EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17 mai 2022

Avis 7/2022

sur la proposition de règlement relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

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 Contrôleur européen de la protection des données 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 concerne la proposition de règlement du Parlement européen et du Conseil relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union. Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations supplémentaires, en particulier si d'autres problèmes sont détectés ou si de nouvelles informations apparaissent. En outre, le présent avis est sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont conférés par le règlement (UE) 2018/1725. Le présent avis se limite aux dispositions pertinentes de la proposition en matière de protection des données.

Synthèse

Le 22 mars 2022, la Commission européenne a adopté une proposition de règlement du Parlement européen et du Conseil relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union (la «proposition»).

Le CEPD se félicite de l'objectif de la proposition qui vise à améliorer la sécurité des informations traitées par les institutions de l'Union, en établissant des règles communes en matière de sécurité de l'information et en favorisant une culture cohérente de la sécurité de l'information dans un instrument juridique spécifique.

Le CEPD observe que la sécurité des données à caractère personnel, telle que prescrite par le RPDUE, a une portée qui n'empiète que partiellement sur celle de la sécurité de l'information prévue par la proposition. Cette dernière porte sur la confidentialité des informations, tandis que le RPDUE garantit également l'intégrité et la disponibilité. En outre, les dispositions relatives à la sécurité des données à caractère personnel du RPDUE traitent spécifiquement des risques pour les droits et libertés des personnes physiques.

La proposition exige des institutions de l'Union qu'elles adoptent des mesures de sécurité de l'information, qui impliqueront inévitablement le traitement de données à caractère personnel et de données de communications électroniques, notamment des données relatives au trafic. Le CEPD estime qu'il convient de mettre en évidence le fait que toutes les mesures de sécurité de l'information impliquant le traitement de données à caractère personnel devraient se conformer au cadre juridique actuel en matière de protection des données et de la vie privée et que les institutions de l'Union devraient prendre les garanties techniques et organisationnelles nécessaires pour garantir ce respect de manière responsable.

Afin de garantir la sécurité juridique et la prévisibilité, ainsi que le respect du RPDUE, le CEPD recommande vivement que la proposition, ou à tout le moins un acte délégué qui sera adopté ultérieurement par la Commission, définisse clairement les activités de traitement de données à caractère personnel autorisées aux fins du présent règlement. Le CEPD attire également l'attention sur la nécessité de veiller au respect des dispositions du RPDUE relatives aux transferts de données à caractère personnel vers des pays tiers et des organisations internationales. En outre, le CEPD recommande d'expliquer dans un considérant que toutes les dispositions du RPDUE s'appliqueront, y compris les règles relatives aux transferts internationaux.

Le CEPD souligne l'importance d'intégrer la dimension de la protection de la vie privée et des données dans la gestion de la sécurité de l'information, pour créer des synergies positives entre la proposition et la législation relative à la protection des données et de la vie privée, et fournit des recommandations spécifiques sur la manière de créer de telles synergies, y compris: l'obligation spécifique pour les fonctionnaires de l'Union chargés de la sécurité de l'information de coopérer étroitement avec le délégué à la protection des données désigné conformément à l'article 43 du RPDUE; l'intégration du chiffrement de bout en bout dans la liste des mesures de sécurité minimales de la proposition, le cas échéant, et en particulier dans le cadre de l'échange d'informations sensibles non classifiées; et la promotion d'une procédure intégrée de gestion des

risques liés à la sécurité de l'information et de traitement des incidents qui à la fois garantisse la sécurité de l'information et satisfasse aux obligations en matière de protection des données s'agissant des notifications de violations des données.

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[1], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 22 mars 2022, la Commission européenne a adopté une proposition de règlement du Parlement européen et du Conseil relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union[2] (la «proposition»).

2. Le même jour, la Commission européenne a adopté une autre proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union[3] (la «proposition sur la cybersécurité»).

