EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17 mai 2022

Avis 8/2022

sur la proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité 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 de la Commission établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité 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.

Synthèse

Le 22 mars 2022, la Commission européenne a adopté une proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité 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 posture de cybersécurité des institutions, organes et organismes de l'Union (les «institutions de l'Union»), et salue également le nouveau rôle de l'ancienne «équipe d'intervention en cas d'urgence informatique», désormais dénommée «centre de cybersécurité» (CERT-UE), compte tenu de l'intensification de la transformation numérique, de l'évolution rapide du paysage des menaces qui pèsent sur la cybersécurité et de la récente évolution de la transformation numérique due également à la pandémie de COVID-19.

Le CEPD regrette que la proposition ne soit pas alignée sur la directive SRI et sur la proposition SRI 2.0, afin que des règles cohérentes et homogènes soient mises en place pour les États membres et les institutions de l'Union, contribuant ainsi au niveau global de cybersécurité de l'Union. Le CEPD recommande d'ajouter dans la proposition que les exigences minimales en matière de sécurité devraient être au moins égales ou supérieures aux exigences minimales en matière de sécurité des entités visées dans la directive SRI et la proposition SRI 2.0.

Afin de se conformer à la proposition, les institutions de l'Union, ainsi que le CERT-UE, devront déployer certaines procédures et mesures de cybersécurité, qui impliqueront nécessairement un traitement supplémentaire des données à caractère personnel. Afin de garantir la sécurité juridique et la prévisibilité et de veiller au 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 une base juridique pour le traitement de données à caractère personnel par le CERT-UE et les institutions de l'Union, notamment les finalités du traitement et les catégories de données à caractère personnel.

Le CEPD souligne l'importance d'intégrer la dimension de la protection de la vie privée et des données dans la gestion de la cybersécurité, afin de créer des synergies positives entre la proposition et la législation en matière de protection de la vie privée et des données, et formule des recommandations spécifiques sur la manière de parvenir à de telles synergies, y compris l'obligation spécifique pour les fonctionnaires de l'UE chargés de la cybersécurité de coopérer étroitement avec le délégué à la protection des données désigné conformément au RPDUE.

Le CEPD recommande vivement que la proposition prévoie une coopération étroite entre le CERT-UE et le CEPD, dans le cadre d'activités telles que le traitement d'incidents donnant lieu à des violations de données à caractère personnel, le traitement de vulnérabilités importantes, d'incidents importants ou d'attaques majeures susceptibles d'entraîner des violations de données à caractère personnel, de même que lorsque le CERT-UE dispose d'éléments indiquant que le non-respect de la proposition entraîne une violation de données à caractère personnel.

Le CEPD recommande également vivement que la proposition prévoie la participation du CEPD

au «conseil interinstitutionnel de cybersécurité» (IICB).

Table des matières

1. Introduction 5

2. Observations générales 6

3. Observations particulières 8

3.1. Champ d'application de la proposition et relation avec la législation relative à la protection des données et de la vie privée 8

3.2. Synergies avec la protection des données et de la vie privée ... 11

3.3. Le rôle du CEPD 12

3.4. Partage d'informations et services du CERT-UE 13

4. Conclusions 14

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 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union[2] (la «proposition»).

2. Le même jour, 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[3] (la «proposition Infosec»).

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 vise 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 l'exposé des motifs, l'objectif de la proposition est double:

   - tenir compte du panorama de plus en plus hostile des cybermenaces et de l'incidence croissante des cyberattaques plus sophistiquées touchant les institutions, organes et organismes de l'UE, rendant indispensable d'accroître les investissements pour atteindre un niveau élevé de cybermaturité, et

   - renforcer l'équipe d'intervention en cas d'urgence informatique de l'UE (CERT-UE) en améliorant le mécanisme de financement nécessaire pour accroître sa capacité à aider les institutions, organes et organismes de l'Union à appliquer les nouvelles règles en matière de cybersécurité et à améliorer leur cyber-résilience.

