EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

9 novembre 2022

Avis 23/2022

sur la proposition de règlement du Parlement européen et du Conseil relatif aux exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

edps.europa.eu

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Rafał Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

*Conformément à l'**article 42, paragraphe 1**, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le [CEPD] en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».*

Le présent avis porte sur la proposition de la Commission pour un règlement du Parlement européen et du Conseil sur les exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020. Le présent avis n'exclut pas que le CEPD formule à l'avenir des observations ou des recommandations supplémentaires, notamment si d'autres problèmes sont identifiés ou si de nouvelles informations sont disponibles. En outre, le présent avis est sans préjudice de toute action future que pourrait entreprendre le CEPD dans l'exercice des pouvoirs que lui confère le règlement (UE) 2018/1725. Le présent avis se limite aux dispositions du projet de proposition pertinentes en matière de protection des données.

Résumé

Le 15 septembre 2022, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil relatif aux exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 (ci-après la «proposition»).

Le CEPD se félicite de la proposition et soutient pleinement son objectif général d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme pour les exigences essentielles de cybersécurité pour la mise sur le marché de l'Union de produits comportant des éléments numériques.

Le CEPD rappelle que l'article 5, paragraphe 1, point f), du RGPD pose la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément l'obligation – applicable tant aux responsables du traitement qu'aux sous-traitants – de garantir un niveau de sécurité approprié. Par conséquent, le CEPD se félicite que les principes de sécurité et de minimisation des données soient déjà intégrés dans les exigences essentielles de cybersécurité énumérées à l'annexe I de la proposition. En outre, le CEPD recommande vivement d'inclure le principe de protection des données dès la conception et par défaut dans les exigences essentielles de cybersécurité des produits comportant des éléments numériques.

Le considérant 17 prévoit des dispositions de gouvernance très importantes qui ne sont pas reflétées dans la partie opérationnelle de la proposition. Par conséquent, le CEPD recommande de préciser dans la partie opérationnelle de la proposition tous les aspects liés à la création de synergies à la fois sur la normalisation et la certification en matière de cybersécurité, ainsi que les synergies entre cette proposition et la législation de l'Union sur la protection des données dans le domaine de la surveillance du marché et de l'application. En outre, le CEPD considère qu'il est nécessaire de préciser que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments.

Le CEPD se félicite que cette disposition reconnaisse que le traitement des données à caractère personnel est une fonction critique et sensible et pourrait, à ce titre, exiger que les produits critiques correspondants comportant des éléments numériques obtiennent un certificat européen de cybersécurité dans le cadre d'un système européen de certification de cybersécurité. En même temps, le CEPD recommande de préciser dans un considérant de la proposition que l'obtention d'une certification européenne de cybersécurité en vertu de la proposition ne garantit pas la conformité avec le RGPD.

Enfin, le CEPD se félicite des sanctions proposées, qui sont similaires à celles du RGPD en cas de violation de l'article 32 du RGPD sur la sécurité du traitement, avec une amende maximale de 2,5 % du chiffre d'affaires annuel mondial. En conséquence, la proposition pourrait servir d'autre forme

de protection pour les individus qui résident dans les États membres de l'UE, en conjonction avec les dispositions du RGPD.

Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne,

vu le 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 («RPDUE»)[1], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 15 septembre 2022, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil relatif aux exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 (ci-après la «proposition»).

2. L'objectif de la proposition est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme pour les exigences essentielles en matière de cybersécurité pour la mise sur le marché de l'Union de produits comportant des éléments numériques[2]. En particulier, la proposition vise à établir les conditions limites pour le développement de produits sûrs comportant des éléments numériques en garantissant 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. Elle vise également à créer les conditions permettant aux utilisateurs de tenir compte de la cybersécurité lorsqu'ils choisissent et utilisent des produits comportant des éléments numériques[3].

3. À cette fin, la proposition prévoit ce qui suit[4]:

   - des règles pour la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;

   - des exigences essentielles pour la conception, le développement et la production de produits comportant des éléments numériques, et des obligations pour les opérateurs économiques en ce qui concerne la cybersécurité de ces produits;

   - des exigences essentielles pour les processus de traitement des vulnérabilités mis en place par les fabricants afin de garantir la cybersécurité des produits comportant

[1] JO L 295 du 21.11.2018, p. 39.
[2] Considérant 1 de la proposition.
[3] Considérant 2 de la proposition.
[4] Article 1 de la proposition.

des éléments numériques tout au long de leur cycle de vie, et des obligations pour les opérateurs économiques en ce qui concerne ces processus;

- des règles relatives à la surveillance du marché et à l'application des règles et exigences susmentionnées.