3. Ces deux propositions avaient été envisagées dans la stratégie de cybersécurité de l'UE pour la décennie numérique présentée le 16 décembre 2020[4] (la «stratégie»). La stratégie visait principalement à renforcer l'autonomie stratégique de l'Union dans les domaines de la cybersécurité et à améliorer sa résilience et sa réponse collective, ainsi qu'à construire un internet ouvert et mondial doté de solides garde-fous pour faire face aux risques pour la sécurité et les libertés et droits fondamentaux des citoyens en Europe[5].

4. La proposition constitue l'une des initiatives réglementaires de la stratégie, en particulier dans le domaine de la cybersécurité des institutions, organes et organismes de l'UE (les «institutions de l'Union»). Selon la stratégie, l'objectif de la proposition est double:

   - faciliter **l'interopérabilité des systèmes d'informations classifiées**, en permettant un transfert sans heurts d'informations entre les différentes entités, et

   - permettre une **approche interinstitutionnelle du traitement des informations classifiées et des informations sensibles non classifiées de l'UE**, qui pourrait également servir de modèle d'interopérabilité entre les États membres, en indiquant que l'UE devrait également développer sa capacité à communiquer de manière sécurisée avec les partenaires concernés, en s'appuyant, dans la mesure du possible, sur les modalités et procédures existantes.

5. Le CEPD fait observer que l'objet de la proposition en question est également directement lié à celui de la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (la «proposition SRI 2.0»). Le CEPD rappelle qu'il a publié l'avis 5/2021 sur la stratégie en matière de cybersécurité[6] et la

directive SRI 2.0 (l'«avis SRI 2.0»)[7]. C'est pourquoi le présent avis fera référence à l'avis SRI 2.0.

6. Selon l'exposé des motifs de la proposition, en raison des volumes toujours plus conséquents d'informations sensibles non classifiées (les «ISNC») et d'informations classifiées de l'Union européenne (les «ICUE») que les institutions de l'Union doivent se partager, et compte tenu de l'évolution spectaculaire des menaces, l'administration européenne est exposée à des attaques dans tous ses domaines d'activité. Les informations traitées par les institutions de l'Union intéressent au plus haut point les acteurs malveillants, et elles doivent être correctement protégées.

7. Selon l'exposé des motifs, la proposition devrait:

   - définir des **catégories d'informations** exhaustives et harmonisées, ainsi que des **règles communes** à toutes les institutions de l'Union;

   - établir un **système rationalisé de coopération** entre les institutions de l'Union **dans le domaine de la sécurité de l'information**, capable de favoriser une culture cohérente de la sécurité de l'information dans l'ensemble de l'administration européenne;

   - **moderniser les politiques en matière de sécurité de l'information** à tous les niveaux de classification/de catégorisation, pour l'ensemble des institutions de l'Union, en tenant compte de la transformation numérique et du développement du télétravail en tant que pratique structurelle.

8. Le 22 mars 2022, la Commission a consulté le Contrôleur européen de la protection des données conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 (le «RPDUE»)[8]. Les observations et recommandations contenues dans le présent avis se limitent aux dispositions les plus pertinentes de la proposition du point de vue de la protection des données et de la vie privée.

2. Observations générales

9. Le CEPD rappelle que la sécurité de l'information, objet de la proposition, fait partie de la législation relative à la protection des données depuis ses débuts. Aujourd'hui, l'article 4, paragraphe 1, point f), du RPDUE pose **la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel**. L'article 33 du RPDUE définit plus précisément les obligations – applicables tant aux responsables du traitement qu'aux sous-traitants – d'**assurer un niveau de sécurité approprié des données à caractère personnel**. Ces deux dispositions indiquent clairement que **la sécurité des données à caractère personnel est essentielle au respect de la législation de l'Union en matière de protection des données.** C'est la raison pour laquelle, d'une part, le présent avis analyse la proposition afin de déterminer si elle établit un système efficace de gestion de la sécurité de l'information ou si elle contient des mesures efficaces pour renforcer la sécurité de l'information, y compris des données à caractère personnel.

