UE) n° 1025/2012.

(86) Afin de faciliter l'évaluation de la conformité aux exigences essentielles de cybersécurité énoncées dans 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.

(87) L'application de normes harmonisées, de spécifications communes ou de schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 et fournissant une présomption de conformité en ce qui concerne les exigences essentielles applicables aux produits comportant des éléments numériques facilitera l'évaluation de la conformité par les fabricants. Si le fabricant choisit de ne pas recourir à ces moyens pour certaines exigences, il doit indiquer dans sa documentation technique de quelle autre manière la conformité est respectée. En outre, l'application de normes harmonisées, de spécifications communes ou de schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 et fournissant une présomption de conformité par les fabricants faciliterait le contrôle, par les autorités de surveillance du marché, de la conformité des produits comportant des éléments numériques. Par conséquent, les fabricants de produits comportant des éléments numériques sont incités à appliquer ces normes harmonisées, spécifications communes ou schémas européens de certification de cybersécurité.

(88) 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 essentielles de cybersécurité énoncées dans le présent règlement et, le cas échéant, par d'autres législations d'harmonisation de l'Union applicables dont relève le produit comportant des éléments numériques. Les fabricants peuvent également être tenus d'établir une déclaration UE de conformité en vertu d'autres actes juridiques 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 juridiques 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.

(89) 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) n° 765/2008 du Parlement européen et du Conseil[28] 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 énoncées dans le présent règlement.

---

[28] Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) n° 339/93 (JO L 218 du 13.8.2008, p. 30).

(90) Afin de permettre aux opérateurs économiques de démontrer qu'ils respectent les exigences essentielles de cybersécurité 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 nécessaire de prévoir des procédures d'évaluation de la conformité. La décision n° 768/2008/CE du Parlement européen et du Conseil[29] 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 devraient être fondées sur ces modules afin de vérifier la conformité des produits comportant des éléments numériques aux exigences essentielles de cybersécurité 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 comportant des éléments numériques.

[29] Décision n° 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).

(91) L'évaluation de la conformité des produits comportant des éléments numériques qui ne sont pas répertoriés dans le présent règlement en tant que produits importants ou critiques comportant des éléments numériques peut être effectuée par le fabricant sous sa propre responsabilité, conformément à la procédure de contrôle interne fondée sur le module A de la décision 768/2008/CE, conformément au présent règlement. Cela s'applique également aux cas où un fabricant choisit de ne pas appliquer, en tout ou en partie, une norme harmonisée, une spécification commune ou un schéma européen de certification de cybersécurité applicable. Le fabricant conserve la possibilité de choisir une procédure d'évaluation de la conformité plus stricte faisant intervenir un tiers. Dans le cadre de la procédure d'évaluation de la conformité par contrôle interne, le fabricant assure et déclare sous sa seule responsabilité que le produit comportant des éléments numériques et les procédés du fabricant satisfont aux exigences essentielles de cybersécurité applicables définies dans le présent règlement. Si un produit important comportant des éléments numériques relève de la classe I, une assurance supplémentaire est requise pour démontrer la conformité aux exigences essentielles de cybersécurité énoncées dans le présent règlement. Le fabricant devrait appliquer des normes harmonisées, des spécifications communes ou des schémas européens de certification de cybersécurité adoptés conformément au 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 européens de certification de cybersécurité, il devrait se soumettre à une évaluation de la conformité par un tiers (sur la base des modules B et C ou du module H). 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 et C ou du module 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 importants 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 importants comportant des éléments numériques qui relèvent de la classe II, l'évaluation de la conformité de ces produits devrait toujours prévoir l'intervention d'un tiers, même lorsque le produit est conforme, en tout ou en partie, à des normes harmonisées, à des spécifications communes ou à des schémas européens de certification de cybersécurité. Les fabricants de produits importants comportant des éléments numériques répondant aux critères de logiciels libres et ouverts devraient pouvoir suivre la procédure de contrôle interne basée sur le module A, à condition de mettre la documentation technique à la disposition du public.

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

(93) En ce qui concerne les microentreprises et les petites entreprises, il convient, afin de garantir la proportionnalité, de réduire les frais administratifs sans pour autant que le niveau de cyberprotection des produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement non plus que l'équité des conditions de concurrence entre les fabricants en pâtissent. Il convient donc que la Commission établisse un formulaire de documentation technique simplifiée ciblant les besoins des microentreprises et des petites entreprises. Il convient que le formulaire de documentation technique simplifiée adopté par la Commission porte sur l'ensemble des éléments applicables relatifs à la documentation technique prévue dans le présent règlement et qu'il précise les modalités suivant lesquelles une microentreprise ou une petite entreprise peut fournir de manière concise les éléments demandés, tels que la description de la conception, du développement et de la fabrication du produit comportant des éléments numériques. Ainsi, le formulaire contribuerait à alléger la charge administrative de la conformité en apportant aux entreprises concernées une sécurité juridique quant au périmètre et au niveau de détail requis des informations à fournir. Il convient de permettre également aux microentreprises et aux petites entreprises de choisir de fournir sous forme développée les éléments applicables relatifs à la documentation technique et de ne pas recourir au formulaire de documentation technique simplifiée mis à leur disposition.

(94) Il importe, pour encourager et protéger l'innovation, de prêter une attention particulière aux intérêts des fabricants qui sont des microentreprises ou des petites et moyennes entreprises, et en particulier des microentreprises et des petites entreprises, y compris les jeunes pousses. À cette fin, les États membres pourraient élaborer des initiatives ciblant les fabricants qui sont des microentreprises ou des petites entreprises, notamment en matière de formation, de sensibilisation, de communication des informations et d'activités d'essai et d'évaluation de la conformité par un tiers, ainsi que créer des sas réglementaires. Les coûts de traduction liés aux documents obligatoires, tels que la documentation technique et les informations et instructions destinées à l'utilisateur exigées en vertu du présent règlement, ainsi qu'à la communication avec les autorités, peuvent être importants pour les fabricants, en particulier s'ils sont de petite taille. Les États membres devraient donc pouvoir envisager qu'une des langues qu'ils choisissent et acceptent pour la documentation pertinente des fabricants et pour la communication avec les fabricants soit une langue largement comprise par le plus grand nombre possible d'utilisateurs.

(95) Pour garantir une bonne application du présent règlement, les États membres devraient s'efforcer de garantir, avant la date d'application du présent règlement, la disponibilité en nombre suffisant d'organismes notifiés à même de réaliser des évaluations de la conformité par un tiers. La Commission devrait s'efforcer d'aider les États membres et les autres parties concernées dans cette démarche afin d'éviter aux fabricants les goulets d'étranglement et les obstacles à l'entrée sur le marché. Des activités de formation ciblées, menées par les États membres, y compris, le cas échéant, avec l'appui de la Commission, peuvent contribuer à la disponibilité de professionnels qualifiés, y compris pour aider les organismes notifiés dans leurs activités au titre du présent règlement. En outre, étant donné les coûts que peut engendrer l'évaluation de la conformité par un tiers, il convient d'envisager la mise en place d'initiatives de financement au niveau de l'Union et au niveau national afin de s'efforcer de réduire ces coûts pour les microentreprises et les petites entreprises.

(96) Afin de garantir la proportionnalité, il convient que les organismes d'évaluation de la conformité, lorsqu'ils fixent les redevances imposées pour les procédures d'évaluation de la conformité, tiennent compte des intérêts et besoins spécifiques des microentreprises et des petites et moyennes entreprises, y compris les jeunes pousses. En particulier, il convient que les organismes d'évaluation de la conformité n'appliquent la procédure d'examen et les essais pertinents prévus dans le présent règlement que lorsqu'il y a lieu et suivant une approche fondée sur les risques.

(97) Les sas réglementaires devraient avoir pour objectif de renforcer l'innovation et la compétitivité des entreprises en créant des environnements d'essai contrôlés avant la mise sur le marché de produits comportant des éléments numériques. Il convient que les sas réglementaires contribuent au renforcement de la sécurité juridique pour l'ensemble des acteurs qui relèvent du champ d'application du présent règlement et accélèrent l'accès au marché de l'Union des produits comportant des éléments numériques, en particulier s'ils sont fournis par des microentreprises et des petites entreprises, y compris des jeunes pousses.

(98) 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.

(99) 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) n° 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.

(100) Il convient d'évaluer et de notifier à nouveau conformément au présent règlement les organismes d'évaluation de la conformité qui ont été accrédités et notifiés conformément au droit de l'Union définissant des exigences similaires à celles prévues par le présent règlement, par exemple un organisme d'évaluation de la conformité qui a été notifié dans le cadre d'un schéma européen de certification de cybersécurité adopté conformément au règlement (UE) 2019/881 ou notifié conformément au règlement délégué (UE) 2022/30. Toutefois, les autorités concernées peuvent prévoir des synergies en cas de chevauchement d'exigences afin d'éviter toute charge financière et administrative inutile et de garantir le bon déroulement en temps utile du processus de notification.

(101) L'accréditation organisée de manière transparente, ainsi que le prévoit le règlement (CE) n° 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.

(102) 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.

(103) 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.

(104) 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.

(105) 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 d'assurer une coordination et une coopération appropriées entre les organismes notifiés.

(106) La surveillance du marché est un outil essentiel pour assurer l'application correcte et uniforme du droit 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 s'appliquent aux produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement.

(107) Conformément au règlement (UE) 2019/1020, une autorité de surveillance du marché est chargée de la surveillance du marché sur le territoire de l'État membre qui l'a désignée. Le présent règlement ne devrait pas empêcher les États membres de choisir les autorités compétentes pour l'accomplissement des tâches de surveillance du marché. Chaque État membre devrait désigner une ou plusieurs autorités de surveillance du marché sur son territoire. Les États membres devraient pouvoir choisir de désigner toute autorité existante ou nouvelle pour agir en qualité d'autorité de surveillance du marché, y compris les autorités compétentes désignées ou établies en vertu de l'article 8 de la directive (UE) 2022/2555, les autorités nationales de certification de cybersécurité désignées en vertu de l'article 58 du règlement (UE) 2019/881 ou les autorités de surveillance du marché désignées aux fins de la directive 2014/53/UE. 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 du marché qui leur incombent en vertu du présent règlement. En vertu de 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.

(108) Il convient de créer un groupe de coopération administrative (ADCO) chargé spécifiquement de la cyberrésilience des produits comportant des éléments numériques aux fins de l'application uniforme du présent règlement, conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. L'ADCO devrait être composé de représentants des autorités de surveillance du marché désignées 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 en vertu de l'article 29 du règlement (UE) 2019/1020 et composé de représentants de chaque État membre, y compris un représentant de chaque bureau de liaison unique visé à l'article 10 dudit règlement et un expert national facultatif, des présidents des ADCO et de représentants de la Commission. La Commission devrait participer aux réunions du réseau de l'Union pour la conformité des produits, de ses sous-groupes et de l'ADCO. Elle devrait également assister l'ADCO au moyen d'un secrétariat exécutif qui lui fournirait une assistance technique et logistique. L'ADCO pourrait également inviter des experts indépendants et nouer des liens avec d'autres ADCO, tels que ceux établis conformément à la directive 2014/53/UE.

(109) Les autorités de surveillance du marché, par l'intermédiaire de l'ADCO établi en vertu du présent règlement, devraient coopérer étroitement entre elles et être en mesure d'élaborer des documents d'orientation afin de faciliter les activités de surveillance du marché au niveau national, par exemple en indiquant des bonnes pratiques et en élaborant des indicateurs qui permettent de vérifier efficacement la conformité des produits comportant des éléments numériques au présent règlement.

(110) 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.

(111) 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 visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555 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 comportant des éléments numériques, l'État membre devrait informer la Commission et les autres États membres sans retard des mesures provisoires prises, en justifiant sa décision. Lorsqu'une autorité de surveillance du marché adopte de telles mesures à l'encontre de produits comportant des éléments numériques qui présentent 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 devrait également envisager l'adoption de propositions de révision de la législation de l'Union pertinente.

(112) 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, pour le respect d'obligations prévues par le droit de l'Union ou le droit national à des fins de protection des droits fondamentaux ou pour la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services offerts au moyen d'un système d'information électronique par des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555, la Commission devrait pouvoir demander à l'ENISA de procéder à une évaluation. Sur la base de cette évaluation, la Commission devrait pouvoir adopter, par voie d'actes d'exécution, des mesures correctives ou restrictives au niveau de l'Union, y compris en exigeant le retrait du marché ou le rappel des produits comportant des éléments numériques concernés, dans un délai raisonnable, proportionné à la nature du risque. La Commission ne devrait pouvoir 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 du marché pour remédier à la situation. De telles circonstances exceptionnelles peuvent être des situations d'urgence dans lesquelles, par exemple, un produit comportant des éléments numériques 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 (UE) 2022/2555, 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 devrait pouvoir 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.

(113) 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.

(114) 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 indices suggèrent que certaines catégories de produits comportant des éléments numériques présentent souvent des risques de cybersécurité. En outre, lors de la sélection des catégories de produits devant faire l'objet d'opérations "coup de balai", il convient que les autorités de surveillance du marché tiennent également compte de circonstances relatives à des facteurs de risque non techniques. Pour ce faire, il convient que les autorités de surveillance du marché puissent tenir compte des résultats des évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22 de la directive (UE) 2022/2555, y compris les circonstances relatives à des facteurs de risque non techniques. L'ENISA devrait soumettre aux autorités de surveillance du marché des propositions concernant des catégories de produits comportant des éléments numériques pour lesquelles des opérations simultanées pourraient être organisées, sur la base, entre autres, des notifications de vulnérabilités et d'incidents qu'elle reçoit.

(115) 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. L'ENISA 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 un non-respect potentiel du présent règlement, dans plusieurs États membres, de produits comportant des éléments numériques ou recenser les catégories de produits pour lesquelles des opérations "coup de balai" devraient être organisées. Dans des circonstances exceptionnelles, l'ENISA devrait, à la demande de la Commission, 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.

(116) Le présent règlement attribue à l'ENISA certaines tâches qui exigent des ressources adaptées, tant en termes de savoir-faire que de ressources humaines, pour être menées à bien de manière efficace. La Commission proposera les ressources budgétaires nécessaires pour le tableau des effectifs de l'ENISA, conformément à la procédure prévue à l'article 29 du règlement (UE) 2019/881, lorsqu'elle élaborera le projet de budget général de l'Union. Au cours de ce processus, la Commission examinera l'ensemble des ressources dont dispose l'ENISA pour mener à bien ses missions, y compris celles qui lui sont conférées en vertu du présent règlement.

(117) 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 sur le fonctionnement de l'Union européenne en ce qui concerne l'établissement et la mise à jour de la liste figurant en annexe des produits importants comportant des éléments numériques. 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 au titre d'un schéma européen de certification de cybersécurité des produits critiques comportant des éléments numériques énoncés en annexe du présent règlement, en ce qui concerne la mise à jour de la liste des produits critiques comportant des éléments numériques sur la base des critères de criticité énoncés dans le présent règlement, et en ce qui concerne la désignation des schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 qui peuvent être utilisés pour démontrer le respect des exigences essentielles de cybersécurité ou de parties de celles-ci énoncées en annexe au présent règlement. Il convient également de déléguer à la Commission le pouvoir d'adopter des actes pour préciser la période d'assistance minimale pour des catégories spécifiques de produits lorsque les données de surveillance du marché tendent à indiquer des périodes d'assistance insuffisantes, ainsi que pour préciser les conditions d'application des motifs ayant trait à la cybersécurité en lien avec des retards de diffusion de notifications de vulnérabilités activement exploitées.

En outre, il convient de déléguer à la Commission le pouvoir d'adopter des actes pour créer des programmes volontaires d'attestation de sécurité afin d'évaluer la conformité des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts à l'ensemble ou à certaines des exigences essentielles de cybersécurité ou d'autres obligations prévues par le présent règlement, ainsi que pour préciser le contenu minimal de la déclaration UE de conformité et pour 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"[30]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués. Le pouvoir d'adopter des actes délégués en vertu du présent règlement devrait être conféré à la Commission pour une période de cinq ans à compter du ... [*date d'entrée en vigueur du présent règlement*]. La Commission devrait élaborer un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir devrait être tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

[30] JO L 123 du 12.5.2016, p. 1.

(118) 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 spécifie la description technique des catégories de produits importants comportant des éléments numériques qui figurent en annexe du présent règlement, qu'elle spécifie le format et les éléments de la nomenclature des logiciels, qu'elle précise davantage le format et la procédure des notifications de vulnérabilités activement exploitées et d'incidents graves ayant des répercussions sur la sécurité de produits comportant des éléments numériques soumises par les fabricants, qu'elle établisse des spécifications communes couvrant les exigences techniques qui offrent un moyen de se conformer aux exigences essentielles de cybersécurité énoncées en annexe du présent règlement, qu'elle établisse des spécifications techniques pour les étiquettes, pictogrammes ou toute autre marque liée à la sécurité des produits comportant des éléments numériques, leur période d'assistance ainsi que les mécanismes visant à promouvoir leur utilisation et à sensibiliser le public à la sécurité des produits comportant des éléments numériques, qu'elle définisse le formulaire de documentation technique simplifiée ciblant les besoins des microentreprises et des petites entreprises et qu'elle décide 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) n° 182/2011 du Parlement européen et du Conseil[31].

(119) Afin de garantir une coopération constructive et de 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.

---

[31] Règlement (UE) n° 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(120) 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 la législation nationale en cas de non-respect des obligations prévues par le présent règlement. Pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas devraient être prises en considération et, au minimum, celles explicitement établies dans le présent règlement, y compris la question de savoir si le fabricant est une microentreprise ou une petite ou moyenne entreprise, y compris une jeune pousse, et si des amendes administratives ont déjà été imposées par la même ou par d'autres autorités de surveillance du marché au même opérateur économique pour une infraction similaire. De telles caractéristiques seraient susceptibles d'être soit aggravantes, dans des situations où l'infraction commise par le même opérateur économique 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 caractéristiques spécifiques pertinentes, d'une sanction imposée dans d'autres États membres et de son montant. Dans tous ces 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. Étant donné qu'une amende administrative ne peut être infligée à une microentreprise ou une petite entreprise pour non-respect du délai de vingt-quatre heures fixé pour notifier une alerte précoce de vulnérabilités activement exploitées ou d'incidents graves ayant des répercussions sur la sécurité du produit comportant des éléments numériques, ni à un intendant de logiciels ouverts pour quelque infraction au présent règlement que ce soit, et compte tenu du principe qui prévoit que les sanctions soient efficaces, proportionnées et dissuasives, il convient que les États membres n'imposent auxdites entités aucun autre type de sanction de nature pécuniaire.

(121) Lorsque des amendes administratives sont imposées à une personne qui n'est 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.

(122) Il convient que les États membres, compte tenu de leurs situations nationales, examinent la possibilité d'utiliser les recettes générées par les sanctions prévues par le présent règlement, ou leur équivalent financier, pour soutenir les politiques de cybersécurité et améliorer le niveau de cybersécurité dans l'Union, notamment en augmentant le nombre de professionnels qualifiés dans le domaine de la cybersécurité, en renforçant les capacités des microentreprises et des petites et moyennes entreprises et en améliorant la sensibilisation du public aux cybermenaces.