5. Le CEPD fait observer que l'objet de la proposition en question est étroitement 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. Conformément à la stratégie, la proposition vise à améliorer encore la résilience de l'ensemble des institutions, organes et organismes de l'Union, ainsi que leurs capacités de réaction aux incidents. Elle est également conforme aux priorités de la Commission consistant à adapter l'Europe à l'ère du numérique et à bâtir une économie au service des personnes et parée pour l'avenir. Elle souligne par ailleurs que la sûreté et la résilience de l'administration publique constituent une pierre angulaire de la transformation numérique de la société dans son ensemble.

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

   - présente des mesures destinées à assurer un niveau élevé commun de cybersécurité pour les institutions, organes et organismes de l'Union européenne,

   - établit le «conseil interinstitutionnel de cybersécurité», qui est chargé de suivre la mise en œuvre du règlement proposé,

   - définit le nouveau rôle de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'UE («CERT-UE»)[8], en tant que «centre de cybersécurité» pour les institutions, organes et organismes de l'Union, pour faire écho à l'évolution observée dans les États membres et au niveau mondial.

8. Le 22 mars 2022, la Commission européenne a demandé au CEPD d'émettre un avis sur la proposition, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 (le «RPDUE»)[9]. 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 **observe** que si la proposition SRI 2.0 s'applique aux entités publiques et privées essentielles et importantes des États membres, la proposition s'applique quant à elle aux institutions, organes et organismes de l'Union.

10. 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 aux fins du traitement des données à caractère personnel, pour ce qui est de la proposition actuelle, qui établit des règles applicables aux institutions de l'Union, **le RPDUE s'applique et joue un rôle tout aussi important**.

11. Le CEPD **se félicite** de l'objectif de la proposition qui consiste à améliorer la posture de cybersécurité des institutions, organes et organismes de l'Union au moyen d'un instrument juridique autonome et dédié, à savoir un règlement. Le CEPD salue également du nouveau rôle du CERT-UE, compte tenu de l'intensification de la transformation numérique, de l'évolution rapide du paysage des menaces qui pèsent sur la cybersécurité et de la récente évolution de la transformation numérique due également à la pandémie de COVID-19.

12. Le CEPD **recommande** de préciser dans un considérant distinct, conformément à la pratique habituelle, que «le Contrôleur européen de la protection des données a été consulté conformément à l'article 42 du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le... [date de l'avis du CEPD]».

13. Le CEPD rappelle que, dans son avis SRI 2.0, il a recommandé aux colégislateurs de créer **un lien concret entre la proposition SRI 2.0 et les actions législatives au niveau des institutions de l'UE, afin d'établir des règles cohérentes et homogènes** pour les États membres et les institutions de l'Union[1]. Il est de la plus haute importance d'assurer un niveau élevé commun d'efficacité et de résilience, en particulier dans le fonctionnement de l'ensemble de l'administration publique au niveau national et de l'Union, en raison du rôle croissant que joue cette dernière sur la base des traités.

14. Le CEPD **regrette** que la proposition n'explique pas suffisamment dans l'exposé des motifs ni dans les considérants (4) et (5) pertinents, en quoi elle s'aligne sur la directive SRI et sur la proposition SRI 2.0 et comment elle contribue au niveau global de cybersécurité de l'Union grâce au lien avec la directive SRI et la proposition SRI 2.0.

15. Compte tenu du rôle essentiel et important que jouent les institutions de l'Union dans le fonctionnement de l'Union, le **CEPD estime que les exigences minimales de la proposition en matière de sécurité devraient être au moins égales ou supérieures aux exigences minimales en matière de sécurité des entités relevant du champ d'application de la directive SRI et de la proposition SRI 2.0**, conformément à l'article 3 de la proposition SRI 2.0 («harmonisation minimale»). Pour cette raison, le CEPD **recommande** d'ajouter dans un considérant que **la proposition s'appuie sur la proposition SRI 2.0** et d'expliquer plus en détail le lien entre la proposition et la directive SRI ainsi que la proposition SRI 2.0 aux considérants (4) et (5). En outre, le CEPD recommande d'inclure le libellé suivant dans le texte principal: «Les exigences minimales en matière de sécurité devraient être au moins égales ou supérieures aux exigences minimales en matière de sécurité des entités relevant du champ d'application de la proposition SRI 2.0».