10. D'autre part, les mesures de sécurité de l'information renforcent non seulement la sécurité des données à caractère personnel et contribuent à leur protection, mais elles sont

également susceptibles de porter atteinte aux droits et libertés des personnes concernées, en particulier les droits fondamentaux à la protection des données à caractère personnel et à la confidentialité des communications électroniques. Par conséquent, le présent avis analyse également la proposition afin de déterminer si elle prévoit des mesures à prendre, notamment, **sur le fondement d'une base juridique valable, à des fins spécifiques et limitées, et si elles sont appropriées, nécessaires et proportionnées**.

11. Le CEPD prend note du fait que l'objet de la proposition est différent de celui des propositions SRI 2.0 et cybersécurité. Nous comprenons que la cybersécurité est axée sur la protection des réseaux et des systèmes d'information, des utilisateurs de ces systèmes et des autres personnes touchées par les cybermenaces, tandis que **la proposition concerne la sécurité de l'information sous toutes ses formes, et pas seulement les informations traitées par les systèmes informatiques qui sont touchés par des cybermenaces**.

12. Le CEPD tient à souligner que, si pour la proposition SRI 2.0, qui prévoit des obligations pour les États membres, l'application du règlement (UE) 2016/679 (le «RGPD») et de la directive 2002/58/CE (la directive «vie privée et communications électroniques») est pertinente pour le traitement de données à caractère personnel, pour ce qui est de la proposition actuelle, qui établit des règles pour les institutions de l'Union, **le RPDUE s'applique et joue un rôle tout aussi important**.

13. Le CEPD **se félicite** de l'objectif de la proposition qui vise à **améliorer la sécurité des informations traitées par les institutions de l'Union**, en établissant des règles communes en matière de sécurité de l'information et en favorisant une culture cohérente de la sécurité de l'information dans un instrument juridique spécifique.

3. Observations particulières

3.1. Champ d'application de la proposition et relation avec la législation relative à la protection des données et de la vie privée

14. Conformément à l'article 3, point b), de la proposition, on entend par «sécurité de l'information» le fait de garantir l'authenticité, la disponibilité, la confidentialité, l'intégrité et la non-répudiation des informations. Toutefois, le CEPD **observe** que, conformément à l'article 2, paragraphe 2, les informations sont classifiées uniquement en ce qui concerne la **confidentialité** et que, conformément à l'article 2, paragraphe 3, les niveaux de confidentialité «sont définis en fonction du préjudice qu'une divulgation non autorisée pourrait causer aux intérêts publics et privés légitimes, y compris ceux de l'Union, des institutions et organes de l'Union, des États membres ou d'autres parties prenantes concernées». L'accent est également mis sur la confidentialité dans le processus de gestion des risques liés à la sécurité de l'information décrit à l'article 5, dans lequel seul le niveau de confidentialité des informations est pris en considération.

15. En conséquence, le CEPD fait valoir que **la sécurité des données à caractère personnel,** telle que prescrite par le RPDUE, **a une portée qui n'empiète que partiellement sur celle de la sécurité de l'information prévue par la proposition**. L'article 4,

paragraphe 1, point f), du RPDUE exige de garantir **l'intégrité et la confidentialité** des données à caractère personnel, tandis que l'article 33 dudit règlement exige de garantir **la confidentialité, l'intégrité, la disponibilité et la résilience** constantes des systèmes et des services de traitement en tenant compte des **risques pour les droits et libertés des personnes physiques**.

16. Dans le même temps, pour rappeler ce que le CEPD a déjà affirmé[1] dans l'avis SRI 2.0, la poursuite des objectifs de sécurité de l'information peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que **toute limitation du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne**, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit.

17. La proposition exige des institutions de l'Union qu'elles appliquent des mesures de sécurité de l'information, soit en les rendant obligatoires, soit en les sélectionnant dans le cadre d'un processus de gestion des risques tenant compte de certains critères. Dans la pratique, certaines de ces mesures impliqueront inévitablement **le traitement de données à caractère personnel et de données de communications électroniques, notamment des données relatives au trafic**. La proposition contient déjà certaines mesures obligatoires qui impliqueraient le traitement de données à caractère personnel:

    - article 11, paragraphe 2: «Identification» et «authentification»;
    - article 11, paragraphe 3: «Journaux de sécurité adéquats»;
    - article 17, paragraphe 1, point a): «Authentification forte»;
    - article 17, paragraphe 1, point f): «mesures de prévention et de détection des fuites de données».