4. Le cadre européen comprend plusieurs textes législatifs horizontaux qui couvrent certains aspects liés à la cybersécurité sous différents angles (produits, services, gestion de crise et infractions). En 2013, la directive relative aux attaques contre les systèmes d'information[5], harmonisant l'incrimination et les sanctions pour un certain nombre d'infractions dirigées contre les systèmes d'information, est entrée en vigueur. En août 2016, la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (directive NIS)[6] est entrée en vigueur en tant que premier texte législatif de l'UE sur la cybersécurité. Sa révision, qui a donné naissance à la directive NIS2, relève le niveau d'ambition commun de l'UE en matière de cybersécurité des services TIC. En 2019, la loi européenne sur la cybersécurité[7] est entrée en vigueur; elle vise à renforcer la sécurité des produits TIC, des services TIC et des processus TIC en introduisant un cadre européen volontaire de certification de la cybersécurité.

5. Le présent avis est émis par le CEPD en réponse à une demande de consultation présentée par la Commission européenne le 15 septembre 2022, en vertu de l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au considérant 71 de la proposition. À cet égard, le CEPD note également avec satisfaction qu'il a déjà été préalablement consulté de manière informelle, conformément au considérant 60 du RPDUE.

2. Observations générales

6. Le CEPD se félicite de la proposition et soutient pleinement son objectif général d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme pour les exigences essentielles de cybersécurité pour la mise sur le marché de l'Union de produits comportant des éléments numériques.

7. La proposition prévoit que les produits comportant des éléments numériques ne seront mis à disposition sur le marché que s'ils répondent à des exigences essentielles spécifiques en matière de cybersécurité pour la conception, le développement et la production de ces produits. En outre, la proposition établit des obligations pour les opérateurs économiques en ce qui concerne la cybersécurité de ces produits. Par exemple, elle exige que les fabricants tiennent compte de la cybersécurité dans la conception et le développement des produits comportant des éléments numériques.

[5] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8-14).
[6] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194/1 du 19.7.2016, p. 1.
[7] 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.

8. Alors que la directive NIS2 incluait dans son champ d'application les opérateurs de services essentiels et les fournisseurs de services numériques afin d'établir un niveau commun élevé de cybersécurité de leurs systèmes TIC, la proposition à l'examen introduirait des règles communes de cybersécurité pour les fabricants et les développeurs de produits avec des éléments numériques, couvrant à la fois le matériel et les logiciels. Le CEPD note que de tels produits peuvent être intégrés dans les systèmes TIC des fournisseurs de services numériques, agissant en tant qu'entités au titre de la directive NIS2 et peuvent être utilisés par des individus qui utilisent des services numériques, tels que des téléphones mobiles, des ordinateurs personnels, des systèmes d'exploitation et des applications logicielles. Dans ce contexte, le CEPD rappelle son avis sur la stratégie de cybersécurité et la directive NIS 2.0[8].

9. Conformément à l'exposé des motifs[9] les exigences horizontales en matière de cybersécurité:

   - contribueraient à la sécurité des données à caractère personnel en protégeant la confidentialité, l'intégrité et la disponibilité des informations dans les produits comportant des éléments numériques.

   - faciliteront le respect de l'exigence de sécurité du traitement des données à caractère personnel en vertu du RGPD.

   - amélioreraient la transparence et l'information des utilisateurs, y compris ceux qui pourraient être moins bien équipés en matière de cybersécurité. Les utilisateurs seraient également mieux informés des risques, des capacités et des limites des produits comportant des éléments numériques, ils seraient ainsi plus à même de prendre les mesures de prévention et d'atténuation nécessaires pour réduire les risques résiduels.

10. Le CEPD rappelle que l'article 5, paragraphe 1, point f), du RGPD pose la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément l'obligation – applicable tant aux responsables du traitement qu'aux sous-traitants – de garantir un niveau de sécurité approprié. Par conséquent, le CEPD se félicite que les principes de sécurité et de minimisation des données soient déjà intégrés dans les exigences essentielles de cybersécurité énumérées à l'annexe I de la proposition.

11. La cybersécurité des produits comportant des éléments numériques qui sont utilisés par des particuliers est de la plus haute importance pour protéger leurs droits et libertés, en particulier le droit à la vie privée, et pour renforcer leur confiance dans les services numériques. Sans ces exigences, les particuliers peuvent être victimes d'attaques de cybersécurité visant à accéder à leurs données à caractère personnel et à leurs communications confidentielles.