16. Plus particulièrement, le CEPD **observe** que la proposition **n'est pas totalement alignée sur la proposition SRI 2.0** en ce qui concerne les points suivants:

    - L'article 5, paragraphe 1, de la proposition SRI 2.0 dispose que «[c]haque État membre adopte une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir». Le CEPD suggère d'inclure dans la proposition la promotion de l'adoption **d'une stratégie de cybersécurité commune à l'ensemble des institutions de l'UE**, tenant compte des exigences énoncées à l'article 5 de la proposition SRI 2.0.

    - Il semble y avoir un certain décalage entre les mesures minimales en matière de cybersécurité[2] de la proposition et les mesures minimales énumérées à l'article 18 de la proposition SRI 2.0. Dans ce contexte, le **CEPD regrette que la proposition ne contienne pas de référence explicite à l'utilisation de la cryptographie et**

[1] *point 25 de l'avis SRI 2.0 du CEPD*
[2] *Annexes I et II de la proposition*

du cryptage (et du chiffrement de bout en bout), qui sont des technologies essentielles pour protéger toutes les informations au repos et en transit et également les communications électroniques.

- Contrairement à la proposition SRI 2.0[3], la proposition ne contient pas de dispositions relatives à la **collaboration** du CERT-UE et du conseil interinstitutionnel de cybersécurité **avec le Contrôleur européen de la protection des données**. **Le CEPD recommande vivement que cette collaboration soit institutionnalisée au moyen d'une disposition dans la proposition**, afin de permettre au CEPD de suivre les évolutions en matière de cybersécurité susceptibles d'entraîner des répercussions sur la sécurité des données à caractère personnel des institutions de l'Union et de contrôler le respect des mesures de cybersécurité. Des précisions supplémentaires sont fournies sur ce point dans la section 3.3.

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

17. Le CEPD note que les entités concernées par la proposition sont les mêmes que celles visées par le RPDUE, à savoir les «institutions, organes et organismes de l'Union» [«Union institutions, bodies, offices and agencies» en anglais]. Si on retrouve cette expression dans l'intitulé de la proposition, l'expression «institutions, organes et organismes de l'Union» [«Union institutions, bodies and agencies» en anglais] est ensuite utilisée dans le reste du texte. Le CEPD **recommande** d'utiliser l'expression **«institutions, organes et organismes de l'Union»** de manière cohérente dans l'ensemble de la proposition afin d'éviter tout malentendu.

18. Le CEPD rappelle[4] que 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 cette obligation – applicable 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 européenne en matière de protection des données**.

19. Le CEPD observe, d'une part, que la proposition reprend la définition de la cybersécurité qui figure dans la proposition SRI 2.0: *«les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces»*, le terme cybermenace désignant *«toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et*

[3] *Considérants 58 et 77, articles 28 et 32 de la proposition SRI 2.0*
[4] *Point 10 de l'avis SRI 2.0 du CEPD*

systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes»[5]. Il ressort clairement de cette définition que l'objectif de la cybersécurité est différent de celui des dispositions relatives à la sécurité du RPDUE, comme à l'article 4, paragraphe 1, point f), et à l'article 33 («sécurité des données à caractère personnel»). Alors que la cybersécurité vise à protéger «*les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes*» des cybermenaces, la sécurité des données à caractère personnel poursuit un objectif spécifique différent: protéger les données à caractère personnel contre **toute menace** (y compris les cybermenaces) susceptible de porter atteinte aux **droits et libertés des personnes**. C'est la raison pour laquelle le CEPD a déclaré au point 10 de l'avis SRI 2.0 **qu'en améliorant la cybersécurité, on améliore également la sécurité des données à caractère personnel ainsi que la confidentialité des communications électroniques**. Cette observation reste valable dans le présent contexte.

20. Par ailleurs, le CEPD rappelle[6] que la poursuite des objectifs de cybersécurité 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 potentielle 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 prévue par la loi, qu'elle soit à la fois nécessaire et proportionnée et qu'elle respecte le contenu essentiel du droit.