18. Le CEPD relève que les organisations agissant en tant que responsables du traitement et sous-traitants n'ont pas toujours conscience du fait que les données traitées dans des systèmes et des services de sécurité de l'information peuvent inclure des données à caractère personnel (comme, par exemple, les adresses IP, les identifiants des appareils, les fichiers journaux du réseau, les fichiers journaux de contrôle des accès, etc.). Cela pourrait entraîner certains risques de non-respect des principes de protection des données et de la vie privée, tels que la licéité du traitement, la minimisation des données, la limitation des finalités, la limitation de la conservation et les obligations en matière de transferts licites de données. Le CEPD estime qu'il convient de mettre en évidence le fait que **toutes les mesures de sécurité de l'information impliquant le traitement de données à caractère personnel devraient se conformer au cadre juridique actuel en matière de protection des données et de la vie privée** et que les institutions de l'Union devraient prendre les garanties techniques et organisationnelles nécessaires pour garantir ce respect de manière responsable. Qui plus est, s'il n'existe pas de base juridique appropriée

[1] *Voir point 11 de l'avis SRI 2.0.*

permettant aux institutions de l'Union de traiter des données à caractère personnel aux fins de la mise en œuvre de certaines mesures de sécurité, il convient d'envisager la création et la justification d'une telle base juridique.

19. Lorsqu'un acte juridique de l'Union prévoit le traitement de données à caractère personnel, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir CJUE, arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 54, et par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, n° 58243/00, § 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

20. Afin de garantir la sécurité juridique et la prévisibilité, et de veiller au respect du RPDUE, notamment l'article 5, paragraphe 1, point a) et l'article 5, paragraphe 2, le CEPD **recommande vivement que la proposition définisse clairement les activités de traitement des données à caractère personnel qui sont autorisées aux fins du présent règlement (sauf indication contraire dans un autre texte juridique sectoriel/spécifique)**, y compris: la ou les finalités du traitement; les catégories de données à caractère personnel; les catégories de personnes concernées; la définition des rôles le cas échéant (responsable du traitement, sous-traitant, responsables conjoints du traitement), les durées de conservation, les destinataires en cas de transmission à des entités qui ne font pas l'objet du RPDUE. Le CEPD estime que ces éléments devraient être explicitement prévus dans la proposition ou, à tout le moins, dans un acte délégué qui sera adopté ultérieurement par la Commission. La proposition devrait prévoir une telle délégation. Le CEPD attire également l'attention sur la nécessité de veiller au respect des dispositions du RPDUE relatives aux transferts de données à caractère personnel vers des pays tiers et des organisations internationales.

21. Le CEPD **se félicite** du considérant 6, selon lequel la proposition est sans préjudice **du** RPDUE. En outre, le CEPD observe que l'article 46, paragraphe 9, contient une référence au RPDUE, en particulier lors du transfert d'ICUE contenant des données à caractère personnel vers des pays tiers. Le CEPD rappelle que le RPDUE s'appliquera à tous les traitements de données à caractère personnel par force de loi. Par conséquent, il n'est pas nécessaire d'introduire dans la proposition une disposition de fond établissant que le RPDUE s'applique en tout ou en partie. Le CEPD reconnaît que les transferts internationaux de données à caractère personnel sont un sujet complexe nécessitant un rappel supplémentaire de l'applicabilité du RPDUE. Dans ce cas, le CEPD recommande d'expliquer dans un considérant, éventuellement au considérant 6, que **toutes les dispositions du RPDUE** s'appliqueront, **y compris** les règles relatives aux transferts internationaux. Le considérant 6 peut également être utilisé pour inclure toute autre recommandation générale sur la protection des données formulée dans le présent avis qui ne vise pas à modifier les dispositions de fond.