(123) Dans ses rapports avec les pays tiers, l'Union 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 ARM 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 avec plusieurs pays tiers. Ces ARM sont conclus dans un certain nombre de secteurs spécifiques pouvant varier selon les pays tiers. Afin de faciliter davantage le commerce et compte tenu du fait que les chaînes d'approvisionnement de produits comportant des éléments numériques sont mondiales, des ARM concernant l'évaluation de la conformité peuvent être conclus par l'Union, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne, pour les produits régis par le présent règlement. La coopération avec les pays tiers 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'Union.

(124) Les consommateurs devraient être en droit de faire valoir leurs droits relatifs aux obligations imposées aux opérateurs économiques dans le cadre du présent règlement, au moyen d'actions représentatives en vertu de la directive (UE) 2020/1828 du Parlement européen et du Conseil[32]. À cette fin, le présent règlement devrait prévoir que la directive (UE) 2020/1828 s'applique aux actions représentatives concernant des infractions au présent règlement qui portent atteinte ou peuvent porter atteinte aux intérêts collectifs des consommateurs. Il convient donc de modifier l'annexe I de ladite directive en conséquence. Il appartient aux États membres de veiller à ce que ces modifications soient prises en compte dans les mesures de transposition adoptées en vertu de ladite directive, bien que l'adoption de mesures de transposition nationales à cet égard ne soit pas une condition de l'applicabilité de ladite directive à ces actions représentatives. L'applicabilité de ladite directive aux actions représentatives intentées contre les infractions aux dispositions du présent règlement commises par des opérateurs économiques qui portent atteinte ou pourraient porter atteinte aux intérêts collectifs des consommateurs devrait débuter au ... [*36 mois à compter de la date d'entrée en vigueur du présent règlement*].

(125) Le présent règlement devrait être évalué et 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. Le présent règlement facilitera le respect des obligations relatives à la sécurité de la chaîne d'approvisionnement incombant aux entités relevant du champ d'application du règlement (UE) 2022/2554 et de la directive (UE) 2022/2555 qui utilisent des produits comportant des éléments numériques. Il convient que la Commission évalue, dans le cadre de ce réexamen périodique, les effets combinés du cadre de cybersécurité de l'Union.

---

[32] Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

(126) Il convient d'accorder un délai suffisant aux opérateurs économiques afin qu'ils s'adaptent aux exigences énoncées dans le présent règlement. Le présent règlement devrait s'appliquer à partir du ... [*36 mois à compter de la date d'entrée en vigueur du présent règlement*], à l'exception des obligations de signalement concernant les vulnérabilités activement exploitées et les incidents graves ayant des répercussions sur la sécurité des produits comportant des éléments numériques, qui devraient s'appliquer à partir du ... [*21 mois à compter de la date d'entrée en vigueur du présent règlement*], et des dispositions relatives à la notification des organismes d'évaluation de la conformité, qui devraient s'appliquer à partir du ... [*18 mois à compter de la date d'entrée en vigueur du présent règlement*].

(127) Il importe de soutenir les microentreprises et les petites et moyennes entreprises, y compris les jeunes pousses, dans l'exécution du présent règlement et de réduire au minimum les risques relatifs à l'exécution résultant d'un manque de connaissances et de savoir-faire sur le marché, y compris dans le but de faciliter le respect par les fabricants des obligations qui leur incombent en vertu du présent règlement. Le programme pour une Europe numérique et d'autres programmes pertinents de l'Union fournissent un soutien financier et technique qui permet à ces entreprises de contribuer à la croissance de l'économie de l'Union et au rehaussement du niveau commun de cybersécurité au sein de l'Union. Le Centre de compétences européen en matière de cybersécurité et les centres nationaux de coordination ainsi que les pôles européens d'innovation numérique établis par la Commission et par les États membres au niveau de l'Union ou au niveau national pourraient également soutenir les entreprises et les organisations du secteur public et pourraient contribuer à l'exécution du présent règlement. Dans le cadre de leurs missions et domaines de compétence respectifs, ils pourraient apporter un soutien technique et scientifique aux microentreprises et aux petites et moyennes entreprises, par exemple pour les activités d'essai et les évaluations de la conformité par un tiers. Ils pourraient également encourager le déploiement d'outils pour faciliter l'application du présent règlement.

(128) En outre, les États membres devraient envisager des mesures complémentaires destinées à fournir des orientations et un soutien aux microentreprises et aux petites et moyennes entreprises, y compris la mise en place de sas réglementaires et de canaux de communication spécifiques. Pour rehausser le niveau de cybersécurité au sein de l'Union, les États membres peuvent également envisager de fournir une aide au développement des capacités et des compétences en matière de cybersécurité des produits comportant des éléments numériques, d'améliorer la cyberrésilience des opérateurs économiques, en particulier des microentreprises et des petites et moyennes entreprises, et de renforcer la sensibilisation du public à la cybersécurité des produits comportant des éléments numériques.

(129) 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 énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(130) 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[33] et a rendu un avis le 9 novembre 2022[34],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

---

[33] 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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[34] JO C 452 du 29.11.2022, p. 23.

Chapitre I
Dispositions générales

Article premier

Objet

Le présent règlement établit:

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

b) les exigences essentielles de cybersécurité 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 de cybersécurité relatives aux processus de gestion des vulnérabilités mis en place par les fabricants pour garantir la cybersécurité des produits comportant des éléments numériques durant la période d'utilisation prévue du produit, et les obligations incombant aux opérateurs économiques en ce qui concerne ces processus;

d) les règles relatives à la surveillance, y compris le contrôle, du marché et au contrôle de l'application des règles et exigences visées au présent article.

Article 2

Champ d'application

1. Le présent règlement s'applique aux produits comportant des éléments numériques mis à disposition sur le marché 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 juridiques 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.

4. Le présent règlement ne s'applique pas aux équipements qui relèvent du champ d'application de la directive 2014/90/UE du Parlement européen et du Conseil[35].

[35] Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146).

5. 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 de cybersécurité énoncées à l'annexe I peut être limitée ou exclue lorsque:

   a) cette limitation ou cette exclusion est compatible avec le cadre réglementaire général qui s'applique à ces produits; et

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

   La Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour compléter le présent règlement en précisant si une telle limitation ou exclusion est nécessaire, quels sont les produits et règles concernés et quelle est la portée de la limitation, le cas échéant.

6. Le présent règlement ne s'applique pas aux pièces de rechange qui sont mises à disposition sur le marché pour remplacer des composants identiques dans des produits comportant des éléments numériques et qui sont fabriquées conformément aux mêmes spécifications que les composants qu'elles sont destinées à remplacer.

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

8. Les obligations prévues dans le présent règlement n'impliquent pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

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

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) "cybersécurité": la cybersécurité au sens de l'article 2, point 1), du règlement (UE) 2019/881;

4) "logiciel": la partie d'un système d'information électronique qui consiste en un code informatique;

5) "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;

6) "composant": un logiciel ou du matériel destiné à être intégré dans un système d'information électronique;

7) "système d'information électronique": un système, y compris des équipements électriques ou électroniques, capable de traiter, de stocker ou de transmettre des données numériques;

8) "connexion logique": une représentation virtuelle d'une connexion de données mise en œuvre au moyen d'une interface logicielle;

9) "connexion physique": une connexion entre des systèmes d'information électroniques ou des composants mis en œuvre par des moyens physiques, y compris par des interfaces électriques, optiques ou mécaniques, des fils ou des ondes radio;

10) "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;

11) "point terminal": tout dispositif connecté à un réseau et servant de point d'entrée à ce réseau;

12) "opérateur économique": le fabricant, le mandataire, l'importateur, le distributeur ou une autre personne physique ou morale soumise à des obligations liées à la fabrication de produits comportant des éléments numériques ou à la mise à disposition sur le marché de produits comportant des éléments numériques conformément au présent règlement;

13) "fabricant": une 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, monétisé ou gratuit;

14) "intendant de logiciels ouverts": une personne morale, autre que le fabricant, qui a pour objectif ou finalité de fournir un soutien systématique et continu au développement de produits spécifiques comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts et sont destinés à des activités commerciales, et qui assure la viabilité de ces produits;

15) "mandataire": une personne physique ou morale établie dans l'Union ayant reçu mandat écrit du fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées;

16) "importateur": une 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;

17) "distributeur": une 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;

18) "consommateur": une personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

19) "microentreprises", "petites entreprises" et "moyennes entreprises": respectivement les microentreprises, les petites entreprises et les moyennes entreprises au sens de l'annexe de la recommandation 2003/361/CE de la Commission;

20) "période d'assistance": la période au cours de laquelle un fabricant est tenu de garantir que les vulnérabilités d'un produit comportant des éléments numériques sont traitées efficacement et conformément aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II;

21) "mise sur le marché": la première mise à disposition d'un produit comportant des éléments numériques sur le marché de l'Union;

22) "mise à disposition sur le marché": la 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;

23) "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, dans les indications publicitaires ou de vente, ainsi que dans la documentation technique;

24) "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, dans les indications publicitaires ou de vente, ainsi que dans la documentation technique, mais qui est susceptible de résulter d'un comportement humain, d'opérations techniques ou d'interactions raisonnablement prévisibles;

25) "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 ou d'une interaction avec d'autres systèmes raisonnablement prévisibles;

26) "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;

27) "évaluation de la conformité": le processus qui permet de vérifier si les exigences essentielles de cybersécurité énoncées à l'annexe I ont été respectées;

28) "organisme d'évaluation de la conformité": un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008;

29) "organisme notifié": un organisme d'évaluation de la conformité désigné en application de l'article 43 et de toute autre législation d'harmonisation de l'Union pertinente;

30) "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 de cybersécurité énoncées à l'annexe I, partie I, ou qui entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué;

31) "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 de cybersécurité énoncées à l'annexe I et toute autre législation d'harmonisation de l'Union applicable prévoyant son apposition;

32) "législation d'harmonisation de l'Union": la législation de l'Union énumérée à l'annexe I du règlement (UE) 2019/1020 et toute autre législation de l'Union harmonisant les conditions de commercialisation des produits auxquels ledit règlement s'applique;

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

34) "norme internationale": une norme internationale au sens de l'article 2, point 1) a), du règlement (UE) n° 1025/2012;

35) "norme européenne": une norme européenne au sens de l'article 2, point 1) b), du règlement (UE) n° 1025/2012;

36) "norme harmonisée": une norme harmonisée au sens de l'article 2, point 1) c), du règlement (UE) n° 1025/2012;

37) "risque de cybersécurité": le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise;

38) "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 des répercussions négatives graves, notamment en causant une perte ou une perturbation matérielle ou immatérielle considérable;

39) "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;

40) "vulnérabilité": une faiblesse, une susceptibilité ou une faille d'un produit comportant des éléments numériques qui peut être exploitée par une cybermenace;

41) "vulnérabilité exploitable": une vulnérabilité susceptible d'être utilisée efficacement par un adversaire en conditions de fonctionnement effectives;

42) "vulnérabilité activement exploitée": une vulnérabilité pour laquelle il existe des preuves fiables qu'elle a été exploitée par un acteur malveillant dans un système sans l'autorisation du propriétaire du système;

43) "incident": un incident au sens de l'article 6, point 6), de la directive (UE) 2022/2555;

44) "incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques": un incident qui entache ou est susceptible d'entacher la capacité d'un produit comportant des éléments numériques à protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou fonctions;

45) "incident évité": un incident évité au sens de l'article 6, point 5), de la directive (UE) 2022/2555;

46) "cybermenace": une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

47) "données à caractère personnel": des données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

48) "logiciel libre et ouvert": un logiciel dont le code source est partagé de manière ouverte et qui est mis à disposition sous licence libre et ouverte prévoyant tous les droits pour qu'il soit librement accessible, utilisable, modifiable et redistribuable;

49) "rappel": un rappel au sens de l'article 3, point 22), du règlement (UE) 2019/1020;

50) "retrait": un retrait au sens de l'article 3, point 23), du règlement (UE) 2019/1020;

51) "CSIRT désigné comme coordinateur": un CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555.

Article 4

Libre circulation

1. 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.

2. Lors de foires commerciales, d'expositions, de démonstrations ou d'événements similaires, les États membres n'empêchent pas la présentation ou l'utilisation d'un produit comportant des éléments numériques non conforme au présent règlement, y compris ses prototypes, à condition que le produit porte une marque visible indiquant clairement qu'il n'est pas conforme au présent règlement et ne doit pas être mis à disposition sur le marché tant qu'il ne sera pas conforme au présent règlement.

3. Les États membres n'empêchent pas la mise à disposition sur le marché 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'il porte une marque visible indiquant clairement que le logiciel n'est pas conforme au présent règlement et qu'il ne sera pas mis à disposition sur le marché à d'autres fins que les essais.

4. Le paragraphe 3 ne s'applique pas aux composants de sécurité visés dans la législation d'harmonisation de l'Union autre que le présent règlement.

Article 5

Achats publics ou utilisation de produits comportant des éléments numériques

1. Le présent règlement n'empêche pas les États membres de soumettre les produits comportant des éléments numériques à des exigences supplémentaires de cybersécurité en cas d'achats publics ou d'utilisation de ces produits à des fins spécifiques, y compris lorsque ces produits sont achetés ou utilisés à des fins de sécurité nationale ou de défense, à condition que ces exigences soient conformes aux obligations des États membres prévues par le droit de l'Union et qu'elles soient nécessaires et proportionnées à la poursuite de ces fins.

2. Sans préjudice des directives 2014/24/UE et 2014/25/UE, lors des achats publics de produits comportant des éléments numériques relevant du champ d'application du présent règlement, les États membres veillent à la prise en compte, au cours du processus d'achat public, du respect des exigences essentielles de cybersécurité énoncées à l'annexe I du présent règlement, y compris la capacité du fabricant à traiter efficacement les vulnérabilités.

Article 6

Exigences applicables aux produits comportant des éléments numériques

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

a) s'ils satisfont aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, à condition qu'ils soient correctement installés, entretenus et utilisés conformément à l'utilisation prévue ou dans des conditions raisonnablement prévisibles et, le cas échéant, que les mises à jour de sécurité nécessaires aient été installées; et

b) si les processus mis en place par le fabricant sont conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II.

Article 7

Produits importants comportant des éléments numériques

1. Les produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produit énoncée à l'annexe III sont considérés comme des produits importants comportant des éléments numériques et sont soumis aux procédures d'évaluation de la conformité visées à l'article 32, paragraphes 2 et 3. L'intégration dans un produit d'un produit comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produits énoncée à l'annexe III n'amène pas en tant que telle le produit dans lequel ledit produit comportant des éléments numériques a été intégré à être soumis aux procédures d'évaluation de la conformité visées à l'article 32, paragraphes 2 et 3.

2. Les catégories de produits comportant des éléments numériques visées au paragraphe 1 du présent article, réparties entre les classes I et II figurant à l'annexe III, remplissent au moins l'un des critères suivants:

a) le produit comportant des éléments numériques exécute des fonctions essentielles pour la cybersécurité d'autres produits, réseaux ou services, y compris la sécurisation des authentifications et des accès, la prévention et la détection des intrusions, la sécurité des points terminaux ou la protection des réseaux;

b) le produit comportant des éléments numériques exécute une fonction qui comporte un risque important d'effets néfastes du fait de son intensité et de sa capacité à perturber, contrôler ou endommager un grand nombre d'autres produits ou à porter atteinte à la santé, à la sécurité ou à la sûreté de ses utilisateurs par une manipulation directe, par exemple une fonction du système central, notamment la gestion du réseau, le contrôle de la configuration, la virtualisation ou le traitement des données à caractère personnel.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour modifier l'annexe III en ajoutant une nouvelle catégorie dans chaque classe de la liste des catégories de produits comportant des éléments numériques et en précisant la définition de celle-ci, en déplaçant une catégorie de produits d'une classe à l'autre 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 des fonctionnalités liées à la cybersécurité ou de la fonction et du niveau de risque de cybersécurité que présentent les produits comportant des éléments numériques qui répondent aux critères visés au paragraphe 2 du présent article.

Les actes délégués visés au premier alinéa du présent paragraphe prévoient, le cas échéant, une période transitoire d'au moins 12 mois, en particulier lorsqu'une nouvelle catégorie de produits importants comportant des éléments numériques est ajoutée à la classe I ou à la classe II ou est déplacée de la classe I à la classe II, figurant à l'annexe III, avant que les procédures d'évaluation de la conformité pertinentes visées à l'article 32, paragraphes 2 et 3, ne deviennent d'application, à moins que des raisons d'urgence impérieuse ne justifient une période transitoire plus courte.

4. Au plus tard le ... [*12 mois à compter de la date d'entrée en vigueur du présent règlement*], la Commission adopte un acte d'exécution précisant la description technique des catégories de produits comportant des éléments numériques qui relèvent des classes I et II figurant à l'annexe III, ainsi que la description technique des catégories de produits comportant des éléments numériques qui figurent à l'annexe IV. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 8

Produits critiques comportant des éléments numériques

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour compléter le présent règlement afin de déterminer quels produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produits qui figure à l'annexe IV du présent règlement doivent être tenus d'obtenir un certificat de cybersécurité européen au minimum au niveau d'assurance dit "substantiel" dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu du règlement (UE) 2019/881, afin de démontrer leur conformité aux exigences essentielles de cybersécurité énoncées à l'annexe I du présent règlement, ou à des parties de ces exigences, à condition qu'un schéma européen de certification de cybersécurité qui couvre ces catégories de produits comportant des éléments numériques ait été adopté en vertu du règlement (UE) 2019/881 et soit à la disposition des fabricants. Ces actes délégués précisent le niveau d'assurance nécessaire qui est proportionné au niveau de risque de cybersécurité associé aux produits comportant des éléments numériques et ils tiennent compte de l'utilisation prévue de ces produits, y compris la dépendance critique à leur égard d'entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555.

   Avant d'adopter ces actes délégués, la Commission procède à une évaluation des effets potentiels sur le marché des mesures envisagées, ainsi qu'à des consultations des parties intéressées, y compris le groupe européen de certification de cybersécurité institué au titre du règlement (UE) 2019/881. L'évaluation prend en considération l'état de préparation et le niveau des capacités des États membres pour la mise en œuvre du schéma européen de certification de cybersécurité pertinent. Lorsqu'aucun acte délégué tel que visé au premier alinéa du présent paragraphe n'a été adopté, les produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produits qui figure à l'annexe IV sont soumis aux procédures d'évaluation de la conformité visées à l'article 32, paragraphe 3.

Les actes délégués visés au premier alinéa prévoient une période transitoire d'au moins six mois, à moins que des raisons d'urgence impérieuse ne justifient une période transitoire plus courte.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour modifier l'annexe IV en ajoutant ou en retirant des catégories de produits critiques comportant des éléments numériques. Lorsqu'elle fixe ces catégories de produits critiques comportant des éléments numériques et le niveau d'assurance requis, conformément au paragraphe 1 du présent article, la Commission tient compte des critères visés à l'article 7, paragraphe 2, et veille à ce que les catégories de produits critiques comportant des éléments numériques remplissent au moins l'un des critères suivants:

a) il existe une dépendance critique d'entités essentielles visées à l'article 3 de la directive (UE) 2022/2555 à l'égard de la catégorie de produits comportant des éléments numériques;

b) des incidents et des vulnérabilités exploitées concernant la catégorie de produits comportant des éléments numériques pourrait entraîner de graves perturbations de chaînes d'approvisionnement critiques du marché intérieur.