21. Afin de se conformer à la proposition, les institutions de l'Union, ainsi que le CERT-UE, devront déployer certains processus et mesures de cybersécurité, qui **impliqueront nécessairement un traitement supplémentaire des données à caractère personnel et des données de communications électroniques, y compris les données relatives au trafic**. De telles mesures seraient adoptées en ce qui concerne la gestion des risques de cybersécurité, ou parce qu'elles figurent sur la liste des mesures minimales en matière de cybersécurité[7] telles que le contrôle des accès, la sécurité des communications, la gestion des incidents et l'authentification à facteurs multiples.

22. Dans ce contexte, 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 cybersécurité peuvent constituer 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 exacerbe les risques de non-respect de la législation relative à la protection des données et de la vie privée, par exemple les principes de licéité du traitement, de limitation des finalités, de minimisation des données, de limitation de la conservation et d'obligations en matière de transferts licites de données. Le CEPD considère donc, pour écarter tout doute, qu'il doit être clairement précisé dans un nouveau considérant que «**tous les systèmes et services de cybersécurité intervenant dans la prévention, la détection et la réaction aux cybermenaces devraient être conformes au cadre actuel de protection des données et de la vie privée et devraient prendre des mesures techniques et**

---

[5] 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, COM(2020) 823 final
[6] Point 11 de l'avis SRI 2.0 du CEPD
[7] Annexes I & II de la proposition

organisationnelles appropriées pour garantir cette conformité de manière responsable».

23. Le CEPD **accueille favorablement** le considérant 22 selon lequel toutes les données à caractère personnel faisant l'objet d'un traitement dans le cadre de la présente proposition devraient être traitées conformément à la législation en matière de protection des données, y compris le règlement (UE) 2018/1725. En outre, le CEPD recommande d'ajouter dans ce considérant 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 du CEPD».**

24. Le CEPD **fait observer** que l'article 18, paragraphe 3, prévoit que le traitement de données à caractère personnel dans le cadre de la présente proposition est régi par le RPDUE, ce qui donne l'impression que cette obligation n'est requise que dans le cadre du traitement des informations par le CERT-UE et les institutions de l'Union. Afin d'éviter d'éventuelles erreurs d'interprétation, le CEPD **recommande** de déplacer la disposition visée à l'article 18, paragraphe 3 au considérant 22 afin de couvrir **tout traitement de données à caractère personnel** effectué par le CERT-EU et les institutions de l'Union dans le cadre de la proposition, y compris sans toutefois s'y limiter: les services de cybersécurité assurés par le CERT-EU conformément à l'article 12, le partage d'informations conformément à l'article 18, les obligations en matière de partage conformément à l'article 19, les mesures impliquant le traitement de données à caractère personnel en ce qui concerne la gestion des risques de cybersécurité à l'article 4, et la liste des mesures minimales en matière de cybersécurité[8] de la proposition, qui impliquent le traitement de données à caractère personnel.

25. 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*, nº 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).

26. 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 prévoie clairement une base juridique pour le traitement des données à caractère personnel par le CERT-UE et les institutions de l'Union,** y compris, en particulier, les finalités du traitement et les catégories de données à caractère personnel. En outre, les éléments suivants devraient être explicitement définis: a) Identification du ou des responsables du traitement, des sous-traitants ou des responsables conjoints du traitement, le cas échéant; b) Catégories de personnes concernées; c) Durées de conservation ou, à tout le moins, critères permettant de déterminer ces durées. Le CEPD estime que ces éléments devraient être explicitement

[8] *Annexes I & II de la proposition*

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.

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

27. Le CEPD rappelle[9] que **l'intégration de la dimension de la protection de la vie privée et des données dans la gestion traditionnelle de la cybersécurité est à même de garantir une approche holistique et donc de permettre aux institutions de l'Union de bénéficier de synergies importantes dans la gestion de la cybersécurité et dans la protection des informations qu'elles traitent sans multiplier inutilement les efforts.**

28. L'utilisation de technologies pour améliorer la cybersécurité 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, le chiffrement, l'exactitude des données et la minimisation des données**, dans la conception, le développement et l'utilisation de ces technologies et systèmes de cybersécurité.

29. Le CEPD souhaite rappeler 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**. Si le chiffrement est **très efficace pour faire face aux risques de cybersécurité**, il **n'implique pas le traitement supplémentaire de données à caractère personnel**.