22. La proposition réglemente les informations classifiées de l'UE de manière très large. Les ICUE, à l'instar de toutes les autres informations relevant du champ d'application de la proposition, peuvent également contenir des données à caractère personnel. En conséquence, elles sont soumises aux règles applicables en matière de protection des données, qui s'appliquent également dans ce cas et doivent être prises en compte à la suite des dispositions relatives aux ICUE. Nous recommandons de rappeler ce point

explicitement dans un considérant, compte tenu du niveau de détail des règles relatives aux ICUE dans le texte.

3.2. Synergies avec la protection des données et de la vie privée

23. L'article 33 du RPDUE considère les personnes physiques et leurs droits et libertés comme des biens à protéger dans le cadre de l'approche de gestion des risques liés à la sécurité lors du traitement de données à caractère personnel.

24. Le CEPD rappelle que **l'intégration de la dimension de la protection de la vie privée et des données et de ses avantages dans le processus de gestion traditionnelle de la sécurité de l'information garantira une approche holistique et permettra aux institutions de l'Union de bénéficier de synergies importantes dans la gestion de la sécurité de l'information et dans la protection des informations qu'elles traitent sans multiplier inutilement les efforts.**

25. L'utilisation de technologies pour améliorer la sécurité de l'information ne devrait pas constituer une ingérence indue dans les droits et libertés des personnes. La première étape pour éviter ou atténuer ces risques consiste à appliquer les exigences de protection des données dès la conception et par défaut visées à l'article 27 du RPDUE, ce qui permettra d'intégrer les garanties appropriées, telles que **la pseudonymisation** et **le chiffrement**, ou de mettre en œuvre des principes tels que **la limitation de la conservation et la minimisation des données**, dans la conception et l'utilisation de ces technologies et systèmes.

26. Le CEPD rappelle que le chiffrement, y compris le chiffrement de bout en bout, est une technologie critique et irremplaçable pour assurer une protection efficace des données et de la vie privée[2]. Le CEPD accueille favorablement les articles 11 et 17 de la proposition, qui incluent le chiffrement dans la liste des mesures minimales de protection des informations au repos et en transit.

27. L'utilisation d'outils et de services de collaboration et de communication électroniques étant devenue la norme dans nos conditions de travail habituelles, il est très important de préserver également la sécurité des communications électroniques. Au-delà des avantages qu'il présente pour la confidentialité des communications électroniques, **le chiffrement de bout en bout** peut également protéger les informations relevant du champ d'application de la présente proposition, lorsqu'elles sont échangées au moyen d'outils de collaboration et de communication électroniques. C'est pourquoi le CEPD **recommande vivement d'inclure le chiffrement de bout en bout dans la liste des mesures de sécurité minimales de la proposition, le cas échéant, et en particulier lors de l'échange d'informations sensibles non classifiées**.

28. Compte tenu de l'accélération de l'utilisation et de l'adoption des services d'informatique en nuage par les institutions de l'Union, le CEPD **recommande d'ajouter à l'article 5, paragraphe 3,** que, **parmi les facteurs pris en considération dans le processus de gestion des risques liés à la sécurité de l'information, les menaces découlant de l'accès fondé sur la juridiction de pays tiers (par exemple, par leurs pouvoirs**

[2] *« The Future of Encryption in the EU» (L'avenir du cryptage dans l'UE), discours de Wojciech Wiewiórowski, Contrôleur européen de la protection des données, lors du webinaire 2020 de l'ISOC*

publics) doivent également être prises en considération. Il s'agit là d'un autre exemple de synergies possibles entre la sécurité de l'information et la protection des données. En faisant face à ces risques dans un domaine, on s'attaque aux risques dans l'autre domaine pour les mêmes systèmes d'information que ceux qui traitent des données à caractère personnel et des informations relevant du champ d'application de la proposition.

29. Enfin, lorsqu'il s'agit d'incidents liés à la sécurité de l'information susceptibles d'entraîner une violation des données à caractère personnel, ou lorsqu'il s'agit d'une violation des données à caractère personnel qui présente des éléments utiles pour faire face à un incident de sécurité de l'information, il est **fortement recommandé d'expliquer dans un considérant pertinent** l'intérêt de mettre en place **une procédure intégrée de traitement des incidents[3] qui à la fois garantisse la sécurité de l'information et satisfasse aux obligations en matière de protection des données s'agissant des notifications de violations des données**. Ainsi, le responsable du traitement peut économiser du temps et des ressources et apporter une réponse bien plus efficace aux incidents dans les deux domaines.