Avant d'adopter ces actes délégués, la Commission procède à une évaluation du même type que celle visée au paragraphe 1.

Les actes délégués visés au premier alinéa prévoient une période transitoire d'au moins six mois, à moins que des raisons d'urgence impérieuse ne justifient une période transitoire plus courte.

Article 9

Consultation des parties intéressées

1. Lors de l'élaboration des mesures de mise en œuvre du présent règlement, la Commission consulte les parties intéressées, telles que les autorités des États membres concernées, les entreprises du secteur privé, y compris les microentreprises et les petites et moyennes entreprises, la communauté des logiciels ouverts, les associations de consommateurs, le milieu universitaire et les organismes et organes compétents de l'Union, ainsi que les groupes d'experts établis au niveau de l'Union. En particulier, la Commission consulte ces parties intéressées et sollicite leur avis, de manière structurée, lorsque cela s'y prête:

   a) au moment d'élaborer les orientations visées à l'article 26;

   b) au moment de préparer les descriptions techniques spécifiques des catégories de produits figurant à l'annexe III conformément à l'article 7, paragraphe 4, d'évaluer la nécessité d'éventuelles mises à jour de la liste des catégories de produits conformément à l'article 7, paragraphe 3, et à l'article 8, paragraphe 2, ou de procéder à l'évaluation des effets potentiels sur le marché visée à l'article 8, paragraphe 1, sans préjudice de l'article 61;

   c) au moment d'entreprendre des travaux préparatoires en vue de l'évaluation et du réexamen du présent règlement.

2. La Commission organise régulièrement des sessions de consultation et d'information, et au moins une fois par an, afin de recueillir l'avis des parties intéressées visées au paragraphe 1 sur la mise en œuvre du présent règlement.

Article 10

Renforcement des compétences dans un environnement numérique cyberrésilient

Aux fins du présent règlement et afin de répondre aux besoins des professionnels à l'appui de la mise en œuvre du présent règlement, les États membres, avec, le cas échéant, le soutien de la Commission, du Centre européen de compétences en matière de cybersécurité et de l'ENISA, tout en respectant pleinement la responsabilité des États membres dans le domaine de l'éducation, favorisent des mesures et des stratégies visant:

a) à développer des compétences en matière de cybersécurité et à créer des outils organisationnels et technologiques pour garantir une disponibilité suffisante de professionnels qualifiés afin de soutenir les activités des autorités de surveillance du marché et des organismes d'évaluation de la conformité;

b) à renforcer la collaboration entre le secteur privé, les opérateurs économiques, y compris par la reconversion ou le perfectionnement des salariés des fabricants, les consommateurs, les prestataires de formation et les administrations publiques, élargissant ainsi les possibilités pour les jeunes d'accéder à des emplois dans le secteur de la cybersécurité.

Article 11

Sécurité générale des produits

Par dérogation à l'article 2, paragraphe 1, troisième alinéa, point b), du règlement (UE) 2023/988, le chapitre III, section 1, les chapitres V et VII, et les chapitres IX à XI dudit règlement s'appliquent aux produits comportant des éléments numériques en ce qui concerne les aspects et les risques ou catégories de risques qui ne sont pas couverts par le présent règlement lorsque ces produits 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 27), du règlement (UE) 2023/988.

Article 12

Systèmes d'IA à haut risque

1. Sans préjudice des exigences en matière d'exactitude et de robustesse énoncées à l'article 15 du règlement (UE) 2024/1689, les produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement et sont classés comme des systèmes d'IA à haut risque conformément à l'article 6 dudit règlement sont réputés conformes aux exigences de cybersécurité énoncées à l'article 15 dudit règlement:

   a) lorsque ces produits satisfont aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I;

b) lorsque les processus mis en place par le fabricant sont conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II; et

c) lorsque le niveau de cyberprotection requis à l'article 15 du règlement (UE) 2024/1689 est démontré par la déclaration UE de conformité délivrée en vertu du présent règlement.

2. Pour les produits comportant des éléments numériques et les exigences de cybersécurité visés au paragraphe 1 du présent article, la procédure d'évaluation de la conformité pertinente prévue à l'article 43 du règlement (UE) 2024/1689 s'applique. Aux fins de cette évaluation, les organismes notifiés qui sont compétents pour contrôler la conformité des systèmes d'IA à haut risque au titre du règlement (UE) 2024/1689 sont également compétents pour contrôler la conformité des systèmes d'IA à haut risque qui relèvent du 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 prévues par l'article 39 du présent règlement ait été évaluée dans le cadre de la procédure de notification prévue par le règlement (UE) 2024/1689.

3. Par dérogation au paragraphe 2 du présent article, les produits importants comportant des éléments numériques énumérés à l'annexe III du présent règlement, qui font l'objet des procédures d'évaluation de la conformité prévues par l'article 32, paragraphe 2, points a) et b), et l'article 32, paragraphe 3, du présent règlement ainsi que les produits critiques comportant des éléments numériques énumérés à l'annexe V du présent règlement qui doivent obtenir un certificat de cybersécurité européen au titre de l'article 8, paragraphe 1, du présent règlement ou, à défaut, qui font l'objet des procédures d'évaluation de la conformité prévues par l'article 32, paragraphe 3, du présent règlement, et qui sont également classés comme systèmes d'IA à haut risque au titre de l'article 6 du règlement (UE) 2024/1689, et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne prévue à l'annexe VI du règlement (UE) 2024/1689, sont soumis aux procédures d'évaluation de la conformité prévues par le présent règlement en ce qui concerne les exigences essentielles de cybersécurité énoncées dans le présent règlement.

4. Les fabricants de produits comportant des éléments numériques visés au paragraphe 1 du présent article peuvent participer aux sas réglementaires en matière d'IA visés à l'article 57 du règlement (UE) 2024/1689.

Chapitre II
Obligations des opérateurs économiques et dispositions relatives aux logiciels libres et ouverts

Article 13

Obligations incombant aux fabricants

1. Lorsqu'ils mettent sur le marché un produit comportant des éléments numériques, les fabricants s'assurent que ce produit a été conçu, développé et fabriqué conformément aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I.

2. Aux fins du respect du paragraphe 1, les fabricants procèdent à une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques et tiennent 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 et d'en réduire au minimum leurs répercussions, y compris en ce qui concerne la santé et la sécurité des utilisateurs.

3. L'évaluation des risques de cybersécurité est documentée et mise à jour selon les besoins au cours d'une période d'assistance à déterminer conformément au paragraphe 8 du présent article. Cette évaluation des risques de cybersécurité comprend au moins une analyse des risques de cybersécurité fondée sur l'utilisation prévue et l'utilisation raisonnablement prévisible, ainsi que sur les conditions d'utilisation du produit comportant des éléments numériques, tels que l'environnement opérationnel ou les actifs à protéger, compte tenu de la durée prévue d'utilisation du produit. L'évaluation des risques de cybersécurité indique si et, dans l'affirmative, de quelle manière, les exigences de sécurité énoncées à l'annexe I, partie I, point 2), sont applicables au produit comportant des éléments numériques concerné et comment ces exigences sont mises en œuvre sur la base de l'évaluation du risque de cybersécurité. Elle indique également de quelle manière le fabricant doit appliquer l'annexe I, partie I, point 1), ainsi que les exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II.

4. Lorsqu'il met sur le marché un produit comportant des éléments numériques, le fabricant inclut l'évaluation des risques de cybersécurité visée au paragraphe 3 du présent article dans la documentation technique requise conformément à l'article 31 et à l'annexe V. Pour les produits comportant des éléments numériques mentionnés à l'article 12, qui relèvent aussi d'autres actes juridiques de l'Union, l'évaluation des risques de cybersécurité peut faire partie de l'évaluation des risques prévue par ces actes juridiques de l'Union. Lorsque certaines exigences essentielles de cybersécurité ne sont pas applicables au produit comportant des éléments numériques commercialisé, le fabricant fait figurer une justification claire dans cette documentation technique.

5. Aux fins du respect de l'obligation énoncée au paragraphe 1, les fabricants font preuve de diligence raisonnable lorsqu'ils intègrent dans des produits comportant des éléments numériques des composants obtenus auprès de tiers, de sorte que ces composants ne compromettent pas la cybersécurité du produit comportant des éléments numériques, y compris lors de l'intégration de composants de logiciels libres et ouverts qui n'ont pas été mis à disposition sur le marché dans le cadre d'une activité commerciale.

6. Lorsqu'ils identifient une vulnérabilité dans un composant, y compris un composant logiciel ouvert, qui est intégré au produit comportant des éléments numériques, les fabricants signalent la vulnérabilité à la personne ou à l'entité qui assure la maintenance du composant, et s'attaquent et remédient à la vulnérabilité conformément aux exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II. Lorsque les fabricants ont mis au point une modification logicielle ou matérielle pour remédier à la vulnérabilité de ce composant, ils partagent le code ou la documentation correspondants avec la personne ou l'entité qui fabrique le composant ou en assure la maintenance, dans un format lisible par machine s'il y a lieu.

7. Les fabricants documentent 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 ils prennent connaissance et toute information pertinente fournie par des tiers, et, le cas échéant, mettent à jour l'évaluation des risques de cybersécurité du produit.

8. Lorsqu'ils mettent sur le marché un produit comportant des éléments numériques, et pendant la période d'assistance, les fabricants veillent à ce que les vulnérabilités de ce produit, y compris de ses composants, soient gérées efficacement et conformément aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II.

Les fabricants fixent la période d'assistance de sorte qu'elle reflète la durée pendant laquelle le produit est censé pouvoir être utilisé, en tenant compte, en particulier, des attentes raisonnables des utilisateurs, de la nature du produit, y compris de son utilisation prévue, ainsi que du droit de l'Union applicable déterminant la durée de vie des produits comportant des éléments numériques. Lorsqu'ils déterminent la période d'assistance, les fabricants peuvent également tenir compte des périodes d'assistance des produits comportant des éléments numériques offrant une fonctionnalité similaire mis sur le marché par d'autres fabricants, de la disponibilité de l'environnement opérationnel, des périodes d'assistance des composants intégrés qui assurent des fonctions essentielles et proviennent de tiers, ainsi que des orientations pertinentes fournies par le groupe de coopération administrative (ADCO) institué en vertu de l'article 52, paragraphe 15, et par la Commission. Les éléments à prendre en compte pour définir la période d'assistance sont pris en compte de manière à garantir la proportionnalité.

Sans préjudice du deuxième alinéa, la période d'assistance est d'au moins cinq ans. Lorsque le produit comportant des éléments numériques est censé pouvoir être utilisé pendant moins de cinq ans, la période d'assistance correspond à la durée d'utilisation prévue.

Compte tenu des recommandations ADCO visées à l'article 52, paragraphe 16, la Commission peut adopter des actes délégués conformément à l'article 61 afin de compléter le présent règlement en précisant la période d'assistance minimale pour des catégories de produits spécifiques lorsque les données de surveillance du marché indiquent que les périodes d'assistance fixées sont insuffisantes.

Les fabricants font figurer dans la documentation technique visée à l'annexe VII les informations qui ont été prises en compte pour déterminer la période d'assistance du produit comportant des éléments numériques.

Les fabricants disposent de politiques et de procédures appropriées, notamment les politiques de divulgation coordonnée des vulnérabilités mentionnées à l'annexe I, partie II, point 5), pour traiter et corriger les vulnérabilités potentielles du produit comportant des éléments numériques signalées par des sources internes ou externes.

9. Les fabricants veillent à ce que chaque mise à jour de sécurité, visée à l'annexe I, partie II, point 8), qui a été mise à la disposition des utilisateurs au cours de la période d'assistance, reste disponible après son émission pendant dix ans au minimum ou pendant le reste de la période d'assistance, la période la plus longue étant retenue.

10. Lorsqu'un fabricant met sur le marché des versions ultérieures substantiellement modifiées d'un logiciel, il peut garantir la conformité avec l'exigence essentielle de cybersécurité énoncée à l'annexe I, partie II, point 2), uniquement pour la dernière version mise sur le marché, à condition que les utilisateurs des versions précédemment mises sur le marché aient accès gratuitement aux dernières versions mises sur le marché et ne doivent pas supporter des coûts supplémentaires pour adapter l'environnement matériel et logiciel dans lequel ils utilisent la version originale de ce produit.

11. Les fabricants peuvent conserver des archives logicielles publiques améliorant l'accès des utilisateurs aux versions antérieures. Dans ces cas, les utilisateurs sont clairement informés, d'une manière aisément accessible, des risques associés à l'utilisation de logiciels non pris en charge.

12. Avant de mettre sur le marché un produit comportant des éléments numériques, les fabricants établissent la documentation technique visée à l'article 31.

    Il applique ou fait appliquer les procédures d'évaluation de la conformité choisies visées à l'article 32.

    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 de cybersécurité énoncées à l'annexe I, partie I, et que les processus mis en place par le fabricant sont conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II, les fabricants établissent la déclaration UE de conformité conformément à l'article 28 et appose le marquage CE conformément à l'article 30.

13. Les fabricants tiennent la documentation technique et la déclaration UE de conformité à la disposition des autorités de surveillance du marché pendant une durée d'au moins dix ans après la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la période la plus longue étant retenue.

14. Les fabricants veillent à ce que des procédures soient en place pour que la conformité avec le présent règlement des produits comportant des éléments numériques produits en série reste assurée. Les fabricants tiennent 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 27 au regard desquelles la conformité du produit comportant des éléments numériques est déclarée ou en application desquelles sa conformité est vérifiée.

15. Les fabricants veillent à ce que leurs produits comportant des éléments numériques portent un numéro de type, de lot ou de série ou tout autre élément permettant leur identification ou, lorsque cela n'est pas possible, à ce que cette information soit fournie sur l'emballage ou dans un document accompagnant le produit comportant des éléments numériques.

16. Le fabricant indique son nom, sa raison sociale ou sa marque déposée et ses adresses postale, électronique ou autre moyen numérique, ainsi que, le cas échéant, l'adresse du site internet, auxquelles il peut être contacté sur le produit comportant des éléments numériques, sur son emballage ou dans un document l'accompagnant. Ces informations figurent également dans les informations et instructions destinées à l'utilisateur énoncées à l'annexe II. Les coordonnées sont indiquées dans une langue aisément compréhensible par les utilisateurs et les autorités de surveillance du marché.

17. Aux fins du présent règlement, les fabricants désignent un point de contact unique pour permettre aux utilisateurs de communiquer directement et rapidement avec lui, y compris afin de faciliter le signalement des vulnérabilités des produits comportant des éléments numériques.

Les fabricants veillent à ce que le point de contact unique soit facilement identifiable par les utilisateurs. Ils font également figurer le point de contact unique dans les informations et instructions destinées à l'utilisateur énoncées à l'annexe II.

Le point de contact unique permet aux utilisateurs de choisir leurs moyens de communication préférés, ces moyens n'étant pas limités aux outils automatisés.

18. Les fabricants veillent à ce que les produits comportant des éléments numériques soient accompagnés des informations et des instructions destinées à l'utilisateur énoncées à l'annexe II, sous forme papier ou électronique. Ces informations et instructions sont fournies dans une langue aisément compréhensible par les utilisateurs et les autorités de surveillance du marché. Elles sont claires, compréhensibles, intelligibles et lisibles. Elles permettent une installation, un fonctionnement et une utilisation sécurisés des produits comportant des éléments numériques. Les fabricants tiennent les informations et instructions destinées à l'utilisateur énoncées à l'annexe II à la disposition des utilisateurs et des autorités de surveillance du marché pendant une durée d'au moins dix ans après la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la période la plus longue étant retenue. Lorsque ces informations et instructions sont fournies en ligne, les fabricants veillent à ce qu'elles soient accessibles, faciles d'utilisation et disponibles en ligne pendant une durée d'au moins dix ans après la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la période la plus longue étant retenue.

19. Les fabricants veillent à ce que la date de fin de la période d'assistance visée au paragraphe 8, y compris au moins le mois et l'année, soit précisée au moment de l'achat, d'une manière claire, compréhensible et aisément accessible et, le cas échéant, sur le produit comportant des éléments numériques, son emballage ou par des moyens numériques.

Lorsque cela est techniquement possible compte tenu de la nature du produit comportant des éléments numériques, les fabricants prévoient l'affichage d'une notification aux utilisateurs les informant que leur produit comportant des éléments numériques a atteint la fin de sa période d'assistance.

20. Les fabricants fournissent soit une copie de la déclaration UE de conformité, soit une déclaration UE de conformité simplifiée avec le produit comportant des éléments numériques. Dans le cas où une déclaration UE de conformité simplifiée est jointe, celle-ci contient l'adresse internet exacte à laquelle le texte complet de la déclaration UE de conformité est accessible.

21. Dès la mise sur le marché et pendant la période d'assistance, les fabricants qui considèrent ou ont 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 de cybersécurité énoncées à l'annexe I prennent 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.

22. Sur requête motivée d'une autorité de surveillance du marché, les fabricants communiquent à cette dernière, dans une langue aisément compréhensible par cette autorité, 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 de cybersécurité énoncées à l'annexe I. Les fabricants coopèrent 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'ils ont mis sur le marché.

23. Un fabricant qui cesse ses activités et qui, de ce fait, n'est pas en mesure de se conformer au présent règlement informe, avant que cette cessation ne prenne effet, les autorités de surveillance du marché concernées, 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 de la cessation imminente de ses activités.

24. La Commission peut, par voie d'actes d'exécution tenant compte des normes et bonnes pratiques européennes et internationales, préciser le format et les éléments de la nomenclature des logiciels visée à l'annexe I, partie II, point 1). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

25. Afin d'évaluer la dépendance des États membres et de l'Union dans son ensemble à l'égard des composants logiciels, et en particulier des composants qui répondent aux critères de logiciels libres et ouverts, l'ADCO peut décider de procéder à une évaluation de la dépendance à l'échelle de l'Union pour des catégories spécifiques de produits comportant des éléments numériques. À cette fin, les autorités de surveillance du marché peuvent demander aux fabricants de ces catégories de produits comportant des éléments numériques de fournir les nomenclatures des logiciels pertinentes du matériel visées à l'annexe I, partie II, point 1). Sur la base de ces informations, les autorités de surveillance du marché peuvent fournir à l'ADCO des informations anonymisées et agrégées sur les dépendances logicielles. L'ADCO soumet un rapport sur les résultats de l'évaluation de la dépendance au groupe de coopération institué en vertu de l'article 14 de la directive (UE) 2022/2555.