30. Compte tenu de l'accélération de l'utilisation et de l'adoption des services en nuage par les institutions de l'Union, le CEPD **recommande vivement d'inclure le «chiffrement au repos», le «chiffrement en transit» ainsi que le «chiffrement de bout en bout» dans la liste des mesures minimales de cybersécurité figurant à l'annexe II de la proposition**.

31. Comme cela a déjà été souligné précédemment, la gestion des risques pour les droits et libertés des personnes physiques, lorsque leurs données à caractère personnel sont traitées, est une obligation prévue à l'article 33 du RPDUE. Alors que les mesures de gestion des risques en matière de cybersécurité prévues à l'article 4 de la proposition visent à protéger les réseaux et les systèmes d'information (ainsi que les données qu'ils contiennent), l'article 33 du RPDUE vise, quant à lui, à tenir compte des risques pour les personnes (qui n'appartiennent pas nécessairement à la même organisation) et leurs droits en protégeant leurs données à caractère personnel. Les actifs à protéger dans le cadre de ces deux activités sont différents, ce qui pourrait aboutir, dans certaines circonstances, à des conclusions différentes. Dans le même temps, le processus de gestion des risques de cybersécurité peut contribuer à l'analyse de l'impact sur la protection des données des faiblesses dans la sécurité des données à caractère personnel. C'est pourquoi le CEPD recommande **d'intégrer les considérations relatives à la protection de la vie privée et des**

[9] *Point 16 de l'avis SRI 2.0 du CEPD*

données dans la gestion des risques de cybersécurité, afin d'assurer une approche holistique et de permettre des synergies sans multiplier inutilement les efforts.

32. Enfin, en ce qui concerne les incidents de cybersécurité susceptibles d'entraîner une violation de données à caractère personnel, ou une violation de données à caractère personnel indiquant l'existence d'un incident de cybersécurité, il est **fortement recommandé d'expliquer, dans un considérant pertinent,** l'intérêt de mettre en place **une procédure intégrée de gestion des incidents[10] qui à la fois garantisse la cybersécurité et satisfasse aux obligations en matière de protection des données s'agissant des notifications de violation des données**. De cette manière, le responsable du traitement peut économiser du temps et des ressources et apporter une réponse bien plus efficace aux incidents dans les deux domaines.

33. Pour garantir de telles synergies entre la cybersécurité et la protection des données, **le CEPD recommande vivement que la proposition prévoie l'obligation spécifique pour le responsable local de la cybersécurité défini à l'article 4, paragraphe 5, de coopérer avec le délégué à la protection des données désigné conformément à l'article 43 du RPDUE**, lorsqu'il s'agit d'activités qui se chevauchent, telles que l'application de la protection des données dès la conception et par défaut aux mesures de cybersécurité, la sélection de mesures de cybersécurité impliquant le traitement de données à caractère personnel, la gestion intégrée des risques et le traitement intégré des incidents de sécurité.

3.3. Le rôle du CEPD

34. Le CEPD relève que la proposition **ne fait aucune mention du CEPD**, malgré l'interaction importante entre la cybersécurité et la protection des données et de la vie privée, ainsi que cela est décrit ci-dessus.

35. Le CEPD doit être associé à ces deux aspects, d'une part pour **surveiller les évolutions en matière de cybersécurité** susceptibles d'avoir des répercussions sur la protection des données et la vie privée et, d'autre part, pour **contrôler et garantir la conformité des mesures de cybersécurité** qui impliquent le traitement de données à caractère personnel.

36. Contrairement à la proposition, l'article 28 et l'article 32 de la proposition SRI 2.0 prévoient des dispositions spécifiques relatives à **la collaboration entre les autorités chargées de la cybersécurité et les autorités chargées de la protection des données**.

37. **Afin d'assurer la cohérence entre les États membres et les institutions de l'Union, et** conformément à l'article 28 de la proposition SRI 2.0, le CEPD **recommande vivement** d'ajouter à l'article 12 de la proposition, intitulé «Mission et tâches du CERT-UE», la disposition selon laquelle **«le CERT-UE travaille en étroite coopération avec le CEPD lorsqu'il traite des incidents donnant lieu à des violations de données à caractère**

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

personnel ou à une violation de la confidentialité des communications électroniques».