12. C'est pourquoi le CEPD considère que l'établissement d'un cadre juridique uniforme pour les exigences essentielles en matière de cybersécurité pour la mise en place de produits avec des éléments numériques est très important pour la sauvegarde des droits et libertés fondamentaux, y compris les droits à la vie privée et à la protection des données à caractère

[8] Avis 5/2021 du CEPD sur la stratégie en matière de cybersécurité et la directive SRI 2.0, émis le 11 mars 2021
[9] COM(2022) 454 final, p. 8.

personnel, et soutient fermement la proposition d'un ensemble complet de mesures techniques et organisationnelles appropriées et efficaces.

13. En outre, le CEPD rappelle que l'article 25 du RGPD énonce le principe de la protection des données dès la conception et par défaut, qui vise à intégrer la protection des données et de la vie privée dans la conception des opérations de traitement et des systèmes d'information, avant même que le traitement n'ait lieu, et à garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires à chaque finalité spécifique du traitement sont traitées. En pratique, ce principe exige, entre autres, l'utilisation de technologies renforçant la protection de la vie privée, telles que le cryptage et la pseudonymisation. Les dispositions du RGPD indiquent clairement que la sécurité et la protection des données dès la conception et par défaut sont essentielles au respect de la législation européenne en matière de protection des données.

14. En ce qui concerne les produits comportant des éléments numériques, le rôle des fabricants se limite généralement à fournir le produit aux particuliers. Le RGPD n'impose pas directement d'exigences aux fabricants, mais les «encourage» seulement, au considérant 78 du RGPD, «*à prendre en compte le droit à la protection des données lors du développement et de la conception de ces produits, services et applications et, en tenant dûment compte de l'état de l'art, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de remplir leurs obligations en matière de protection des données*». Néanmoins, il est clair que les utilisateurs finiront par renoncer à un produit si son utilisation les empêche, en tant que responsables du traitement, de respecter les exigences en matière de protection des données. Cela crée une «obligation» indirecte pour les fabricants de concevoir leurs produits de manière à ce que les utilisateurs soient en mesure d'adhérer aux exigences du RGPD lors du traitement des données à l'avenir.

15. Par conséquent, malgré le fait que le RGPD ne s'adresse pas directement aux fabricants de produits comportant des éléments numériques, mais uniquement aux responsables du traitement lorsque ces produits sont intégrés dans leurs systèmes TIC, il est essentiel que le principe de la protection des données par conception et par défaut soit également appliqué aux produits. D'une part, cela faciliterait la conformité des responsables du traitement avec le principe de la protection des données dès la conception et par défaut et d'autre part, cela garantirait la protection en bonne et due forme des données à caractère personnel des personnes utilisant ces produits pour accéder aux services numériques. Par conséquent, le CEPD recommande vivement d'inclure le principe de protection des données dès la conception et par défaut dans les exigences essentielles de cybersécurité des produits comportant des éléments numériques.

3. Champ d'application de la proposition

16. Le vaste champ d'application de la proposition couvre tous les produits comportant des éléments numériques, et plus précisément *«tout produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels devant*

être mis sur le marché séparément»[10] ... «*dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte de données logiques ou physiques à un dispositif ou à un réseau*»[11]. Cela comprend à la fois les produits qui peuvent être connectés physiquement via des interfaces matérielles et les produits qui sont connectés logiquement, par exemple via des prises de réseau, des tuyaux, des fichiers, des interfaces de programmation d'applications et tout autre type d'interface logicielle.

17. Le CEPD comprend que les produits avec des éléments numériques entrant dans le champ d'application de la proposition peuvent être intégrés dans les systèmes TIC des responsables du traitement[12] et peuvent être utilisés par les individus[13] afin d'accéder aux services de traitement des données à caractère personnel fournis par les responsables du traitement.

18. Dans ce contexte, le CEPD recommande d'expliquer dans le préambule de la proposition l'importance des produits comportant des éléments numériques qui effectuent des opérations cryptographiques[14] y compris le cryptage au repos et en transit et la pseudonymisation qui sont nécessaires pour une sécurité de l'information efficace, la cybersécurité, la protection des données et la vie privée. En outre, conformément au considérant 26 de la proposition, il recommande également d'ajouter à l'annexe II les produits matériels et immatériels comportant des éléments numériques qui effectuent des opérations de cryptage.

19. Le CEPD note que certains produits et services numériques soumis à une législation sectorielle n'entrent pas dans le champ d'application de la proposition. Il s'agit notamment des logiciels en tant que service, des dispositifs médicaux, des dispositifs médicaux de diagnostic in vitro, des véhicules à moteur, des produits utilisés exclusivement à des fins de sécurité nationale ou militaires ou conçus spécifiquement pour traiter des informations classifiées.