Article 14

Obligations en matière de communication d'informations incombant aux fabricants

1. Un fabricant notifie toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques dont il prend connaissance simultanément au CSIRT désigné comme coordinateur conformément au paragraphe 7 du présent article, et à l'ENISA. Le fabricant notifie cette vulnérabilité activement exploitée par l'intermédiaire de la plateforme unique de signalement établie en vertu de l'article 16.

2. Aux fins de la notification visée au paragraphe 1, le fabricant soumet:

   a) une alerte précoce de vulnérabilité activement exploitée, sans retard injustifié et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance, en indiquant, le cas échéant, les États membres sur le territoire desquels il a connaissance que son produit comportant des éléments numériques a été mis à disposition;

b) à moins que les informations pertinentes n'aient déjà été communiquées, une notification de vulnérabilité, sans retard injustifié et, en tout état de cause, au plus tard 72 heures après avoir eu connaissance de la vulnérabilité activement exploitée, fournissant les informations générales disponibles sur le produit comportant des éléments numériques concerné, la nature générale de l'exploitation et de la vulnérabilité concernée, ainsi que toute mesure corrective ou d'atténuation prise et les mesures correctives ou d'atténuation que les utilisateurs peuvent prendre, et précisant, s'il y a lieu, le degré de sensibilité qu'il attribue aux informations notifiées;

c) à moins que les informations pertinentes n'aient déjà été communiquées, un rapport final, au plus tard 14 jours après la mise à disposition d'une mesure de correction ou d'atténuation, comprenant au moins les éléments suivants:

   i) une description de la vulnérabilité, y compris de sa gravité et de ses répercussions;

   ii) le cas échéant, des informations concernant tout acteur malveillant ayant exploité ou exploitant la vulnérabilité;

   iii) des précisions concernant la mise à jour de sécurité ou les autres mesures correctives qui ont été mises en place pour remédier à la vulnérabilité.

3. Un fabricant notifie tout incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques dont il prend connaissance simultanément au CSIRT désigné comme coordinateur conformément au paragraphe 7 du présent article et à l'ENISA. Le fabricant notifie cet incident par l'intermédiaire de la plateforme unique de signalement établie en vertu de l'article 16.

4. Aux fins de la notification visée au paragraphe 3, le fabricant soumet:

a) une alerte précoce d'incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques, sans retard injustifié et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance, indiquant, au minimum, si l'incident pourrait avoir été causé par des actes illicites ou malveillants et, le cas échéant, les États membres sur le territoire desquels il a connaissance que son produit comportant des éléments numériques a été mis à disposition;

b) à moins que les informations pertinentes n'aient déjà été communiquées, une notification d'incident, sans retard injustifié et, en tout état de cause, au plus tard 72 heures après avoir eu connaissance de l'incident, fournissant les informations générales, lorsqu'elles sont disponibles, sur la nature de l'incident, l'évaluation initiale de l'incident, ainsi que toute mesure corrective ou d'atténuation prise et les mesures correctives ou d'atténuation que les utilisateurs peuvent prendre, et précisant, le cas échéant, le degré de sensibilité qu'il attribue aux informations notifiées;

c) à moins que les informations pertinentes n'aient déjà été communiquées, dans un délai d'un mois à compter de la présentation de la notification d'incident visée au point b), un rapport final comprenant au moins les éléments suivants:

i) une description détaillée de l'incident, y compris de sa gravité et de ses répercussions;

ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

iii) les mesures d'atténuation appliquées et en cours.

5. Aux fins du paragraphe 3, un incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques est considéré comme grave lorsque:

a) il entache ou est susceptible d'entacher la capacité d'un produit comportant des éléments numériques à protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données ou fonctions sensibles ou importantes; ou

b) il a conduit ou est susceptible de conduire à l'introduction ou à l'exécution d'un code malveillant dans un produit comportant des éléments numériques ou dans le réseau et les systèmes d'information d'un utilisateur du produit comportant des éléments numériques.

6. Si nécessaire, le CSIRT désigné comme coordinateur qui reçoit initialement la notification peut demander au fabricant de fournir un rapport intermédiaire de situation concernant la vulnérabilité activement exploitée ou l'incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques.

7. Les notifications visées aux paragraphes 1 et 3 du présent article sont soumises par l'intermédiaire de la plateforme unique de signalement visée à l'article 16 en utilisant l'un des points finaux de notification électronique visés à l'article 16, paragraphe 1. La notification est soumise au moyen du point final de notification électronique du CSIRT désigné comme coordinateur de l'État membre dans lequel le fabricant a son établissement principal dans l'Union et est simultanément mise à la disposition de l'ENISA.

Aux fins du présent règlement, un fabricant est réputé avoir son établissement principal dans l'Union dans l'État membre où sont principalement prises les décisions relatives à la cybersécurité des produits comportant des éléments numériques. Si un tel État membre ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre où le fabricant concerné possède l'établissement comptant le plus grand nombre de salariés dans l'Union.

Lorsqu'un fabricant n'a pas d'établissement principal dans l'Union, il soumet les notifications visées aux paragraphes 1 et 3 en utilisant le point final de notification électronique du CSIRT désigné comme coordinateur dans l'État membre déterminé conformément à l'ordre suivant, selon les informations dont dispose le fabricant:

a) l'État membre dans lequel le mandataire agissant au nom du fabricant pour le plus grand nombre de produits comportant des éléments numériques de ce fabricant est établi;

b) l'État membre dans lequel l'importateur qui met sur le marché le plus grand nombre de produits comportant des éléments numériques de ce fabricant est établi;

c) l'État membre dans lequel le distributeur qui met à disposition sur le marché le plus grand nombre de produits comportant des éléments numériques de ce fabricant est établi;

d) l'État membre dans lequel se trouvent le plus grand nombre d'utilisateurs de produits comportant des éléments numériques de ce fabricant.

En ce qui concerne le troisième alinéa, point d), un fabricant peut soumettre des notifications relatives à tout nouveau cas de vulnérabilité activement exploitée ou d'incident grave ayant un impact sur la sécurité du produit comportant des éléments numériques au même CSIRT désigné comme coordinateur que celui avec lequel il a communiqué la première fois.

8. Après avoir pris connaissance d'une vulnérabilité activement exploitée ou d'un incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques, le fabricant informe les utilisateurs du produit comportant des éléments numériques touchés et, s'il y a lieu, tous les utilisateurs de ladite vulnérabilité ou dudit incident et, si nécessaire, de toute mesure corrective ou d'atténuation des risques que les utilisateurs peuvent mettre en place pour atténuer les répercussions de cette vulnérabilité ou de cet incident, s'il y a lieu dans un format structuré, lisible par machine pouvant être facilement traité automatiquement. Lorsque le fabricant n'informe pas les utilisateurs du produit comportant des éléments numériques en temps utile, les CSIRT notifiés désignés comme coordinateurs peuvent fournir ces informations aux utilisateurs lorsqu'ils le jugent proportionné et nécessaire pour prévenir ou atténuer les répercussions de cette vulnérabilité ou de cet incident.

9. Au plus tard le ... [*12 mois à compter de la date d'entrée en vigueur du présent règlement*], la Commission adopte des actes délégués conformément à l'article 61 du présent règlement pour compléter le présent règlement en précisant les conditions d'application des motifs ayant trait à la cybersécurité en lien avec les retards de diffusion des notifications prévus à l'article 16, paragraphe 2, du présent règlement. La Commission coopère avec le réseau des CSIRT établi en vertu de l'article 15 de la directive (UE) 2022/2555 et l'ENISA pour préparer les projets d'actes délégués.

10. La Commission peut, par voie d'actes d'exécution, préciser plus en détail le format et les procédures des notifications visées au présent article ainsi qu'aux articles 15 et 16. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2. La Commission coopère avec le réseau des CSIRT et l'ENISA pour préparer les projets d'actes d'exécution.

Article 15

Signalement volontaire

1. Les fabricants mais aussi d'autres personnes physiques ou morales peuvent notifier toute vulnérabilité contenue dans un produit comportant des éléments numériques ainsi que les cybermenaces susceptibles d'affecter le profil de risque d'un produit comportant des éléments numériques, de manière volontaire, à un CSIRT désigné comme coordinateur ou à l'ENISA.

2. Les fabricants ainsi que d'autres personnes physiques ou morales peuvent notifier tout incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques ainsi que des incidents évités qui auraient pu entraîner un tel incident, de manière volontaire, à un CSIRT désigné comme coordinateur ou à l'ENISA.

3. Le CSIRT désigné comme coordinateur ou l'ENISA traite les notifications visées au paragraphes 1 et 2 du présent article conformément à la procédure prévue à l'article 16.

   Le CSIRT désigné comme coordinateur peut accorder la priorité au traitement des notifications obligatoires par rapport aux notifications volontaires.

4. Lorsqu'une personne physique ou morale autre que le fabricant notifie une vulnérabilité activement exploitée ou un incident grave ayant des répercussions sur la sécurité d'un produit comportant des éléments numériques conformément au paragraphe 1 ou 2, le CSIRT désigné comme coordinateur en informe le fabricant sans retard injustifié.

5. Les CSIRT désignés comme coordinateurs ainsi que l'ENISA garantissent la confidentialité et une protection appropriée des informations fournies par la personne physique ou morale à l'origine de la notification. Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet d'imposer à la personne physique ou morale à l'origine de la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas fait la notification.

Article 16

Mise en place d'une plateforme unique de signalement

1. Aux fins des notifications visées à l'article 14, paragraphes 1 et 3, et à l'article 15, paragraphes 1 et 2, et afin de simplifier les obligations de signalement des fabricants, l'ENISA met en place une plateforme unique de signalement. Les opérations quotidiennes de la plateforme unique de signalement sont administrées par l'ENISA, qui en assure le fonctionnement. L'architecture de la plateforme unique de signalement permet aux États membres et à l'ENISA de mettre en place leurs propres points finaux de notification électronique.

2. Après réception d'une notification, le CSIRT désigné comme coordinateur qui reçoit initialement la notification diffuse, sans retard, la notification via la plateforme unique de signalement aux CSIRT désignés comme coordinateurs sur le territoire desquels le fabricant a indiqué que le produit comportant des éléments numériques a été mis à disposition.

Dans des circonstances exceptionnelles et, en particulier, à la demande du fabricant et compte tenu du degré de sensibilité des informations notifiées indiqué par celui-ci en vertu de l'article 14, paragraphe 2, point a), du présent règlement, la diffusion de la notification peut être retardée pour des motifs justifiés ayant trait à la cybersécurité pour une période limitée à ce qui est strictement nécessaire, y compris lorsqu'une vulnérabilité fait l'objet d'une procédure de divulgation coordonnée des vulnérabilités au titre de l'article 12, paragraphe 1, de la directive (UE) 2022/2555. Lorsqu'un CSIRT décide de retarder la diffusion d'une notification, il en informe immédiatement l'ENISA et fournit à la fois une justification du report de la diffusion de la notification et une indication de la date à laquelle il diffusera la notification conformément à la procédure de diffusion prévue au présent paragraphe. L'ENISA peut soutenir le CSIRT pour l'application de motifs ayant trait à la cybersécurité en ce qui concerne le report de la diffusion de la notification.

Dans des circonstances particulièrement exceptionnelles, lorsque le fabricant indique, dans la notification visée à l'article 14, paragraphe 2, point b):

a) que la vulnérabilité notifiée a été activement exploitée par un acteur malveillant et que, selon les informations disponibles, elle n'a été exploitée dans aucun autre État membre que celui du CSIRT désigné comme coordinateur auquel le fabricant a notifié la vulnérabilité;

b) que toute diffusion ultérieure immédiate de la vulnérabilité notifiée entraînerait probablement la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels de cet État membre; ou

c) que la vulnérabilité notifiée présente un risque de cybersécurité imminent élevé en cas de poursuite de la diffusion.

Seules l'information qu'une notification a été effectuée par le fabricant, les informations générales sur le produit, les informations sur la nature générale de l'exploitation et les informations indiquant que des motifs ayant trait à la sécurité ont été soulevés sont mises simultanément à la disposition de l'ENISA jusqu'à ce que la notification complète soit diffusée aux CSIRT concernés et à l'ENISA. Lorsque, sur la base de ces informations, l'ENISA considère qu'il existe un risque systémique compromettant la sécurité du marché intérieur, elle recommande au CSIRT destinataire de diffuser la notification complète aux autres CSIRT désignés comme coordinateurs et à elle-même.

3. Après avoir reçu notification d'une vulnérabilité activement exploitée d'un produit comportant des éléments numériques ou d'un incident grave ayant des répercussions sur la sécurité d'un produit comportant des éléments numériques, les CSIRT désignés comme coordinateurs fournissent aux autorités de surveillance du marché de leurs États membres respectifs les informations notifiées dont elles ont besoin pour s'acquitter des obligations qui leur incombent en vertu du présent règlement.

4. L'ENISA prend des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques pesant sur la sécurité de la plateforme unique de signalement et des informations soumises ou diffusées par l'intermédiaire de cette plateforme. Elle notifie sans retard injustifié tout incident de sécurité affectant la plateforme unique de signalement au réseau des CSIRT ainsi qu'à la Commission.

5. L'ENISA, en coopération avec le réseau des CSIRT, fournit et met en œuvre des spécifications pour les mesures techniques, opérationnelles et organisationnelles relatives à la mise en place, à la maintenance et au fonctionnement sécurisé de la plateforme unique de signalement visée au paragraphe 1, comprenant au moins les dispositions de sécurité liées à la mise en place, au fonctionnement et à la maintenance de la plateforme unique de signalement, ainsi que les points finaux de notification électronique mis en place par les CSIRT désignés comme coordinateurs au niveau national et par l'ENISA au niveau de l'Union, y compris les aspects procéduraux visant à garantir que, lorsqu'une vulnérabilité notifiée ne comporte pas de mesures correctives ou d'atténuation des risques, les informations relatives à cette vulnérabilité sont partagées conformément à des protocoles de sécurité stricts et sur la base du besoin d'en connaître.

6. Lorsqu'un CSIRT désigné comme coordinateur a été informé d'une vulnérabilité activement exploitée dans le cadre d'une procédure de divulgation coordonnée des vulnérabilités visée à l'article 12, paragraphe 1, de la directive (UE) 2022/2555, le CSIRT désigné comme coordinateur qui reçoit initialement la notification peut retarder la diffusion de la notification en question par l'intermédiaire de la plateforme unique de signalement pour des motifs justifiés ayant trait à la cybersécurité pour une période limitée à ce qui est strictement nécessaire et jusqu'à ce que les parties à la divulgation coordonnée des vulnérabilités concernées aient donné leur consentement. Cette exigence n'empêche pas les fabricants de notifier une telle vulnérabilité de manière volontaire conformément à la procédure prévue au présent article.

Article 17

Autres dispositions liées au signalement

1. L'ENISA peut soumettre au réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE – CyCLONe) institué par l'article 16 de la directive (UE) 2022/2555 les informations notifiées conformément à l'article 14, paragraphes 1 et 3, et à l'article 15, paragraphes 1 et 2, du présent règlement, si elles sont pertinentes pour la gestion coordonnée au niveau opérationnel des incidents et crises de cybersécurité majeurs. Afin de déterminer cette pertinence, l'ENISA peut prendre en considération les analyses techniques effectuées par le réseau des CSIRT, lorsqu'elles existent.

2. Lorsque la sensibilisation du public est nécessaire pour prévenir ou atténuer un incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques ou pour traiter un incident en cours, ou lorsque la divulgation de l'incident est par ailleurs dans l'intérêt public, le CSIRT désigné comme coordinateur de l'État membre concerné peut, après consultation du fabricant concerné et, le cas échéant, en coopération avec l'ENISA, informer le public de l'incident ou exiger du fabricant qu'il le fasse.

3. Sur la base des notifications reçues conformément à l'article 14, paragraphes 1 et 3, et à l'article 15, paragraphes 1 et 2, du présent règlement, l'ENISA élabore tous les 24 mois un rapport technique 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 institué en vertu de l'article 14 de la directive (UE) 2022/2555. Le premier rapport de ce type est présenté dans les 24 mois suivant le début de l'application des obligations prévues à l'article 14, paragraphes 1 et 3. L'ENISA inclut les informations pertinentes de ses rapports techniques dans son rapport sur l'état de la cybersécurité dans l'Union établi conformément à l'article 18 de la directive (UE) 2022/2555.

4. Le simple acte de notification conformément à l'article 14, paragraphes 1 et 3, ou à l'article 15, paragraphes 1 et 2, ne soumet pas la personne physique ou morale à l'origine de la notification à une responsabilité accrue.

5. Après qu'une mise à jour de sécurité ou une autre forme de mesure corrective ou d'atténuation est mise à disposition, l'ENISA ajoute, en accord avec le fabricant du produit comportant des éléments numériques concerné, la vulnérabilité connue du public notifiée conformément à l'article 14, paragraphe 1, ou à l'article 15, paragraphe 1, du présent règlement à la base de données européenne des vulnérabilités établie en vertu de l'article 12, paragraphe 2, de la directive (UE) 2022/2555.

6. Les CSIRT désignés comme coordinateurs fournissent aux fabricants, et en particulier aux fabricants qui peuvent être considérés comme des microentreprises ou des petites ou moyennes entreprises, un service d'assistance en ce qui concerne les obligations de signalement énoncées à l'article 14.

Article 18

Mandataires

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

2. Les obligations énoncées à l'article 13, paragraphes 1 à 11, à l'article 13, paragraphe 12, premier alinéa, et à l'article 13, paragraphe 14, 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 mandataire fournit une copie du mandat aux autorités de surveillance du marché à leur demande. 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 28 et la documentation technique mentionnée à l'article 31 pendant au moins dix ans à partir de la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la période la plus longue étant retenue;

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 19

Obligations incombant aux importateurs

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

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 visées à l'article 32 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 visé à l'article 30 et soit accompagné de la déclaration UE de conformité visée à l'article 13, paragraphe 20, ainsi que des informations et instructions destinées à l'utilisateur figurant à l'annexe II, rédigées dans une langue aisément compréhensible par les utilisateurs et les autorités de surveillance du marché;

   d) le fabricant ait respecté les exigences prévues à l'article 13, paragraphes 15, 16 et 19.

   Aux fins du présent paragraphe, les importateurs doivent être en mesure de fournir les documents nécessaires prouvant le respect des exigences énoncées dans le présent article.

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 au présent règlement, 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 le présent règlement. 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.

Lorsqu'un importateur a des raisons de croire qu'un produit comportant des éléments numériques peut présenter un risque de cybersécurité important à la lumière de facteurs de risque non techniques, il en informe les autorités de surveillance du marché. Dès réception de cette information, les autorités de surveillance du marché appliquent les procédures visées à l'article 54, paragraphe 2.

4. L'importateur indique son nom, sa raison sociale ou sa marque déposée et les adresses postale, électronique ou autre moyen numérique, ainsi que, le cas échéant, l'adresse du site internet auxquelles il peut être contacté sur le produit comportant des éléments numériques, 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. Tout importateur qui considère ou a des raisons de croire qu'un produit comportant des éléments numériques, qu'il a mis sur le marché n'est pas conforme au présent règlement prend immédiatement les mesures correctives nécessaires pour veiller à ce que ce produit comportant des éléments numériques soit mis en conformité avec le présent règlement, ou pour procéder au retrait ou au rappel du produit, si nécessaire.