38. Dans le même esprit, le CEPD estime que **le CERT-UE doit l'informer lorsqu'il traite des vulnérabilités importantes, des incidents importants ou des attaques majeures susceptibles d'entraîner des violations de données à caractère personnel et/ou une violation de la confidentialité des communications électroniques**. Une obligation correspondante devrait être ajoutée à l'article 12 «Mission et tâches du CERT-UE» de la proposition.

39. De surcroît, le CEPD **recommande** de prévoir, à l'article 12, que le CEPD est associé aux activités de sensibilisation des institutions de l'Union en ce qui concerne les services de cybersécurité assurés par le CERT-UE, afin de tenir compte de l'interaction entre la violation de données à caractère personnel et les incidents de cybersécurité.

40. En outre, conformément à l'article 32 de la proposition SRI 2.0, le CEPD **recommande** d'ajouter à l'article 12 de la proposition, intitulé «Mission et tâches du CERT-UE», une disposition précisant que **le CERT-UE informe sans retard injustifié le CEPD lorsqu'il dispose d'éléments indiquant qu'une violation par les institutions de l'Union des obligations énoncées dans la proposition entraîne une violation de données à caractère personnel**.

41. Le CEPD ne figure pas sur la liste des participants permanents du «conseil interinstitutionnel de cybersécurité» (l'«IICB») défini à l'article 9 de la proposition. Comme indiqué ci-dessus, la sécurité du traitement de données à caractère personnel, et donc également la cybersécurité, est l'une des pierres angulaires de la protection des données. En outre, le CEPD est chargé, en vertu de l'article 57, paragraphe 1, point h), du RPDUE, de suivre les évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et des communications. Cela inclut les évolutions en matière de cybersécurité, et, afin de pouvoir publier des orientations spécifiques en matière de protection des données liées à la cybersécurité, le CEPD **recommande vivement d'ajouter le Contrôleur européen de la protection des données à l'article 9, paragraphe 3, en tant que participant permanent à l'IICB avec un représentant**.

3.4. Partage d'informations et services du CERT-UE

42. En vertu de l'article 12, le CERT-UE fournit certains services de cybersécurité dans le cadre desquels il agit en qualité de sous-traitant des informations relatives à la cybersécurité qui comprennent des données à caractère personnel. Il convient de s'assurer d'emblée que ces activités de traitement de données sont pleinement conformes au RPDUE et au RGPD.

43. L'article 16, paragraphe 2, dispose que le CERT-UE «peut échanger des informations propres à un incident avec les homologues nationaux dans les États membres afin de faciliter la détection de cybermenaces ou d'incidents similaires sans le consentement de la partie touchée» et que «[l]e CERT-UE ne peut échanger des informations propres à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de la partie touchée».

44. En vertu de l'article 19, le CERT-UE peut demander et obtenir des informations provenant des inventaires des systèmes informatiques des institutions de l'UE, afin de coordonner la gestion des vulnérabilités et la réaction aux incidents. En outre, les institutions de l'Union sont tenues de fournir au CERT-UE, à sa demande et dans les meilleurs délais, les informations numériques générées par l'utilisation de dispositifs électroniques impliqués dans les incidents qui les ont respectivement touchés.

45. Le CEPD estime qu'il est très probable que les informations propres à un incident ainsi que les informations numériques générées par l'utilisation de dispositifs électroniques impliqués dans l'incident contiennent des données à caractère personnel. C'est pourquoi le CEPD conseille de préciser les catégories de données à caractère personnel qui seront traitées dans le cadre de ces échanges, la ou les finalités du traitement, les destinataires des données et leur éventuelle transmission, afin d'assurer la clarté juridique, la sécurité juridique et la prévisibilité nécessaires. 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.

46. En outre, le CEPD note l'utilisation du terme «consentement» que le législateur a déjà défini à l'article 3, paragraphe 15, du RPDUE. Étant donné que la proposition, dans le contexte de l'article 16, paragraphe 2, fait référence aux institutions, organes et organismes de l'Union («parties touchées») plutôt qu'aux personnes concernées, le CEPD suggère d'utiliser le terme «autorisation» au lieu de «consentement».