30. Pour garantir de telles synergies entre la sécurité de l'information et la protection des données, **le CEPD recommande vivement que la proposition prévoie l'obligation spécifique pour les fonctionnaires de l'UE chargés de la sécurité de l'information de coopérer étroitement avec le délégué à la protection des données désigné conformément à l'article 43 du RPDUE,** dans le cadre d'activités telles que l'application de la protection des données dès la conception et par défaut aux mesures de sécurité de l'information, la sélection de mesures de sécurité impliquant le traitement de données à caractère personnel, la gestion intégrée des risques et le traitement intégré des incidents de sécurité.

4. Conclusions

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

- le CEPD recommande vivement que la proposition définisse clairement les activités de traitement des données à caractère personnel qui sont autorisées aux fins du présent règlement, y compris: la ou les finalités du traitement; les catégories de données à caractère personnel; les catégories de personnes concernées; la définition des rôles le cas échéant (responsable du traitement, sous-traitant, responsables conjoints du traitement), les durées de conservation, les destinataires en cas de transmission à des entités qui ne font pas l'objet du RPDUE. Le CEPD estime que ces éléments devraient être explicitement prévus dans la proposition ou, à tout le moins, dans un acte délégué qui sera adopté ultérieurement par la Commission. La proposition devrait prévoir une telle délégation.

[3] *Voir aussi les Lignes directrices du CEPD sur les notifications de violations de données à caractère personnel*

- le CEPD recommande d'expliquer dans un considérant que toutes les dispositions du RPDUE s'appliqueront, y compris les règles relatives aux transferts internationaux. Le considérant 6 peut également être utilisé pour inclure toute autre recommandation générale sur la protection des données formulée dans le présent avis qui ne vise pas à modifier les dispositions de fond.

- le CEPD recommande vivement d'inclure le chiffrement de bout en bout dans la liste des mesures de sécurité minimales de la proposition, le cas échéant, et en particulier lors de l'échange d'informations sensibles non classifiées.

- le CEPD recommande d'ajouter à l'article 5, paragraphe 3, que, parmi les facteurs pris en considération dans le processus de gestion des risques liés à la sécurité de l'information, les menaces découlant de l'accès fondé sur la juridiction de pays tiers (par exemple, par leurs pouvoirs publics) doivent également être prises en considération.

- le CEPD recommande vivement d'expliquer dans un considérant pertinent les avantages que présentent une procédure intégrée de gestion des risques liés à la sécurité de l'information et de traitement des incidents qui à la fois garantisse la sécurité de l'information et satisfasse aux obligations en matière de protection des données s'agissant des notifications de violations des données.

- le CEPD recommande vivement que la proposition prévoie l'obligation spécifique pour les fonctionnaires de l'UE chargés de la sécurité de l'information de coopérer étroitement avec le délégué à la protection des données désigné conformément à l'article 43 du RPDUE, dans le cadre d'activités telles que l'application de la protection des données dès la conception et par défaut aux mesures de sécurité de l'information, la sélection de mesures de sécurité impliquant le traitement de données à caractère personnel, la gestion intégrée des risques et le traitement intégré des incidents de sécurité.

Bruxelles, le 17 mai 2022

Wojciech Rafał WIEWIÓROWSKI

[signature électronique]

Notes

[1] JO L 295 du 21.11.2018, p. 39.
[2] COM(2022) 119 final
[3] COM(2022) 122 final
[4] Stratégie de cybersécurité de l'UE pour la décennie numérique | «Façonner l'avenir numérique de l'Europe» (europa.eu), qui inclut une communication conjointe avec le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité [JOIN(2020)18].
[5] Voir chapitre I. INTRODUCTION, page 4 de la stratégie.
[6] Communication conjointe de la Commission européenne et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil, intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique».
[7] Avis 5/2021 du CEPD sur la stratégie en matière de cybersécurité et la directive SRI 2.0
[8] 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).