   Lorsqu'il prend connaissance d'une vulnérabilité du produit comportant des éléments numériques, l'importateur en informe le fabricant sans retard injustifié. 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.

6. Pendant au moins dix ans à partir de la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la période la plus longue étant retenue, 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.

7. 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 de cybersécurité énoncées à l'annexe I, partie I, ainsi que la conformité des processus mis en place par le fabricant aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II, 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.

8. 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 prévues par 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 20

Obligations des distributeurs

1. Lorsqu'ils mettent un produit comportant des éléments numériques à disposition sur le marché, les distributeurs agissent avec la diligence requise en ce qui concerne les exigences énoncées au présent règlement.

2. Avant de mettre un produit comportant des éléments numériques à disposition sur le marché, les distributeurs vérifient que:

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

b) le fabricant et l'importateur se sont conformés aux obligations énoncées à l'article 13, paragraphes 15, 16, 18, 19 et 20, et à l'article 19, paragraphe 4, et ont communiqué tous les documents nécessaires au distributeur.

3. Lorsqu'un distributeur considère ou a des raisons de croire, sur la base des informations en sa possession, qu'un produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles de cybersécurité 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'a pas été mis en conformité avec le présent règlement. 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 sans retard injustifié.

4. Les distributeurs sachant ou ayant des raisons de croire, sur la base des informations en sa possession, qu'un produit comportant des éléments numériques, qu'ils ont mis à disposition sur le marché, ou bien les processus mis en place par son fabricant ne sont pas conformes au présent règlement veillent 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'ils prennent connaissance d'une vulnérabilité du produit comportant des éléments numériques, les distributeurs en informent le fabricant sans retard injustifié. En outre, si le produit comportant des éléments numériques présente un risque de cybersécurité important, les distributeurs en informent immédiatement les autorités de surveillance du marché des États membres dans lesquels ils ont 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, les distributeurs communiquent à cette dernière 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 son fabricant avec le présent règlement dans une langue aisément compréhensible par cette autorité. Ils coopèrent 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'ils ont mis à disposition sur le marché.

6. Lorsque le distributeur d'un produit comportant des éléments numériques apprend, sur la base des informations en sa possession, que le fabricant de ce produit a cessé ses activités et, de ce fait, n'est pas en mesure de se conformer aux obligations prévues par le présent règlement, il informe sans retard injustifié 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 21

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 au respect de l'article 13 et de l'article 14 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 22

Autres cas dans lesquels les obligations des fabricants s'appliquent

1. 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 et met ce produit à disposition sur le marché est considérée comme un fabricant aux fins du présent règlement.

2. La personne visée au paragraphe 1 du présent article, est soumise aux obligations énoncées à l'article 13 et à l'article 14 en ce qui concerne la partie du produit comportant des éléments numériques sur laquelle porte la modification substantielle, ou en ce qui concerne l'ensemble du produit si la modification substantielle a des répercussions sur la cybersécurité du produit comportant des éléments numériques dans son ensemble.

Article 23

Identification des opérateurs économiques

1. Les opérateurs économiques fournissent aux autorités de surveillance du marché, sur demande, les informations suivantes:

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

   b) lorsqu'il dispose de ces informations, le nom et l'adresse de tout opérateur économique auquel il a fourni un produit comportant des éléments numériques.

2. Les opérateurs économiques sont 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 leur a été fourni et pendant dix ans à compter de la date à laquelle ils l'ont fourni.

Article 24

Obligations des intendants de logiciels ouverts

1. Les intendants de logiciels ouverts mettent en place et documentent de manière vérifiable une politique de cybersécurité afin de favoriser le développement d'un produit comportant des éléments numériques sécurisé ainsi qu'un traitement efficace des vulnérabilités par les développeurs de ce produit. Cette politique encourage également le signalement volontaire des vulnérabilités, prévu à l'article 15, par les développeurs de ce produit et tient compte de la nature spécifique de l'intendant de logiciels ouverts et des modalités juridiques et organisationnelles auxquelles il est soumis. Cette politique comprend, en particulier, des aspects liés à la documentation, au traitement et à la correction des vulnérabilités, ainsi qu'à la promotion du partage d'informations sur les vulnérabilités découvertes au sein de la communauté des logiciels ouverts.

2. Les intendants de logiciels ouverts coopèrent avec les autorités de surveillance du marché, à leur demande, en vue d'atténuer les risques de cybersécurité posés par un produit comportant des éléments numériques qui répond aux critères de logiciel libre et ouvert.

   Sur demande motivée d'une autorité de surveillance du marché, les intendants de logiciels ouverts fournissent à cette autorité, dans une langue aisément compréhensible par celle-ci, la documentation visée au paragraphe 1, sur support papier ou sous forme électronique.

3. Les obligations prévues à l'article 14, paragraphe 1, s'appliquent aux intendants de logiciels ouverts dès lors qu'ils participent au développement des produits comportant des éléments numériques. Les obligations prévues à l'article 14, paragraphes 3 et 8, s'appliquent aux intendants de logiciels ouverts dès lors que des incidents graves ayant des répercussions sur la sécurité des produits comportant des éléments numériques touchent les réseaux et les systèmes d'information fournis par les intendants de logiciels ouverts pour le développement de ces produits.

Article 25

Attestation de sécurité des logiciels libres et ouverts

Afin de faciliter le respect de l'obligation de diligence raisonnable énoncée à l'article 13, paragraphe 5, en particulier en ce qui concerne les fabricants qui intègrent des composants logiciels libres et ouverts dans leurs produits comportant des éléments numériques, la Commission est habilitée à adopter des actes délégués conformément à l'article 61 afin de compléter le présent règlement en mettant en place des programmes volontaires d'attestation de sécurité permettant aux développeurs ou aux utilisateurs de produits comportant des éléments numériques répondant aux critères de logiciel libre et ouvert ainsi qu'à d'autres tiers d'évaluer la conformité de ces produits à l'ensemble ou à une partie des exigences essentielles de cybersécurité ou d'autres obligations prévues par le présent règlement.

Article 26

Orientations

1. Afin de faciliter la mise en œuvre et de veiller à sa cohérence, la Commission publie des orientations pour aider les opérateurs économiques à appliquer le présent règlement, en mettant tout particulièrement l'accent sur la nécessité de favoriser la conformité par les microentreprises et les petites et moyennes entreprises.

2. Lorsqu'elle entend fournir les orientations visées au paragraphe 1, la Commission aborde au moins les aspects suivants:

   a) le champ d'application du présent règlement, en particulier les solutions de traitement de données à distance et les logiciels libres et ouverts;

   b) l'application de périodes d'assistance pour certaines catégories particulières de produits comportant des éléments numériques;

   c) des orientations destinées aux fabricants soumis au présent règlement qui sont également soumis à une législation d'harmonisation de l'Union autre que le présent règlement ou à d'autres actes juridiques connexes de l'Union;

   d) la notion de modification substantielle.

   La Commission tient également à jour une liste facile d'accès des actes délégués et des actes d'exécution adoptés en vertu du présent règlement.

3. Dans le cadre de l'élaboration des orientations visées au présent article, la Commission consulte les parties intéressées.

Chapitre III

Conformité du produit comportant des éléments numériques

Article 27

Présomption de conformité

1. Les produits 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 de cybersécurité énoncées à l'annexe I qui sont couvertes par ces normes ou parties de ces normes.

   Conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées relatives aux exigences essentielles de cybersécurité énoncées à l'annexe I du présent règlement. Lorsqu'elle prépare des demandes de normalisation aux fins du présent règlement, la Commission s'efforce de tenir compte des normes européennes et internationales existantes en matière de cybersécurité qui sont en place ou en cours d'élaboration afin de simplifier l'élaboration de normes harmonisées, conformément au règlement (UE) n° 1025/2012.

2. La Commission peut adopter des actes d'exécution qui établissent des spécifications communes couvrant les exigences techniques qui offrent un moyen de se conformer aux exigences essentielles de cybersécurité énoncées à l'annexe I en ce qui concerne les produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement.

Ces actes d'exécution ne sont adoptés que lorsque les conditions suivantes sont remplies:

a) La Commission, conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée relative aux exigences essentielles de cybersécurité énoncées à l'annexe I et:

i) la demande n'a pas été acceptée;

ii) les normes harmonisées répondant à cette demande ne sont pas présentées dans le délai fixé conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012; ou

iii) les normes harmonisées ne sont pas conformes à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences essentielles pertinentes de cybersécurité énoncées à l'annexe I n'a été publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012 et il n'est pas prévu que la publication d'une telle référence soit publiée dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

3. Avant d'élaborer le projet d'acte d'exécution visé au paragraphe 2 du présent article, la Commission informe le comité visé à l'article 22 du règlement (UE) n° 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 2 du présent article sont remplies.

4. Lorsqu'elle élabore le projet d'acte d'exécution visé au paragraphe 2, la Commission tient compte de l'avis des organismes compétents et consulte dûment toutes les parties prenantes concernées.

5. Les produits comportant des éléments numériques et les processus mis en place par le fabricant qui sont conformes aux spécifications communes établies par des actes d'exécution visés au paragraphe 2 du présent article, ou à des parties de ces spécifications communes, sont présumés conformes aux exigences essentielles de cybersécurité énoncées à l'annexe I couvertes par ces spécifications communes ou parties de spécifications communes.

6. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission aux fins de la publication de sa référence au *Journal officiel de l'Union européenne*, la Commission évalue la norme harmonisée conformément au règlement (UE) n° 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au *Journal officiel de l'Union européenne*, la Commission abroge les actes d'exécution visés au paragraphe 2 ou les parties de ces actes qui couvrent les mêmes exigences essentielles de cybersécurité que celles couvertes par cette norme harmonisée.

7. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles de cybersécurité énoncées à l'annexe I, il en informe la Commission en lui fournissant une explication détaillée. La Commission examine cette explication détaillée et peut, s'il y a lieu, modifier l'acte d'exécution établissant la spécification commune en question.

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

9. La Commission est habilitée à adopter des actes délégués conformément à l'article 61 du présent règlement pour compléter le présent règlement en précisant les schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 qui peuvent être utilisés afin de démontrer la conformité de produits comportant des éléments numériques avec les exigences essentielles de cybersécurité énoncées à l'annexe I du présent règlement, ou avec des parties de ces exigences. En outre, la délivrance d'un certificat de cybersécurité européen au titre de tels schémas, au minimum au niveau d'assurance dit "substantiel", 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 32, paragraphe 2, points a) et b), et à l'article 32, paragraphe 3, points a) et b), du présent règlement.

Article 28

Déclaration UE de conformité

1. La déclaration UE de conformité est établie par le fabricant conformément à l'article 13, paragraphe 12, et atteste que le respect des exigences essentielles de cybersécurité applicables énoncées à l'annexe I a été démontré.

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

La déclaration UE de conformité simplifiée visée à l'article 13, paragraphe 20, est établie selon le modèle figurant à l'annexe VI. Elle est disponible dans les langues requises par l'État membre dans lequel le produit comportant des éléments numériques est mis sur le marché ou mis à disposition sur le marché.

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

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour compléter le présent règlement aux fins d'ajouter des éléments au contenu minimal de la déclaration UE de conformité prévu à l'annexe V afin de tenir compte des progrès techniques.

Article 29

Principes généraux du marquage CE

Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 765/2008.

Article 30

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 28 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 28, soit sur le site internet qui accompagne le logiciel. Dans ce dernier cas, la section correspondante du site internet est aisément et directement accessible aux consommateurs.

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 en matière de cybersécurité 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 32.

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'une législation d'harmonisation de l'Union autre que le présent règlement qui prévoit aussi l'apposition du marquage CE, le marquage CE indique que le produit satisfait également aux exigences énoncées dans cette autre législation d'harmonisation de l'Union.

6. La Commission peut, par voie d'actes d'exécution, définir des spécifications techniques pour les étiquettes, les pictogrammes ou tout autre marquage en lien avec la sécurité des produits comportant des éléments numériques, leurs périodes d'assistance ainsi que des mécanismes visant à promouvoir leur utilisation et à sensibiliser le public à la sécurité des produits comportant des éléments numériques. Lors de l'élaboration des projets d'actes d'exécution, la Commission consulte les parties prenantes concernées et, s'il a déjà été établi en vertu de l'article 52, paragraphe 15, l'ADCO. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 31

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 de cybersécurité énoncées à l'annexe I. Elle contient, au minimum, les éléments énumérés à l'annexe VII.

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, au moins pendant la période d'assistance.

3. Pour les produits comportant des éléments numériques visés à l'article 12, qui relèvent aussi d'autres actes juridiques de l'Union prévoyant une documentation technique, une seule documentation technique est établie, contenant les informations visées à l'annexe VII ainsi que les informations requises en vertu de ces actes juridiques 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 61 pour compléter le présent règlement en ajoutant des éléments à inclure dans la documentation technique figurant à l'annexe VII pour tenir compte des progrès techniques ainsi que des évolutions rencontrées dans le processus de mise en œuvre du présent règlement. À cette fin, la Commission s'efforce de faire en sorte que la charge administrative pesant sur les microentreprises et les petites et moyennes entreprises soit proportionnée.

Article 32

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 de cybersécurité énoncées à l'annexe I sont respectées. Le fabricant démontre la conformité avec les exigences essentielles de cybersécurité en suivant l'une des procédures suivantes:

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

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

c) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VIII; ou

d) lorsqu'il est disponible et s'il y a lieu, un schéma européen de certification de cybersécurité en vertu de l'article 27, paragraphe 9.

2. Lorsque, lors de l'évaluation de la conformité d'un produit important comportant des éléments numériques qui relève de la classe I figurant à l'annexe III et des processus mis en place par son fabricant avec les exigences essentielles de cybersécurité énoncées à l'annexe I, le 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 au minimum au niveau d'assurance dit "substantiel" visés à l'article 27, 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 de cybersécurité, à l'une des procédures suivantes:

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

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

3. Lorsque le produit est un produit important comportant des éléments numériques qui relève de la classe II figurant à l'annexe III, le fabricant démontre la conformité avec les exigences essentielles de cybersécurité 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 VIII, suivie de la conformité au type "UE" sur la base du contrôle interne de la production (module C), prévue à l'annexe VIII;

b) une évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VIII; ou

c) lorsqu'il est disponible et s'il y a lieu, un schéma européen de certification de cybersécurité conformément à l'article 27, paragraphe 9, du présent règlement au minimum au niveau d'assurance dit "substantiel" en vertu du règlement (UE) 2019/881.

4. Les produits critiques comportant des éléments numériques répertoriés à l'annexe IV démontrent la conformité avec les exigences essentielles de cybersécurité énoncées à l'annexe I au moyen de l'une des procédures suivantes:

a) un schéma européen de certification de cybersécurité, conformément à l'article 8, paragraphe 1; ou

b) lorsque les conditions énoncées à l'article 8, paragraphe 1, ne sont pas remplies, l'une des procédures visées au paragraphe 3 du présent article.

5. Les fabricants de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts et relèvent des catégories énoncées à l'annexe III ont la faculté de démontrer la conformité avec les exigences essentielles de cybersécurité énoncées à l'annexe I en utilisant l'une des procédures visées au paragraphe 1 du présent article, à condition que la documentation technique visée à l'article 31 soit mise à la disposition du public au moment de la mise sur le marché de ces produits.

6. Les intérêts et besoins spécifiques des microentreprises et des petites et moyennes entreprises, y compris les jeunes pousses, sont pris en compte lors de la fixation des redevances imposées pour les procédures d'évaluation de la conformité, et ces redevances sont réduites proportionnellement auxdits intérêts et besoins spécifiques.

Article 33

Mesures de soutien pour les microentreprises et les petites et moyennes entreprises, y compris les jeunes pousses

1. Les États membres entreprennent, le cas échéant, les actions suivantes, adaptées aux besoins des microentreprises et des petites entreprises:

   a) organiser des activités spécifiques de sensibilisation et de formation sur l'application du présent règlement;

b) mettre en place un canal de communication spécifique avec les microentreprises et les petites entreprises et, le cas échéant, les autorités publiques locales afin de fournir des conseils et de répondre aux questions à propos de la mise en œuvre du présent règlement;

c) soutenir les activités d'essai et d'évaluation de la conformité, y compris, le cas échéant, avec le soutien du Centre de compétences européen en matière de cybersécurité.

2. Les États membres peuvent, le cas échéant, mettre en place des sas réglementaires en matière de cyberrésilience. Ces sas réglementaires prévoient des environnements d'essai contrôlés pour les produits innovants comportant des éléments numériques afin de faciliter leur développement, leur conception, leur validation et leur mise à l'essai aux fins de se conformer au présent règlement pendant une période de temps limitée avant la mise sur le marché. La Commission et, le cas échéant, l'ENISA peuvent fournir un soutien technique, des conseils et des outils pour la mise en place et le fonctionnement de sas réglementaires. Les sas réglementaires sont mis en place sous la surveillance et le contrôle et avec le soutien directs des autorités de surveillance du marché. Les États membres informent la Commission et les autres autorités de surveillance du marché de la mise en place d'un sas réglementaire par l'intermédiaire de l'ADCO. Les sas réglementaires n'ont pas d'incidence sur les pouvoirs des autorités compétentes en matière de contrôle et de mesures correctives. Les États membres garantissent un accès ouvert, équitable et transparent aux sas réglementaires et, en particulier, facilitent l'accès des microentreprises et des petites entreprises, y compris les jeunes pousses.

3. Conformément à l'article 26, la Commission fournit des orientations aux microentreprises et aux petites et moyennes entreprises en ce qui concerne la mise en œuvre du présent règlement.

4. La Commission fait connaître le soutien financier disponible dans le cadre réglementaire des programmes de l'Union existants, notamment dans le but d'alléger la charge financière pesant sur les microentreprises et les petites entreprises.

5. Les microentreprises et les petites entreprises peuvent fournir tous les éléments de la documentation technique indiqués à l'annexe VII en utilisant un format simplifié. À cette fin, la Commission définit, par voie d'actes d'exécution, le formulaire de documentation technique simplifié adapté aux besoins des microentreprises et des petites entreprises, y compris la manière dont les éléments énoncés à l'annexe VII doivent être fournis. Lorsqu'une microentreprise ou une petite entreprise choisit de fournir les informations énoncées à l'annexe VII d'une manière simplifiée, elle utilise le formulaire visé au présent paragraphe. Les organismes notifiés acceptent ce formulaire aux fins de l'évaluation de la conformité.

   Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 34

Accords de reconnaissance mutuelle

Compte tenu du niveau de développement technique et de l'approche en matière d'évaluation de la conformité d'un pays tiers, l'Union peut conclure des accords de reconnaissance mutuelle avec des pays tiers, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne, afin de promouvoir et de faciliter le commerce international.

Chapitre IV

Notification des organismes d'évaluation de la conformité

Article 35

Notification

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

2. Les États membres, au plus tard le … [*24 mois à compter de la date d'entrée en vigueur du présent règlement*], s'efforcent d'assurer la disponibilité, en nombre suffisant, d'organismes notifiés dans l'Union pour effectuer des évaluations de la conformité, afin d'éviter les goulets d'étranglement et les obstacles à l'entrée sur le marché.