47. L'article 17, paragraphe 3, dispose que «le CERT-UE peut, avec le consentement de la partie touchée par un incident, fournir des informations relatives à l'incident aux partenaires [homologues des pays tiers] susceptibles de contribuer à son analyse». Le CEPD rappelle que ces transferts internationaux de données doivent être pleinement conformes au chapitre V du RPDUE. Par conséquent, le CEPD recommande d'inclure dans la proposition un considérant faisant référence au chapitre susmentionné.

4. Conclusions

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

- Le CEPD recommande d'ajouter dans un considérant que la proposition s'appuie sur la proposition SRI 2.0 et d'expliquer plus en détail le lien entre la proposition et la directive SRI ainsi que la proposition SRI 2.0 aux considérants (4) et (5). En outre, le CEPD recommande d'inclure le libellé suivant dans le texte principal: «Les exigences minimales en matière de sécurité devraient être au moins égales ou supérieures aux exigences minimales en matière de sécurité des entités visées dans la directive SRI 2.0 et la proposition SRI 2.0».

- le CEPD recommande vivement que la proposition prévoie clairement une base juridique pour le traitement des données à caractère personnel par le CERT-UE et les institutions de l'Union, notamment en ce qui concerne les finalités du traitement et les catégories de données à caractère personnel. En outre, les éléments suivants devraient être explicitement définis: a) Identification du ou des responsables du

traitement, des sous-traitants ou des responsables conjoints du traitement, le cas échéant; b) Catégories de personnes concernées; c) Durées de conservation ou, à tout le moins, critères permettant de déterminer ces durées. 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 recommande vivement d'inclure le «chiffrement au repos», le «chiffrement en transit» ainsi que le «chiffrement de bout en bout» dans la liste des mesures minimales de cybersécurité figurant à l'annexe II de la proposition.

- le CEPD recommande vivement que la proposition prévoie l'obligation spécifique pour le responsable local de la cybersécurité défini à l'article 4, paragraphe 5, de coopérer avec le délégué à la protection des données désigné conformément à l'article 43 du RPDUE, lorsqu'il s'agit d'activités qui se chevauchent, telles que l'application de la protection des données dès la conception et par défaut aux mesures de cybersécurité, la sélection de mesures de cybersécurité impliquant le traitement de données à caractère personnel, la gestion intégrée des risques et le traitement intégré des incidents de sécurité.

- le CEPD recommande vivement d'ajouter à l'article 12 de la proposition, intitulé «Mission et tâches du CERT-UE», la disposition selon laquelle «le CERT-UE travaille en étroite coopération avec le CEPD lorsqu'il traite des incidents donnant lieu à des violations de données à caractère personnel ou à une violation de la confidentialité des communications électroniques».

- le CEPD recommande d'ajouter l'obligation pour le CERT-UE d'informer le CEPD lorsqu'il traite des vulnérabilités importantes, des incidents importants ou des attaques majeures susceptibles d'entraîner des violations de données à caractère personnel et/ou une violation de la confidentialité des communications électroniques.

- le CEPD recommande de prévoir, à l'article 12, que le CEPD est associé aux activités de sensibilisation des institutions de l'Union en ce qui concerne les services de cybersécurité assurés par le CERT-UE, afin de tenir compte de l'interaction entre la violation de données à caractère personnel et les incidents de cybersécurité.

- le CEPD recommande d'ajouter à l'article 12 de la proposition, intitulé «Mission et tâches du CERT-UE», une disposition précisant que le CERT-UE informe sans retard injustifié le CEPD lorsqu'il dispose d'éléments indiquant qu'une violation par les institutions de l'Union des obligations énoncées dans la proposition entraîne une violation de données à caractère personnel.

- le CEPD recommande vivement que le Contrôleur européen de la protection des données soit ajouté à l'article 9, paragraphe 3, en tant que participant permanent à l'IICB avec un représentant.

Bruxelles, le 17 mai 2022

Wojciech Rafał WIEWIÓROWSKI

[signature électronique]

Notes

[1] JO L 295 du 21.11.2018, p. 39.
[2] COM(2022) 122 final.
[3] COM(2022) 119 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 de la stratégie, page 4.
[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] Le rôle actuel de la CERT-UE découle de l'accord interinstitutionnel 2018/C 12/01.
[9] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018).