20. Néanmoins, les dispositions relatives à la sécurité de certaines législations sectorielles exclues du champ d'application de la proposition ne sont pas toujours aussi détaillées et concrètes que celles de la proposition elle-même. C'est le cas du règlement (UE) 2017/745[15] qui établit des mesures de sécurité générales pour les dispositifs médicaux, mais n'exige pas que les dispositifs soient livrés sans vulnérabilités connues ou qu'ils chiffrent les données pertinentes au repos ou en transit selon les mécanismes de l'état de l'art. En outre, le même règlement prévoit l'obligation d'*«établir, mettre en œuvre, documenter et maintenir un système de gestion des risques»*. Cependant, il n'est pas clair si ce système couvrira également les aspects liés à la cybersécurité et à la protection des données. En conséquence,

---

[10] L'article 3, paragraphe 1, de la proposition dispose que: «produit comportant des éléments numériques»: tout produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels devant être mis sur le marché séparément.

[11] L'article 3, paragraphe 2, de la proposition dispose que: «Le présent règlement s'applique aux produits comportant des éléments numériques dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte de données logiques ou physiques à un dispositif ou à un réseau.»

[12] Par exemple: matériel et système d'exploitation des serveurs, logiciels des serveurs d'applications, logiciels des applications web, etc.

[13] Par exemple: téléphones mobiles, ordinateurs personnels, systèmes d'exploitation, applications logicielles, etc.

[14] Le CEPD rappelle l'impact des bugs découverts dans les produits de cryptage utilisés par les fournisseurs de services et les utilisateurs, tels que «Heartbleed», «POODLE», ainsi que le cas «VeraCrypt».

[15] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1-175).

le CEPD recommande de supprimer le règlement (UE) 2017/745 de la liste des législations exclues de l'application de la proposition.

21. Le CEPD note également que le considérant 15 indique que les exigences essentielles fixées par la proposition «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 relative à la commercialisation des équipements hertziens[16]». Le point e) faisant référence aux données à caractère personnel et à la vie privée, le CEPD recommande de préciser expressément dans la proposition quels sont les éléments des exigences essentielles visées à l'article 3, paragraphe 3, point e), de la directive 2014/53/UE sur les données à caractère personnel et la vie privée.

4. Relation avec la législation existante de l'Union en matière de protection des données à caractère personnel

22. Le CEPD observe que le considérant 17 de la proposition précise qu'elle est *«sans préjudice»* du RGPD et indique que:

- des synergies en matière de normalisation et de certification des aspects liés à la cybersécurité devraient être envisagées dans le cadre de la coopération entre la Commission, les organismes européens de normalisation, l'Agence de l'Union européenne pour la cybersécurité (ENISA), le Comité européen de la protection des données (EDPB) institué par le RGPD et les autorités nationales de contrôle de la protection des données;
- des synergies entre la présente proposition et le droit de l'Union en matière de protection des données devraient également être créées dans le domaine de la surveillance du marché et de l'application de la législation. À cette fin, les autorités nationales de surveillance du marché désignées dans le cadre de la présente proposition devraient coopérer avec les autorités chargées de contrôler le droit de l'Union en matière de protection des données. Ces dernières devraient également avoir accès aux informations pertinentes pour l'accomplissement de leurs tâches.

23. Le CEPD prend note que le considérant 17 prévoit des dispositions de gouvernance très importantes qui ne sont pas reflétées dans le dispositif de la proposition. En outre, la manière dont ces «synergies» pourraient être créées n'est pas détaillée. Le CEPD s'inquiète du fait que de telles synergies sont peu susceptibles de se produire dans la pratique en l'absence de dispositions claires correspondantes. Par conséquent, le CEPD recommande de spécifier dans la partie opérationnelle de la proposition tous les aspects liés à la création de synergies à la fois sur la normalisation et la certification en matière de cybersécurité ainsi que les synergies entre cette proposition et la législation de l'Union sur la protection des données dans le domaine de la surveillance du marché et de l'application de la loi (tels que la coopération structurée entre les organes concernés, les dispositions rendant le

[16] 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, texte présentant de l'intérêt pour l'EEE, JO L 153 du 22.5.2014, p. 62-106.

partage d'informations obligatoire, y compris les données à caractère personnel, dans des cas spécifiques, etc.).

24. En outre, le CEPD considère qu'il est nécessaire de préciser explicitement que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments.