Article 36

Autorités notifiantes

1. Chaque État membre désigne une autorité notifiante responsable de la mise en place et de l'application des procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité ainsi qu'à leur contrôle, y compris le respect de l'article 41.

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) n° 765/2008 et conformément à ses dispositions.

3. Lorsque l'autorité notifiante délègue ou confie d'une autre façon l'évaluation, la notification ou le contrôle visés au paragraphe 1 du présent article à un organisme qui n'appartient pas au secteur public, cet organisme est une personne morale et se conforme mutatis mutandis aux dispositions de l'article 37. En outre, cet organisme prend ses dispositions pour assumer les responsabilités qui découlent de ses activités.

4. L'autorité notifiante assume la pleine responsabilité des tâches accomplies par l'organisme visé au paragraphe 3.

Article 37

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 38

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 les informations visées au paragraphe 1.

Article 39

Exigences relatives aux 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 comportant des éléments numériques 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, à condition que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées, être considéré comme étant un tel organisme tiers.

4. Un organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter les tâches d'évaluation de la conformité ne peuvent être le concepteur, le développeur, le fabricant, le fournisseur, l'importateur, le distributeur, 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 chargé d'exécuter les tâches d'évaluation de la conformité n'interviennent pas directement dans la conception, le développement, la production, l'importation, la distribution, la commercialisation, l'installation, l'utilisation ou l'entretien des produits comportant des éléments numériques qu'ils évaluent 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 VIII 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 à utiliser 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.

Un organisme d'évaluation de la conformité 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 de cybersécurité énoncées à l'annexe I, des normes harmonisées et des spécifications communes 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 leur État membre 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 VIII 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 institué en vertu de l'article 51, 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, proportionnées et raisonnables, tout en évitant de créer une charge inutile pour les opérateurs économiques, notamment en tenant compte des intérêts des microentreprises et des petites et moyennes entreprises pour ce qui est des redevances.

Article 40

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 39 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

Article 41

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 39 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 42

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 comportant des éléments numériques pour lesquels cet organisme se déclare compétent, ainsi que, le cas échéant, d'un certificat d'accréditation délivré par un organisme national d'accréditation, qui atteste que l'organisme d'évaluation de la conformité remplit les exigences prévues à l'article 39.

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 prévues à l'article 39.

Article 43

Procédure de notification

1. Les autorités notifiantes ne notifient que les organismes d'évaluation de la conformité qui satisfont aux exigences prévues à l'article 39.

2. L'autorité notifiante notifie la Commission et les autres États membres à l'aide du système d'information *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 comportant des éléments numériques 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 42, 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 prévues à l'article 39.

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 44

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 juridiques 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 45

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 prévues à l'article 39, 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 46

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 pour remplir les exigences qui lui sont applicables et s'acquitter des responsabilités qui lui incombent, ou quant au fait qu'il continue à remplir ces exigences et à s'acquitter de ces responsabilités.

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 s'assure 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 47

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 32 et à l'annexe VIII.

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, en particulier en ce qui concerne les microentreprises et les petites et moyennes entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, de leur degré de complexité, du niveau du risque pour la cybersécurité des produits comportant des éléments numériques et de la technologie 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 des produits comportant des éléments numériques avec les dispositions du présent règlement.

4. Lorsqu'un organisme notifié constate que les exigences énoncées à l'annexe I ou dans les normes harmonisées correspondantes ou les spécifications communes telles que visées à l'article 27 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 comportant des éléments numériques ne respecte plus les exigences prévues par le présent règlement, il exige du fabricant qu'il prenne les mesures correctives 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, selon cas.

Article 48

Recours contre les décisions des organismes notifiés

Les États membres veillent à ce que les décisions des organismes notifiés soient susceptibles de recours.

Article 49

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 comportant des éléments numériques des informations pertinentes sur les questions relatives aux résultats négatifs de l'évaluation de la conformité et, sur demande, aux résultats positifs.

Article 50

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 51

Coordination des organismes notifiés

1. La Commission assure la mise en place et le bon fonctionnement d'une coordination et d'une coopération appropriées des organismes notifiés 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 52

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. Les autorités de surveillance du marché désignées en vertu du paragraphe 2 du présent article sont également chargées d'effectuer des activités de surveillance du marché en ce qui concerne les obligations des intendants de logiciels ouverts prévues à l'article 24. Lorsqu'une autorité de surveillance du marché constate qu'un intendant de logiciels ouverts ne respecte pas les obligations énoncées audit article, elle demande audit intendant de veiller à ce que toutes les mesures correctives appropriées soient prises. Les intendants de logiciels ouverts veillent à ce que toutes les mesures correctives appropriées soient prises en ce qui concerne les obligations qui leur incombent en vertu du présent règlement.

4. 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 et échangent régulièrement des informations avec les CSIRT désignés comme coordinateurs et 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 14 du présent règlement.

5. Les autorités de surveillance du marché peuvent demander à un CSIRT désigné comme coordinateur ou à l'ENISA de fournir des conseils techniques sur des questions liées à la mise en œuvre et à l'application du présent règlement. Lorsqu'elles mènent une enquête en vertu de l'article 54, les autorités de surveillance du marché peuvent demander au CSIRT désigné comme coordinateur ou à l'ENISA de fournir une analyse à l'appui des évaluations de conformité de produits comportant des éléments numériques.

6. Le cas échéant, les autorités de surveillance du marché coopèrent avec d'autres autorités de surveillance du marché désignées sur la base d'une législation d'harmonisation de l'Union autre que le présent règlement et échangent des informations régulièrement.

7. 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 10, 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.

8. Les États membres veillent à ce que les autorités de surveillance du marché désignées disposent de ressources financières et techniques suffisantes, y compris, le cas échéant, d'outils de traitement automatisé, ainsi que de ressources humaines dotées des compétences nécessaires en matière de cybersécurité pour mener à bien les tâches qui leur sont confiées au titre du présent règlement.

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

10. Avec le soutien de la Commission et, le cas échéant, des CSIRT et de l'ENISA, les autorités de surveillance du marché peuvent fournir des orientations et des conseils aux opérateurs économiques sur la mise en œuvre du présent règlement.

11. Les autorités de surveillance du marché informent les consommateurs de l'endroit où déposer des réclamations qui pourraient indiquer un non-respect du présent règlement, conformément à l'article 11 du règlement (UE) 2019/1020, et leur donnent des informations sur les points et modalités d'accès aux mécanismes qui facilitent le signalement des vulnérabilités, des incidents et des cybermenaces susceptibles d'affecter des produits comportant des éléments numériques.

12. Les autorités de surveillance du marché facilitent, le cas échéant, la coopération avec les parties prenantes concernées, notamment des organisations scientifiques, de recherche et de consommateurs.

13. 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.

14. Pour les produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement et sont classés comme systèmes d'IA à haut risque en vertu de l'article 6 du règlement (UE) 2024/1689, les autorités de surveillance du marché désignées aux fins du règlement (UE) 2024/1689 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 (UE) 2024/1689 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 14 du présent règlement, avec les CSIRT désignés comme coordinateurs et l'ENISA. Les autorités de surveillance du marché désignées en vertu du règlement (UE) 2024/1689 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.

15. L'ADCO est établi pour l'application uniforme du présent règlement, conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. L'ADCO se compose de représentants des autorités de surveillance du marché désignées et, si nécessaire, de représentants des bureaux de liaison uniques. L'ADCO traite également de questions spécifiques liées aux activités de surveillance du marché en ce qui concerne les obligations imposées aux intendants de logiciels ouverts.

16. Les autorités de surveillance du marché contrôlent la manière dont les fabricants ont appliqué les critères indiqués à l'article 13, paragraphe 8, en déterminant la période d'assistance pour leurs produits comportant des éléments numériques.

L'ADCO publie sous une forme accessible au public et conviviale des statistiques pertinentes sur les catégories de produits comportant des éléments numériques, y compris leur période d'assistance moyenne, telle que déterminée par le fabricant conformément à l'article 13, paragraphe 8, et fournit des orientations qui comprennent des périodes d'assistance indicatives pour les catégories de produits comportant des éléments numériques.

Lorsque les données donnent à penser que les périodes d'assistance sont insuffisantes pour des catégories spécifiques de produits comportant des éléments numériques, l'ADCO peut adresser des recommandations aux autorités de surveillance du marché afin qu'elles concentrent leurs activités sur ces catégories de produits comportant des éléments numériques.

Article 53

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 de cybersécurité énoncées à l'annexe I, les autorités de surveillance du marché, sur demande motivée, ont accès, dans une langue qu'elles comprennent facilement, 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 54

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 sans retard injustifié et, le cas échéant, en coopération avec le CSIRT concerné, à une évaluation de la conformité de ce produit avec l'ensemble des exigences prévues par 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 prévues par le présent règlement, elle invite sans retard l'opérateur économique en cause à prendre toutes les mesures correctives appropriées pour mettre le produit comportant des éléments numériques en conformité avec ces exigences, le retirer du marché ou le rappeler dans un délai raisonnable, proportionné à la nature du risque de cybersécurité, que l'autorité de surveillance du marché 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.

2. Lorsqu'elles déterminent l'importance d'un risque de cybersécurité visé au paragraphe 1 du présent article, les autorités de surveillance du marché tiennent également compte des facteurs de risque non techniques, en particulier de ceux établis à la suite des évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques effectuées conformément à l'article 22 de la directive (UE) 2022/2555. Lorsqu'une autorité de surveillance du marché a des raisons suffisantes de considérer qu'un produit comportant des éléments numériques présente un risque de cybersécurité important à la lumière de facteurs de risque non techniques, elle en informe les autorités compétentes désignées ou établies en vertu de l'article 8 de la directive (UE) 2022/2555 et coopère avec ces autorités en tant que de besoin.

3. 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 prescrites à l'opérateur économique.

4. L'opérateur économique 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.

5. Lorsque l'opérateur économique 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 comportant des éléments numériques sur son marché national ou pour procéder à son retrait de ce marché ou à son rappel.

L'autorité notifie sans retard ces mesures à la Commission et aux autres États membres.

6. Les informations visées au paragraphe 5 contiennent toutes les précisions disponibles, notamment en ce qui concerne les données nécessaires pour identifier le produit comportant des éléments numériques non conforme, l'origine de ce 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 économique 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 comportant des éléments numériques ou des processus mis en place par le fabricant avec les exigences essentielles de cybersécurité énoncées à l'annexe I;

   b) des lacunes dans les normes harmonisées, les systèmes européens de certification de cybersécurité ou les spécifications communes visés à l'article 27.

7. 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 comportant des éléments numériques concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception de la notification visée au paragraphe 5 du présent article, 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 économique concerné conformément à l'article 18 du règlement (UE) 2019/1020.

9. 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 comportant des éléments numériques concerné.

Article 55

Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 54, paragraphe 5, un État membre soulève des objections à l'encontre d'une mesure prise par un autre État membre ou que la Commission considère que la mesure est contraire à la législation de l'Union, la Commission entame sans retard 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 54, paragraphe 5, et communique cette 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 n'est pas jugée justifiée, 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 11 du règlement (UE) n° 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 27, la Commission examine s'il y a lieu de modifier ou d'abroger l'acte délégué adopté conformément à l'article 27, paragraphe 9, 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 27, la Commission examine s'il y a lieu de modifier ou d'abroger tout acte d'exécution adopté en vertu de l'article 27, paragraphe 2, qui établit ces spécifications communes.

Article 56

Procédure au niveau de l'Union 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 prévues par le présent règlement, elle en informe les autorités de surveillance du marché concernées. Lorsque les autorités de surveillance du marché procèdent à une évaluation de ce produit comportant des éléments numériques susceptible de présenter un risque de cybersécurité important en ce qui concerne sa conformité avec les exigences prévues par le présent règlement, les procédures visées aux articles 54 et 55 s'appliquent.

2. Lorsque la Commission a des raisons suffisantes de considérer qu'un produit comportant des éléments numériques présente un risque de cybersécurité important à la lumière de facteurs de risque non techniques, elle en informe les autorités de surveillance du marché concernées et, le cas échéant, les autorités compétentes désignées ou établies en vertu de l'article 8 de la directive (UE) 2022/2555 et coopère avec ces autorités en tant que de besoin. La Commission examine également la pertinence des risques recensés pour ce produit comportant des éléments numériques au regard de ses tâches en ce qui concerne les évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques prévues à l'article 22 de la directive (UE) 2022/2555, et consulte, le cas échéant, le groupe de coopération institué en vertu de l'article 14 de la directive (UE) 2022/2555 et l'ENISA.

3. Dans des circonstances 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 comportant des éléments numériques visé au paragraphe 1 demeure non conforme aux exigences prévues par le présent règlement et qu'aucune mesure effective n'a été prise par les autorités de surveillance du marché concernées, la Commission procède à une évaluation de la conformité et peut demander à l'ENISA de fournir une analyse afin d'étayer cette évaluation. La Commission en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

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

5. Sur la base de la consultation visée au paragraphe 4 du présent article, la Commission peut adopter des actes d'exécution afin de fournir des mesures correctives ou restrictives au niveau de l'Union, y compris en exigeant le retrait du marché ou le rappel des produits comportant des éléments numériques concernés, 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 62, paragraphe 2.

6. La Commission communique immédiatement à l'opérateur ou aux opérateurs économiques concernés les actes d'exécution visés au paragraphe 5. Les États membres exécutent ces actes d'exécution sans retard et en informent la Commission.

7. Les paragraphes 3 à 6 sont applicables pendant la durée de la situation exceptionnelle qui a justifié l'intervention de la Commission, pour autant que le produit comportant des éléments numériques concerné ne soit pas mis en conformité avec le présent règlement.

Article 57

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

1. L'autorité de surveillance du marché d'un État membre exige d'un opérateur économique qu'il prenne toutes les mesures appropriées lorsque, après avoir effectué une évaluation au titre de l'article 54, elle 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:

   a) la santé ou la sécurité des personnes;

   b) le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux;

c) la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services proposés au moyen d'un système d'information électronique par des entités essentielles visées à l'article 3, paragraphe 1, de la directive (UE) 2022/2555; ou

d) d'autres aspects de la protection de l'intérêt public.

Les mesures visées au premier alinéa peuvent comprendre des mesures visant à garantir que le produit comportant des éléments numériques concerné et les processus mis en place par le fabricant ne présentent plus les risques pertinents lors de la mise à disposition sur le marché, le retrait du marché du produit comportant des éléments numériques concerné ou son rappel, et sont proportionnées à la nature de ces risques.

2. Le fabricant ou les autres opérateurs économiques 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 la décision visée au paragraphe 4 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 du présent article, elle en informe les autorités de surveillance du marché concernées et peut leur demander de procéder à une évaluation et de suivre les procédures visées à l'article 54 et aux paragraphes 1, 2 et 3 du présent article.

7. Dans des circonstances 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 comportant des éléments numériques 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 procède à une évaluation des risques présentés par ledit produit comportant des éléments numériques, peut demander à l'ENISA de fournir une analyse afin d'étayer cette évaluation 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 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 retard les États membres concernés et le ou les opérateurs économiques concernés.

9. Sur la base de la consultation visée au paragraphe 8 du présent article, la Commission peut adopter des actes d'exécution afin de décider de mesures correctives ou restrictives au niveau de l'Union, y compris en exigeant le retrait du marché ou le rappel des produits comportant des éléments numériques concernés, 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 62, paragraphe 2.

10. La Commission communique immédiatement à l'opérateur ou aux opérateurs économiques concernés les actes d'exécution visés au paragraphe 9. Les États membres exécutent ces actes d'exécution sans retard 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 comportant des éléments numériques concerné continue de présenter les risques visés au paragraphe 1.

Article 58

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 CE a été apposé en violation de l'article 29 ou 30;

b) le marquage CE 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 59

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 comportant des éléments numériques dont il est souvent constaté qu'ils présentent des risques de cybersécurité.

2. La Commission ou l'ENISA proposent 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 comportant des éléments numériques qui relèvent du champ d'application du présent règlement, aux exigences prévues par le présent règlement.

3. Les autorités de surveillance du marché et, le cas échéant, la Commission, 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 obtenues à la suite des activités conjointes menées dans le cadre des enquêtes qu'elle entreprend.

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

Article 60

Opérations "coup de balai"

1. Les autorités de surveillance du marché mènent des actions de contrôle coordonnées et simultanées (ci-après dénommées "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. Ces opérations "coup de balai" peuvent comprendre des inspections des produits comportant des éléments numériques acquis sous une fausse identité.

2. Sauf accord contraire des autorités de surveillance du marché participantes, les opérations "coup de balai" sont coordonnées par la Commission. Le coordinateur de l'opération "coup de balai" met, s'il y a lieu, les résultats agrégés de l'opération à la disposition du public.

3. Lorsque, dans l'exécution de ses tâches, y compris sur la base des notifications reçues en vertu de l'article 14, paragraphes 1 et 3, l'ENISA identifie des catégories de produits comportant des éléments numériques pour lesquelles des opérations "coup de balai" peuvent être organisées, elle soumet une proposition d'opération coup de balai" au coordinateur visé au paragraphe 2 du présent article 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 52 à 58, 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 61

Exercice de la délégation

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

2. Le pouvoir d'adopter des actes délégués visé à l'article 2, paragraphe 5, deuxième alinéa, à l'article 7, paragraphe 3, à l'article 8, paragraphes 1 et 2, à l'article 13, paragraphe 8, quatrième alinéa, à l'article 14, paragraphe 9, à l'article 25, à l'article 27, paragraphe 9, à l'article 28, paragraphe 5, et à l'article 31, paragraphe 5, est conféré à la Commission pour une période de cinq ans à compter du … [*date d'entrée en vigueur du présent règlement*]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 2, paragraphe 5, deuxième alinéa, à l'article 7, paragraphe 3, à l'article 8, paragraphes 1 et 2, à l'article 13, paragraphe 8, quatrième alinéa, à l'article 14, paragraphe 9, à l'article 25, à l'article 27, paragraphe 9, à l'article 28, paragraphe 5, et à l'article 31, 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 l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis 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 5, deuxième alinéa, de l'article 7, paragraphe 3, de l'article 8, paragraphe 1 ou 2, de l'article 13, paragraphe 8, quatrième alinéa, de l'article 14, paragraphe 9, de l'article 25, de l'article 27, paragraphe 9, de l'article 28, paragraphe 5, ou de l'article 31, 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 62

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 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 63

Confidentialité

1. Toutes les parties intervenant dans 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[36];

   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.

[36] 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).

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 64

Sanctions

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

2. Le non-respect des exigences de cybersécurité énoncées à l'annexe I et avec les obligations énoncées aux articles 13 et 14 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.

3. Le non-respect des obligations établies aux articles 18 à 23, à l'article 28, à l'article 30, paragraphes 1 à 4, à l'article 31, paragraphes 1 à 4, à l'article 32, paragraphes 1, 2 et 3, à l'article 33, paragraphe 5, et aux articles 39, 41, 47, 49 et 53 fait l'objet d'une amende administrative 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.