5. Produits numériques critiques pour le traitement des données à caractère personnel et le système européen de cybersécurité

25. Le considérant 39 indique que la proposition vise à créer des synergies avec le règlement (UE) 2019/881 relatif au règlement sur la cybersécurité de l'UE[17] qui établit un cadre européen de certification volontaire de la cybersécurité pour les produits, processus et services TIC.

26. En outre, conformément à l'article 6, paragraphe 5, point b), de la proposition, la Commission est habilitée à adopter des actes délégués afin de préciser les catégories de produits hautement critiques comportant des éléments numériques pour lesquels les fabricants devraient être tenus d'obtenir un certificat de cybersécurité européen dans le cadre d'un système européen de certification de la cybersécurité. Lorsqu'elle détermine ces catégories de produits hautement critiques comportant des éléments numériques, la Commission devrait tenir compte, entre autres, de l'utilisation prévue pour l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel[18].

27. À cet égard, le CEPD se félicite que la proposition reconnaisse que le traitement des données à caractère personnel est une fonction critique et sensible et pourrait, à ce titre, exiger que les produits critiques correspondants comportant des éléments numériques obtiennent un certificat européen de cybersécurité dans le cadre d'un système européen de certification de la cybersécurité. En même temps, le CEPD recommande de préciser dans le préambule que l'obtention d'une certification européenne de cybersécurité en vertu de la proposition ne garantit pas la conformité avec le RGPD.

[17] 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. 15-69).
[18] Article 6, paragraphe 2, point c), de la proposition.

6. Sanctions applicables aux infractions commises par les opérateurs économiques

28. Conformément à la proposition, les États membres établissent des sanctions applicables aux infractions commises par les opérateurs économiques, dont les limites sont fixées comme suit:

    - Le non-respect des exigences essentielles énoncées à l'annexe I et des obligations des fabricants est passible d'amendes administratives pouvant aller jusqu'à 15 millions d'euros ou jusqu'à 2,5 % de son chiffre d'affaires mondial, le montant le plus élevé étant retenu.
    - Le non-respect des autres obligations prévues par la CRA est passible d'amendes administratives pouvant aller jusqu'à 10 millions d'euros ou jusqu'à 2 % des recettes mondiales, le montant le plus élevé étant retenu.

29. Si des informations incorrectes, incomplètes ou trompeuses sont fournies aux organismes notifiés et aux autorités de surveillance du marché en réponse à une demande, le contrevenant est passible d'amendes administratives pouvant atteindre 5 millions d'euros ou 1 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu.

30. Le CEPD se félicite des sanctions proposées, qui sont similaires à celles du RGPD en cas de violation de l'article 32 du RGPD sur la sécurité du traitement, avec une amende maximale de 2,5 % du chiffre d'affaires annuel mondial. En conséquence, la proposition pourrait servir d'autre forme de protection pour les individus qui résident dans les États membres de l'UE, en conjonction avec les dispositions du RGPD.

7. Conclusions

31. À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

(1) inclure le principe de protection des données dès la conception et par défaut dans les exigences essentielles de cybersécurité des produits comportant des éléments numériques;

(2) expliquer dans le préambule l'importance des produits comportant des éléments numériques qui effectuent des opérations cryptographiques, y compris le cryptage au repos et en transit et la pseudonymisation, qui sont nécessaires pour une sécurité de l'information, une cybersécurité, une protection des données et une vie privée efficaces;

(3) ajouter à l'annexe II les produits matériels et immatériels comportant des éléments numériques qui effectuent des opérations cryptographiques;

(4) supprimer le règlement (UE) 2017/745 de la liste des législations exclues de l'application de la proposition;

(5) préciser expressément dans la proposition quels sont les éléments des exigences essentielles visées par l'article 3, paragraphe 3, point e), de la directive 2014/53/UE relative aux données à caractère personnel et à la vie privée;

(6) préciser dans la partie opérationnelle de la proposition tous les aspects pratiques liés à la création de synergies à la fois sur la normalisation et la certification en matière de cybersécurité, ainsi que les synergies entre cette proposition et la législation de l'Union sur la protection des données dans le domaine de la surveillance du marché et de l'application;

(7) préciser que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments;

(8) ajouter des définitions pertinentes des termes «logiciel libre», «logiciel ouvert» et «logiciel libre et ouvert»;

(9) préciser dans le considérant de la proposition que l'obtention d'une certification européenne de cybersécurité en vertu de la proposition ne garantit pas la conformité avec le RGPD.

Bruxelles, le 9 novembre 2022

(signature électronique)
Wojciech Rafał WIEWIÓROWSKI