4. 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.

5. 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 les mêmes ou d'autres autorités de surveillance du marché au même opérateur économique pour une infraction similaire;

   c) la taille, en particulier en ce qui concerne les microentreprises, les petites et moyennes entreprises, y compris les jeunes entreprises, et la part de marché de l'opérateur économique qui commet l'infraction.

6. 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.

7. 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.

8. 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.

9. 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.

10. Par dérogation aux paragraphes 3 à 9, les amendes administratives visées auxdits paragraphes ne s'appliquent pas:

    a) aux fabricants considérés comme des microentreprises ou des petites entreprises en cas de non-respect du délai visé à l'article 14, paragraphe 2, point a), ou à l'article 14, paragraphe 4, point a);

    b) à toute violation du présent règlement par les intendants de logiciels ouverts.

Article 65

Actions représentatives

La directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des opérateurs économiques aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs.

Chapitre VIII

Dispositions transitoires et finales

Article 66

Modification du règlement (UE) 2019/1020

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

"XX[+]) Règlement (UE) 2024/... du Parlement européen et du Conseil[*++].

---

[*] Règlement (UE) 2024/... du Parlement européen et du Conseil du … relatif aux exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, ..., ELI: ...).".

[+] JO: veuillez insérer dans le texte le numéro consécutif suivant de la liste figurant à l'annexe I du règlement (UE) 2019/1020.

[++] JO: veuillez insérer dans le texte le numéro du règlement contenu dans le document PE-CONS 100/23 (2022/0272 (COD)) et insérer le numéro, la date et la référence de publication au JO de ce règlement dans la note de bas de page.

Article 67

Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

"XX[+]) Règlement (UE) 2024/… du Parlement européen et du Conseil[*++].

---

[*] Règlement (UE) 2024/... du Parlement européen et du Conseil du … relatif aux exigences horizontales de cybersécurité pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, ..., ELI: ...).".

[+] JO: veuillez insérer dans le texte le numéro consécutif suivant de la liste figurant à l'annexe I de la directive (UE) 2020/1828.

[++] JO: veuillez insérer dans le texte le numéro du règlement contenu dans le document PE-CONS 100/23 (2022/0272 (COD)) et insérer le numéro, la date et la référence de publication au JO de ce règlement dans la note de bas de page.

Article 68

Modification du règlement (UE) n° 168/2013

L'annexe II du règlement (UE) n° 168/2013 du Parlement européen et du Conseil[37] est modifiée comme suit:

Dans la partie C1, l'entrée suivante est ajoutée dans le tableau:

"

XX[+]	18	Protection du véhicule contre les cyberattaques		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

".

[37] Règlement (UE) n° 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52).

[+] JO: veuillez insérer le numéro consécutif suivant dans la rubrique C1 de l'annexe II du règlement (UE) n° 168/2013.

Article 69

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 à compter de 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 d'harmonisation de l'Union, auquel cas elles restent valables conformément à cette législation.

2. Les produits comportant des éléments numériques qui ont été mis sur le marché avant le ... [*36 mois à compter de la date d'entrée en vigueur du présent règlement*] ne sont soumis aux exigences énoncées dans le présent règlement que si, à compter de cette date, ces produits font l'objet d'une modification substantielle.

3. Par dérogation au paragraphe 2 du présent article, les obligations prévues à l'article 14 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 le … [*36 mois à compter de la date d'entrée en vigueur du présent règlement*].

Article 70

Évaluation et réexamen

1. Au plus tard le … [*72 mois à compter de la date d'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, la Commission présente un rapport sur l'évaluation et le réexamen du présent règlement au Parlement européen et au Conseil. Ces rapports sont rendus publics.

2. Au plus tard le … [*45 mois à compter de la date d'entrée en vigueur du présent règlement*], la Commission, après consultation de l'ENISA et du réseau des CSIRT, présente au Parlement européen et au Conseil un rapport pour évaluer l'efficacité de la plateforme unique de signalement prévue à l'article 16, ainsi que les répercussions de l'application des motifs liés à la cybersécurité visés à l'article 16, paragraphe 2, par les CSIRT désignés comme coordinateurs sur l'efficacité de la plateforme unique de signalement en ce qui concerne la diffusion en temps utile des notifications reçues à d'autres CSIRT concernés.

Article 71

Entrée en vigueur et application

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

2. Le présent règlement est applicable à partir du … [*36 mois à compter de la date d'entrée en vigueur du présent règlement*].

   Toutefois, l'article 14 est applicable à partir du ... [*21 mois à compter de la date d'entrée en vigueur du présent règlement*] et le chapitre IV (articles 35 à 51) à partir du ... [*18 mois à compter de 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 …, le

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

ANNEXE I

EXIGENCES ESSENTIELLES DE CYBERSÉCURITÉ

Partie I Exigences de cybersécurité relatives aux propriétés des produits comportant des éléments numériques

1) Les produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques.

2) Sur la base de l'évaluation des risques de cybersécurité visée à l'article 13, paragraphe 2, les produits comportant des éléments numériques doivent, le cas échéant:

   a) être mis à disposition sur le marché sans vulnérabilité exploitable connue;

   b) être mis à disposition sur le marché avec une configuration de sécurité par défaut, sauf accord contraire entre le fabricant et l'entreprise utilisatrice en ce qui concerne un produit sur mesure comportant des éléments numériques, y compris la possibilité de réinitialiser le produit à son état d'origine;

   c) être conçus de façon à ce leurs vulnérabilités puissent être corrigées par des mises à jour de sécurité, y compris, le cas échéant, par des mises à jour automatiques de sécurité régulières activées par défaut, mais faciles à désactiver, par la communication aux utilisateurs des mises à jour disponibles et par la possibilité de les différer temporairement;

d) assurer la protection contre les accès non autorisés par des mécanismes de contrôle appropriés, y compris, mais sans s'y limiter, par des systèmes d'authentification, d'identité ou de gestion des accès et signaler tout accès non autorisé;

e) protéger la confidentialité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, par exemple en chiffrant les données pertinentes au repos ou en transit au moyen de mécanismes de pointe et par d'autres moyens techniques;

f) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur et signaler les corruptions;

g) ne traiter que les données, à caractère personnel ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité prévue du produit comportant des éléments numériques (minimisation des données);

h) protéger la disponibilité des fonctions essentielles et de base, notamment après un incident, y compris par des mesures de résilience et d'atténuation face aux attaques par déni de service;

i) réduire au maximum les répercussions négatives générées par les produits eux-mêmes ou par les appareils connectés sur la disponibilité des services fournis par d'autres dispositifs ou réseaux;

j) être conçus, développés et fabriqués de manière à limiter les surfaces d'attaque, y compris les interfaces externes;

k) être conçus, développés et fabriqués de manière à réduire les répercussions d'un incident, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles;

l) fournir des informations relatives à la sécurité en enregistrant et en surveillant les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions, tout en laissant à l'utilisateur la possibilité de désactiver le mécanisme;

m) donner aux utilisateurs la possibilité de supprimer facilement, en toute sécurité et de manière permanente toutes les données et tous les paramètres et, lorsque ces données peuvent être transférées vers d'autres produits ou systèmes, veiller à ce que cela puisse se faire de manière sécurisée.

Partie II Exigences relatives à la gestion des vulnérabilités

Les fabricants des produits comportant des éléments numériques:

1) recensent et documentent les vulnérabilités et les composants des produits, notamment par l'établissement d'une nomenclature des logiciels dans un format couramment utilisé et lisible par machine couvrant au moins les dépendances de niveau supérieur des produits;

2) gèrent et corrigent sans retard les vulnérabilités qui touchent les produits comportant des éléments numériques, y compris par des mises à jour de sécurité; lorsque cela est techniquement possible, de nouvelles mises à jour de sécurité sont fournies séparément des mises à jour de fonctionnalité;

3) soumettent régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficaces;

4) dès la publication d'une mise à jour de sécurité, communiquent sur les vulnérabilités corrigées, en publiant notamment une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit comportant des éléments numérique concerné, les conséquences de ces vulnérabilités, leur gravité et des informations claires et accessibles aidant les utilisateurs à y remédier; dans des cas dûment justifiés, lorsque les fabricants considèrent que les risques pour la sécurité liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent retarder la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif adapté;

5) mettent en place et appliquent une politique de divulgation coordonnée des vulnérabilités;

6) prennent des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques ainsi que des composants tiers contenus dans ces produits, y compris en fournissant une adresse de contact pour le signalement des vulnérabilités découvertes dans les produits concernés;

7) prévoient des mécanismes de distribution sécurisée des mises à jour pour les produits comportant des éléments numériques afin de garantir que les vulnérabilités soient corrigées ou atténuées rapidement et, le cas échéant, automatisent les mises à jour de sécurité;

8) veillent à ce que, lorsque des correctifs ou des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité constatés, ils soient diffusés sans retard et, sauf accord contraire entre un fabricant et un utilisateur professionnel en ce qui concerne un produit sur mesure comportant des éléments numériques, gratuitement et accompagnées de messages consultatifs fournissant aux utilisateurs les informations pertinentes, y compris sur les éventuelles mesures à prendre.

ANNEXE II

INFORMATIONS ET INSTRUCTIONS DESTINÉES À L'UTILISATEUR

Le produit comportant des éléments numériques doit au moins être accompagné des informations et instructions suivantes:

1) le nom, la raison sociale ou la marque déposée du fabricant et l'adresse postale, l'adresse électronique ou tout autre contact numérique ainsi que, le cas échéant, le site internet sur lequel le fabricant peut être contacté;

2) le point de contact unique où les informations sur les vulnérabilités du produit comportant des éléments numériques peuvent être signalées et reçues, et où peut être trouvée la politique du fabricant en matière de divulgation coordonnée des vulnérabilités;

3) nom et type, ainsi que toute information supplémentaire permettant l'identification unique du produit comportant des éléments numériques;

4) l'utilisation prévue du produit comportant des éléments numériques, y compris l'environnement de sécurité fourni par le fabricant, ainsi que les fonctionnalités essentielles du produit et les informations sur ses propriétés de sécurité;

5) toutes circonstances connues ou prévisibles liées à l'utilisation du produit comportant des éléments numériques conformément à son utilisation prévue ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques de cybersécurité importants;

6) le cas échéant, l'adresse internet à laquelle la déclaration UE de conformité peut être consultée;

7) le type d'assistance technique en matière de sécurité proposé par le fabricant et la date de fin de la période d'assistance pendant laquelle les utilisateurs peuvent s'attendre à recevoir des mises à jour de sécurité;

8) des instructions détaillées ou une adresse internet renvoyant à des instructions détaillées et informations sur:

   a) les mesures nécessaires lors de la mise en service initiale du produit comportant des éléments numériques et pendant toute sa durée de vie pour assurer sa sécurité d'utilisation;

   b) la façon dont les modifications apportées au produit comportant des éléments numériques peuvent affecter la sécurité des données;

   c) la façon dont les mises à jour pertinentes pour la sécurité peuvent être installées;

   d) la mise hors service sécurisée du produit comportant des éléments numériques, en ce compris des informations sur la manière dont les données utilisateur peuvent être supprimées en toute sécurité;

   e) la manière dont le réglage par défaut permettant l'installation automatique des mises à jour de sécurité, conformément à l'annexe I, partie I, point c), peut être désactivé;

   f) lorsque le produit comportant des éléments numériques est destiné à être intégré dans d'autres produits comportant des éléments numériques, les informations nécessaires à l'intégrateur pour se conformer aux exigences essentielles de cybersécurité énoncées à l'annexe I et aux exigences en matière de documentation énoncées à l'annexe VII;

9) lorsque le fabricant décide de mettre à la disposition de l'utilisateur la nomenclature des logiciels, des informations sur l'endroit où celle-ci peut être consultée.

ANNEXE III

PRODUITS IMPORTANTS COMPORTANT DES ÉLÉMENTS NUMÉRIQUES

Classe I

1. Systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés, dont lecteurs d'authentification et de contrôle d'accès et lecteurs biométriques;

2. navigateurs autonomes et intégrés;

3. gestionnaires de mots de passe;

4. logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants;

5. produits comportant des éléments numériques avec la fonction de réseau privé virtuel (VPN);

6. systèmes de gestion de la qualité;

7. systèmes de gestion des informations et des événements de sécurité (SIEM);

8. gestionnaires de démarrage;

9. infrastructure à clé publique et logiciels d'émission de certificats numériques;

10. interfaces réseau physiques et virtuelles;

11. systèmes d'exploitation;

12. routeurs, modems destinés à la connexion à l'internet et commutateurs;

13. microprocesseurs dotés de fonctionnalités liées à la sécurité;

14. microcontrôleurs dotés de fonctionnalités liées à la sécurité;

15. circuits intégrés spécifiques à l'application (ASIC) et réseaux de portes programmables (FPGA) dotés de fonctionnalités liées à la sécurité;

16. assistants virtuels polyvalents pour maison intelligente;

17. produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes d'alarme;

18. jouets connectés couverts par la directive 2009/48/CE du Parlement européen et du Conseil[1] qui présentent des caractéristiques sociales interactives (par exemple, parler ou filmer) ou qui possèdent des fonctions de localisation;

19. produits portables personnels destinés à être portés ou mis sur un corps humain à des fins de surveillance de la santé (suivi par exemple) et auxquels le règlement (UE) 2017/745 ou le règlement (UE) 2017/746 ne s'appliquent pas, ou produits portables personnels destinés à être utilisés par et pour les enfants.

Classe II

1. Hyperviseurs et systèmes d'exécution de conteneurs prenant en charge l'exécution virtualisée de systèmes d'exploitation et d'environnements similaires;

2. pare-feu, systèmes de détection et de prévention des intrusions;

3. microprocesseurs résistants aux manipulations;

4. microcontrôleurs résistants aux manipulations.

---

[1] Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1).

ANNEXE IV

PRODUITS CRITIQUES COMPORTANT DES ÉLÉMENTS NUMÉRIQUES

1. Dispositifs matériels avec boîtier de sécurité;

2. "passerelles pour compteur intelligent" au sein des systèmes intelligents de mesure tels que définis à l'article 2, paragraphe 23, de la directive (UE) 2019/944 du Parlement européen et du Conseil[1] et autres dispositifs à des fins de sécurité avancées, y compris pour un traitement cryptographique sécurisé;

3. cartes à puce ou dispositifs similaires, y compris éléments sécurisés.

---

[1] Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125).

ANNEXE V

DÉCLARATION UE DE CONFORMITÉ

La déclaration UE de conformité prévue à l'article 28 contient l'ensemble des informations suivantes:

1) nom et type, ainsi que toute information supplémentaire permettant l'identification unique du produit comportant des éléments numériques;

2) nom et adresse du fabricant ou de son mandataire;

3) attestation certifiant que la déclaration UE de conformité est établie sous la seule responsabilité du fournisseur;

4) objet de la déclaration (identification du produit comportant des éléments numériques permettant sa traçabilité et pouvant inclure une photographie);

5) une mention indiquant que l'objet de la déclaration décrit ci-dessus est conforme à la législation d'harmonisation de l'Union applicable;

6) les références de toute norme harmonisée pertinente appliquée ou de toute autre spécification commune ou certification de cybersécurité par rapport auxquelles la conformité est déclarée;

7) le cas échéant, le nom et le numéro de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;

8) informations supplémentaires:

Signé par et au nom de:.....

(date et lieu d'établissement):

(nom, fonction) (signature):

ANNEXE VI

DÉCLARATION UE DE CONFORMITÉ SIMPLIFIÉE

La déclaration UE de conformité simplifiée visée à l'article 13, paragraphe 20, est établie comme suit:

[Nom du fabricant] déclare que le produit comportant des éléments numériques de type [désignation du type de produit comportant un élément numérique] est conforme au règlement (UE) .../... du Parlement européen et du Conseil[1].

Le texte complet de la déclaration UE de conformité est disponible à l'adresse internet suivante:

---

[1] JO: veuillez insérer dans le texte le numéro du règlement figurant dans le document PE-CONS 100/23 (2022/0272 (COD)).

ANNEXE VII

CONTENU DE LA DOCUMENTATION TECHNIQUE

La documentation technique visée à l'article 31 contient au moins les informations ci-après, selon le produit comportant des éléments numériques concerné:

1) une description générale du produit comportant des éléments numériques, y compris:

   a) l'utilisation prévue;

   b) les versions de logiciel ayant des incidences sur la conformité aux exigences essentielles de cybersécurité;

   c) lorsque le produit comportant des éléments numériques est un produit matériel, des photographies ou des illustrations montrant les caractéristiques extérieures, le marquage et la disposition intérieure;

   d) les informations et instructions destinées à l'utilisateur figurant à l'annexe II;

2) une description de la conception, du développement et de la fabrication du produit comportant des éléments numériques et des processus de gestion des vulnérabilités, y compris:

   a) les informations nécessaires sur la conception et le développement du produit comportant des éléments numériques, y compris, le cas échéant, des dessins et des schémas et/ou une description de l'architecture du système expliquant comment les composants logiciels s'appuient les uns sur les autres ou s'alimentent et s'intègrent dans le traitement global;

b) les informations et spécifications nécessaires concernant le processus de gestion des vulnérabilités mis en place par le fabricant, en ce compris la nomenclature des logiciels, la politique coordonnée de divulgation des vulnérabilités, la preuve de la fourniture d'une adresse de contact pour le signalement des vulnérabilités et une description des solutions techniques choisies pour la distribution sécurisée des mises à jour;

c) les informations et spécifications nécessaires concernant les processus de production et de suivi du produit comportant des éléments numériques et la validation de ces processus;

3) une évaluation des risques de cybersécurité sur la base de laquelle le produit comportant des éléments numériques est conçu, développé, produit, livré et entretenu, en vertu de l'article 13, y compris la manière dont les exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, sont applicables;

4) les informations qui ont été prises en compte pour déterminer la période d'assistance en vertu de l'article 13, paragraphe 8, du produit comportant des éléments numériques;

5) une liste des normes harmonisées, appliquées entièrement ou en partie, dont les références ont été publiées au *Journal officiel de l'Union européenne*, des spécifications communes telles que définies à l'article 27 du présent règlement ou des schémas européens de certification de cybersécurité adoptés au titre du règlement (UE) 2019/881, conformément à l'article 27, paragraphe 8, du présent règlement, lorsque ces normes harmonisées, spécifications communes ou schémas européens de certification de cybersécurité n'ont pas été appliqués, une présentation des solutions adoptées pour répondre aux exigences essentielles de cybersécurité énoncées à l'annexe I, parties I et II, y compris une liste des autres spécifications techniques pertinentes appliquées. Dans le cas où des normes harmonisées, spécifications communes ou schémas européens de certifications de cybersécurité ont été appliquées en partie, la documentation technique précise les parties appliquées;

6) les rapports des essais effectués pour vérifier la conformité du produit comportant des éléments numériques et des processus de gestion des vulnérabilités aux exigences essentielles de cybersécurité applicables énoncées à l'annexe I, parties I et II;

7) une copie de la déclaration UE de conformité;

8) le cas échéant, la nomenclature des logiciels, à la suite d'une demande motivée d'une autorité de surveillance du marché, pour autant que celle-ci soit nécessaire pour permettre à cette autorité de vérifier le bon respect des exigences essentielles de cybersécurité énoncées à l'annexe I.

ANNEXE VIII

PROCÉDURES D'ÉVALUATION DE LA CONFORMITÉ

Partie I Procédure d'évaluation de la conformité basée sur le contrôle interne (basée sur le module A)

1. Le contrôle interne correspond à la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations énoncées aux points 2, 3 et 4 de la présente partie, assure et déclare sous sa seule responsabilité que les produits comportant des éléments numériques satisfont à toutes les exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et par laquelle le fabricant satisfait aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II.

2. Le fabricant établit la documentation technique décrite à l'annexe VII.

3. Conception, développement, production et gestion des vulnérabilités des produits comportant des éléments numériques

   Le fabricant prend toutes les mesures nécessaires pour que les processus de conception, de développement, de production et de gestion des vulnérabilités ainsi que leur suivi garantissent la conformité des produits comportant des éléments numériques fabriqués ou développés et des processus mis en place par lui avec les exigences essentielles de cybersécurité énoncées à l'annexe I, parties I et II.

4. Marquage de conformité et déclaration de conformité

4.1. Le fabricant appose le marquage CE sur chaque produit comportant des éléments numériques qui répond aux exigences applicables énoncées dans le présent règlement.

4.2. Le fabricant établit une déclaration UE de conformité écrite pour chaque produit comportant des éléments numériques conformément à l'article 28 et la tient, accompagnée de la documentation technique, à la disposition des autorités nationales pendant dix ans à partir du moment où le produit concerné a été mis sur le marché ou pendant la période d'assistance, la durée la plus longue étant retenue. La déclaration UE de conformité précise le produit comportant des éléments numériques pour lequel elle a été établie. Une copie de la déclaration UE de conformité est mise à la disposition des autorités compétentes sur demande.

5. Mandataires

Les obligations du fabricant énoncées au point 4 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant que les obligations en question soient spécifiées dans le mandat.

Partie II Examen UE de type (basé sur le module B)

1. L'examen UE de type correspond à la partie d'une procédure d'évaluation de la conformité dans laquelle un organisme notifié examine la conception technique et le développement d'un produit comportant des éléments numériques et les processus de gestion des vulnérabilités mis en place par le fabricant, et atteste qu'un produit comportant des éléments numériques satisfait aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et que le fabricant satisfait aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II.

2. L'examen UE de type consiste en une évaluation de l'adéquation de la conception technique et du développement du produit comportant des éléments numériques par un examen de la documentation technique et des preuves visées au point 3, avec examen d'échantillons d'une ou de plusieurs parties critiques du produit (combinaison du type de fabrication et du type de conception).

3. Le fabricant introduit une demande d'examen UE de type auprès d'un seul organisme notifié de son choix.

   Cette demande comporte:

   3.1. le nom et l'adresse du fabricant, ainsi que le nom et l'adresse du mandataire si la demande est introduite par celui-ci;

3.2. une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié;

3.3. la documentation technique, qui permet d'évaluer la conformité du produit comportant des éléments numériques aux exigences essentielles applicables de cybersécurité énoncées à l'annexe I, partie I, et les processus de gestion des vulnérabilités du fabricant énoncés à l'annexe I, partie II, et comprend une analyse et une évaluation adéquates du ou des risques. La documentation technique précise les exigences applicables et couvre, dans la mesure nécessaire à l'évaluation, la conception, la fabrication et le fonctionnement du produit comportant des éléments numériques. La documentation technique contient, le cas échéant, au moins les éléments énoncés à l'annexe VII;

3.4. les preuves à l'appui de l'adéquation des solutions de conception technique et de développement et des processus de gestion des vulnérabilités. Ces preuves mentionnent tous les documents qui ont été utilisés, en particulier lorsque les normes harmonisées ou les spécifications techniques applicables n'ont pas été appliquées dans leur intégralité. Elles comprennent, si nécessaire, les résultats des essais effectués par le laboratoire approprié du fabricant ou par un autre laboratoire d'essai en son nom et sous sa responsabilité.

4. L'organisme notifié:

4.1. examine la documentation technique et les éléments de preuve pour évaluer l'adéquation de la conception technique et du développement du produit comportant des éléments numériques aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et des processus de gestion des vulnérabilités mis en place par le fabricant aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie II;

4.2. vérifie que le ou les échantillons ont été développés ou fabriqués en conformité avec la documentation technique et relève les éléments qui ont été conçus et développés conformément aux dispositions applicables des normes harmonisées ou des spécifications techniques pertinentes, ainsi que les éléments dont la conception et le développement ne s'appuient pas sur les dispositions pertinentes desdites normes;

4.3. effectue ou fait effectuer les examens et les essais appropriés pour vérifier que, si le fabricant a choisi d'appliquer les solutions indiquées dans les normes harmonisées ou les spécifications techniques pertinentes pour les exigences énoncées à l'annexe I, l'application a été faite correctement;

4.4. effectue ou fait effectuer les contrôles et les essais appropriés pour vérifier que, si les solutions indiquées dans les normes harmonisées ou les spécifications techniques pertinentes pour les exigences de l'annexe I n'ont pas été appliquées, les solutions adoptées par le fabricant satisfont aux exigences essentielles de cybersécurité correspondantes;

4.5. convient avec le fabricant de l'endroit où les examens et les essais seront effectués.

5. L'organisme notifié établit un rapport d'évaluation répertoriant les activités effectuées conformément au point 4 et leurs résultats. Sans préjudice de ses obligations vis-à-vis des autorités notifiantes, l'organisme notifié ne divulgue le contenu de ce rapport, en totalité ou en partie, qu'avec l'accord du fabricant.

6. Lorsque le type et les processus de gestion des vulnérabilités satisfont aux exigences essentielles de cybersécurité énoncées à l'annexe I, l'organisme notifié délivre au fabricant une attestation d'examen UE de type. L'attestation contient le nom et l'adresse du fabricant, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du type et des processus de gestion des vulnérabilités approuvés. Une ou plusieurs annexes peuvent être jointes à l'attestation.

L'attestation et ses annexes contiennent toutes les informations nécessaires pour permettre l'évaluation de la conformité des produits comportant des éléments numériques fabriqués ou développés au type examiné et des processus de gestion des vulnérabilités à évaluer et pour permettre un contrôle en service.

Lorsque le type et les processus de gestion des vulnérabilités ne satisfont pas aux exigences essentielles de cybersécurité applicables énoncées à l'annexe I, l'organisme notifié refuse de délivrer une attestation d'examen UE de type et en informe le demandeur, en lui précisant les raisons de son refus.

7. L'organisme notifié suit l'évolution de l'état de la technique généralement reconnu, et lorsque cette évolution donne à penser que le type et les processus de gestion des vulnérabilités approuvés pourraient ne plus être conformes aux exigences essentielles de cybersécurité applicables énoncées à l'annexe I, il détermine si des examens complémentaires sont nécessaires. Si tel est le cas, l'organisme notifié en informe le fabricant.

Le fabricant informe l'organisme notifié qui détient la documentation technique relative à l'attestation d'examen UE de type de toutes les modifications du type et des processus de gestion des vulnérabilités approuvés qui peuvent remettre en cause la conformité aux exigences essentielles de cybersécurité énoncées à l'annexe I, ou les conditions de validité de l'attestation. Ces modifications nécessitent une nouvelle approbation sous la forme d'un complément à l'attestation initiale d'examen UE de type.

8. L'organisme notifié effectue périodiquement des audits afin de s'assurer que les processus de traitement des vulnérabilités décrits à l'annexe I, partie II, sont mis en œuvre de manière adéquate.

9. Chaque organisme notifié informe ses autorités notifiantes des attestations d'examen UE de type et des compléments qu'il a délivrés ou retirés et leur transmet, périodiquement ou sur demande, la liste des attestations et des compléments qu'il a refusés, suspendus ou soumis à d'autres restrictions.

Chaque organisme notifié informe les autres organismes notifiés des attestations d'examen UE de type ou des compléments qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions et, sur demande, des attestations et des compléments qu'il a délivrés.

La Commission, les États membres et les autres organismes notifiés peuvent, sur demande, obtenir une copie des attestations d'examen UE de type et de leurs compléments. Sur demande, la Commission et les États membres peuvent obtenir une copie de la documentation technique et des résultats des examens réalisés par l'organisme notifié. L'organisme notifié conserve une copie de l'attestation d'examen UE de type, de ses annexes et compléments, ainsi que le dossier technique, y compris la documentation communiquée par le fabricant, jusqu'à la fin de la validité de ladite attestation.

10. Le fabricant tient à la disposition des autorités nationales une copie de l'attestation d'examen UE de type, de ses annexes et compléments, ainsi que la documentation technique, pour une durée de dix ans à partir du moment où le produit comportant des éléments numériques a été mis sur le marché ou pendant la période d'assistance, la plus longue des deux durées étant retenue.

11. Le mandataire du fabricant peut introduire la demande visée au point 3 et s'acquitter des obligations énoncées aux points 7 et 10 pour autant que lesdites obligations soient spécifiées dans le mandat.

Partie III Conformité au type sur la base du contrôle interne de la fabrication (basée sur le module C)

1. La conformité au type sur la base du contrôle interne de la fabrication correspond à la partie de la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations énoncées aux points 2 et 3 de la présente partie, et garantit et déclare que les produits comportant des éléments numériques concernés sont conformes au type décrit dans l'attestation d'examen UE de type et satisfont aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et que lui-même respecte les exigences essentielles de cybersécurité énoncées à l'annexe I, partie II.

2. Production

Le fabricant prend toutes les mesures nécessaires pour que la production et le suivi de celle-ci garantissent la conformité des produits comportant des éléments numériques fabriqués au type approuvé décrit dans l'attestation d'examen UE de type et aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et que lui-même respecte les exigences essentielles énoncées à l'annexe I, partie II.

3. Marquage de conformité et déclaration de conformité

3.1. Le fabricant appose le marquage CE sur chaque produit comportant des éléments numériques conforme au type décrit dans l'attestation d'examen UE de type et satisfait aux exigences de cybersécurité applicables énoncées dans l'instrument législatif.

3.2. Le fabricant établit une déclaration écrite de conformité concernant un modèle de produit et la tient à la disposition des autorités nationales pendant une durée de dix ans à partir du moment où le produit comportant des éléments numériques a été mis sur le marché ou pendant la période d'assistance, la durée la plus longue étant retenue. La déclaration de conformité précise le modèle de produit pour lequel elle a été établie. Une copie de la déclaration de conformité est mise à la disposition des autorités compétentes sur demande.

4. Mandataire

Les obligations du fabricant énoncées au point 3 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant que lesdites obligations soient spécifiées dans le mandat.

Partie IV Conformité sur la base de l'assurance complète de la qualité (basée sur le module H)

1. La conformité sur la base de l'assurance complète de la qualité correspond à la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations énoncées aux points 2 et 5 de la présente partie, et garantit et déclare sous sa seule responsabilité que les produits comportant des éléments numériques (ou catégories de produits) concernés satisfont aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et que les processus de gestion des vulnérabilités mis en place par le fabricant satisfont aux exigences énoncées à l'annexe I, partie II.

2. Conception, développement, production et gestion des vulnérabilités des produits comportant des éléments numériques.

Le fabricant applique un système de qualité approuvé, tel que spécifié au point 3, pour la conception, le développement et l'inspection finale et l'essai des produits comportant des éléments numériques concernés et pour la gestion des vulnérabilités, maintient son efficacité tout au long de la période d'assistance des produits concernés et fait l'objet d'une surveillance, tel que spécifié au point 4.

3. Système de qualité

3.1. Le fabricant introduit, auprès d'un organisme notifié de son choix, une demande d'évaluation de son système de qualité pour les produits comportant des éléments numériques concernés.

Cette demande comporte:

– le nom et l'adresse du fabricant, ainsi que le nom et l'adresse du mandataire si la demande est introduite par celui-ci;

– la documentation technique, pour un modèle de chaque catégorie de produits comportant des éléments numériques destinés à être fabriqués ou développés. La documentation technique contient, le cas échéant, au minimum, les éléments énoncés à l'annexe VII;

– la documentation relative au système de qualité; et

– une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de qualité garantit la conformité des produits comportant des éléments numériques avec les exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, et la conformité des processus de gestion des vulnérabilités mis en place par le fabricant avec les exigences énoncées à l'annexe I, partie II.

Tous les éléments, exigences et dispositions adoptés par le fabricant sont réunis de manière systématique et ordonnée dans une documentation sous la forme de mesures, de procédures et d'instructions écrites. Cette documentation relative au système de qualité facilite une interprétation homogène des programmes, des plans, des manuels et des dossiers concernant la qualité.

Elle contient en particulier une description adéquate des éléments suivants:

– les objectifs de qualité, l'organigramme ainsi que les responsabilités et les compétences du personnel d'encadrement en matière de qualité de la conception, du développement et des produits, ainsi que de gestion des vulnérabilités;

– les spécifications de la conception technique et du développement, y compris les normes, qui seront appliquées et, lorsque les normes harmonisées ou les spécifications techniques pertinentes ne sont pas appliquées intégralement, les moyens qui seront utilisés pour faire en sorte de respecter les exigences essentielles de cybersécurité énoncées à l'annexe I, partie I, qui s'appliquent aux produits comportant des éléments numériques;

– les spécifications des procédures, y compris les normes, qui seront appliquées et, lorsque les normes harmonisées ou les spécifications techniques pertinentes ne sont pas appliquées intégralement, les moyens qui seront utilisés pour faire en sorte de respecter les exigences essentielles de cybersécurité énoncées à l'annexe I, partie II, qui s'appliquent au fabricant;

– le contrôle de la conception et du développement, ainsi que les techniques de vérification de la conception et du développement, les procédés et les actions systématiques qui seront utilisés lors de la conception et du développement des produits comportant des éléments numériques appartenant à la catégorie couverte;

– les techniques correspondantes de production, de contrôle de la qualité et d'assurance de la qualité, les procédés et les actions systématiques qui seront utilisés;

– les examens et les essais qui seront effectués avant, pendant et après la production et la fréquence à laquelle ils auront lieu;

– des dossiers de qualité tels que les rapports d'inspection et les données d'essais et d'étalonnage, et les rapports sur la qualification du personnel concerné;

– les moyens de surveillance permettant de contrôler l'obtention de la qualité requise en matière de conception et de produit et le bon fonctionnement du système de qualité.

3.3. L'organisme notifié évalue le système de qualité pour déterminer s'il répond aux exigences visées au point 3.2.

Il présume la conformité à ces exigences pour les éléments du système de qualité qui sont conformes aux spécifications correspondantes de la norme nationale transposant la norme harmonisée applicable ou la spécification technique.

L'équipe d'auditeurs doit posséder une expérience des systèmes de gestion de la qualité et comporter au moins un membre ayant de l'expérience en tant qu'évaluateur dans le groupe de produits et la technologie concernés, ainsi qu'une connaissance des exigences applicables énoncées dans le présent règlement. L'audit comprend une visite d'évaluation dans les installations du fabricant, si de telles installations existent. L'équipe d'auditeurs examine la documentation technique visée au point 3.1, deuxième tiret, afin de vérifier la capacité du fabricant à déterminer les exigences applicables énoncées dans le présent règlement et à réaliser les examens nécessaires en vue de garantir la conformité du produit comportant des éléments numériques à ces exigences.

La décision est notifiée au fabricant ou à son mandataire.

La notification contient les conclusions de l'audit et la décision d'évaluation motivée.

3.4. Le fabricant s'engage à remplir les obligations découlant du système de qualité tel qu'il est approuvé et à faire en sorte qu'il demeure adéquat et efficace.

3.5. Le fabricant informe l'organisme notifié ayant approuvé le système de qualité de tout projet de modification de celui-ci.

L'organisme notifié examine les modifications envisagées et décide si le système de qualité modifié continuera de répondre aux exigences énoncées au point 3.2 ou si une nouvelle évaluation s'impose.

Il notifie sa décision au fabricant. La notification contient les conclusions de l'examen et la décision d'évaluation motivée.

4. Surveillance sous la responsabilité de l'organisme notifié

4.1. Le but de la surveillance est de s'assurer que le fabricant remplit correctement les obligations découlant du système de qualité approuvé.

4.2. Le fabricant autorise l'organisme notifié à accéder, à des fins d'évaluation, aux lieux de conception, de développement, de production, d'inspection, d'essai et de stockage et lui fournit toutes les informations nécessaires, notamment:

– la documentation sur le système de qualité;

– les dossiers de qualité prévus dans la partie du système de qualité consacrée à la conception, tels que les résultats des analyses, des calculs et des essais;

– les dossiers de qualité prévus par la partie du système de qualité consacrée à la fabrication, tels que les rapports d'inspection, les données d'essais et d'étalonnage et les rapports sur la qualification du personnel concerné.

4.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fabricant maintient et applique le système de qualité, et il transmet un rapport d'audit au fabricant.

5. Marquage de conformité et déclaration de conformité

5.1. Sur chaque produit comportant des éléments numériques qui satisfait aux exigences énoncées à l'annexe I, partie I, du présent règlement, le fabricant doit apposer le marquage CE et, sous la responsabilité de l'organisme notifié visé au point 3.1, le numéro d'identification de ce dernier.

5.2. Le fabricant établit une déclaration écrite de conformité concernant chaque modèle de produit et la tient à la disposition des autorités nationales pendant une durée de dix ans à partir du moment où le produit comportant des éléments numériques a été placé sur le marché ou pendant la période d'assistance, la durée la plus longue étant retenue. La déclaration de conformité précise le modèle de produit pour lequel elle a été établie.

Une copie de la déclaration de conformité est mise à la disposition des autorités compétentes sur demande.

6. Pendant une période d'au moins dix ans à compter de la mise sur le marché du produit comportant des éléments numériques ou pendant la période d'assistance, la durée la plus longue étant retenue, le fabricant doit tenir à la disposition des autorités nationales:

6.1. la documentation technique visée au point 3.1;

6.2. la documentation concernant le système de qualité visée au point 3.1;

6.3. les modifications approuvées visées au point 3.5;

6.4. les décisions et rapports de l'organisme notifié visés aux points 3.5 et 4.3.

7. Chaque organisme notifié informe ses autorités notifiantes des approbations de systèmes de qualité délivrées ou retirées et leur transmet, périodiquement ou sur demande, la liste des approbations qu'il a refusées, suspendues ou soumises à d'autres restrictions.

Chaque organisme notifié informe les autres organismes notifiés des approbations de systèmes de qualité qu'il a refusées, suspendues ou retirées et, sur demande, des approbations qu'il a délivrées.

8. Mandataire

Les obligations du fabricant visées aux points 3.1, 3.5, 5 et 6 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant que lesdites obligations soient spécifiées dans le mandat.

Une déclaration a été faite en ce qui concerne le présent acte et figure au … [*JO: veuillez insérer la référence au JO: JO C, ..., ELI: ...*] et à l'adresse suivante: … [*JO: veuillez insérer le lien vers la déclaration*].