EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

10 janvier 2024

Avis 2/2024

sur la proposition de règlement modifiant le règlement sur la cybersécurité en ce qui concerne les services de sécurité gérés

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 règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés[1]. Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations complémentaires, en particulier si d'autres difficultés se posent ou si de nouvelles informations apparaissent. En outre, il est fourni sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont attribués par le règlement (UE) 2018/1725. Le présent avis se limite aux dispositions de la proposition pertinentes sous l'angle de la protection des données.

[1] COM(2023) 208 final.

Résumé

Le 18 avril 2023, la Commission européenne a publié la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (la «proposition»).

L'objectif de cette proposition est de permettre l'adoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés», en plus de ceux concernant les produits TIC (technologies de l'information et de la communication), services TIC et processus TIC, qui sont déjà couverts par le règlement (UE) 2019/881. Le CEPD a été consulté par la Commission européenne le 14 novembre 2023, conformément à l'article 42, paragraphe 1, du RPDUE.

Dans le présent avis, le CEPD accueille favorablement les objectifs de la proposition et estime que les schémas de certification de cybersécurité pour les services de sécurité gérés pourraient en effet encourager l'offre de tels services et, dans le même temps, faciliter le choix d'un fournisseur de services qualifié pour les petites et moyennes entreprises qui ne disposent pas de spécialistes de la sécurité internes et qui dépendent de prestataires de services externes. Le CEPD propose un certain nombre de modifications à apporter à des éléments du nouvel article 51 *bis* et recommande d'établir, dans la proposition, une obligation pour les prestataires de déclarer eux-mêmes que les services et mesures qu'ils proposent sont conformes au cadre réglementaire applicable, y compris la protection des données, comme condition de la certification.

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, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (ci-après le «RPDUE»)[2], et notamment son article 42, paragraphe 1,

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction

1. Le 18 avril 2023, la Commission européenne a publié la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés[3] (la «proposition»).

2. L'objectif de cette proposition est de permettre, au moyen d'actes d'exécution de la Commission, l'adoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés», en plus de ceux concernant les produits TIC (technologies de l'information et de la communication), services TIC et processus TIC, qui sont déjà couverts par le règlement sur la cybersécurité[4]. Selon l'exposé des motifs[5], les services de sécurité gérés jouent un rôle de plus en plus important dans la prévention et la limitation des incidents de cybersécurité. La certification des services de sécurité gérés est considérée comme un moyen efficace de renforcer la confiance dans la qualité de ces services et de faciliter ainsi l'émergence d'un secteur européen des services de cybersécurité fiable. Certains États membres ont déjà commencé à adopter des schémas de certification pour les services de sécurité gérés. Il existe donc, en raison des incohérences relatives aux schémas de certification de cybersécurité dans les différents pays de l'Union, un risque croissant de fragmentation du marché intérieur concernant les services de sécurité gérés. La présente proposition permet la création de schémas européens de certification de cybersécurité pour ces services afin d'éviter une telle fragmentation[6].

3. Le présent avis du CEPD est émis en réponse à une consultation de la Commission européenne le 14 novembre 2023, conformément à l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au dernier considérant (non numéroté) de la proposition.

[2] JO L 295 du 21.11.2018, p. 39.
[3] COM(2023) 208 final.
[4] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité), JO L 151 du 7.6.2019, p. 15.
[5] COM(2023) 208 final, p. 1.
[6] COM(2023) 208 final, p. 1.

2. Observations générales

4. Le CEPD accueille favorablement les objectifs de la proposition et estime que les schémas de certification de cybersécurité pour les services de sécurité gérés pourraient en effet encourager l'offre de tels services et, dans le même temps, faciliter le choix d'un fournisseur de services qualifié pour les petites et moyennes entreprises qui ne disposent pas de spécialistes de la sécurité internes et qui dépendent de prestataires de services externes.

5. Le CEPD rappelle les recommandations formulées dans l'avis 7/2022 du CEPD[7] sur la relation entre la cybersécurité et la protection des données, qui restent également valables dans le contexte de la proposition actuelle. Si la cybersécurité fait partie de la législation en matière de protection des données depuis ses débuts et est établie aujourd'hui par l'article 5, paragraphe 1, point f), du RGPD comme l'un des grands principes relatifs au traitement des données à caractère personnel, le CEPD rappelle également que les mesures en matière de sécurité de l'information non seulement renforcent la sécurité des données à caractère personnel et contribuent à la protection de ces données, mais qu'elles sont également susceptibles d'interférer avec les 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. Certains des services proposés sous la forme de services de sécurité gérés, par exemple les tests de pénétration, peuvent avoir le potentiel d'entraver gravement ces droits fondamentaux. Le CEPD considère donc que les fournisseurs de services de sécurité gérés, même lorsqu'ils ne sont pas officiellement considérés comme les responsables du traitement d'un traitement suggéré ou initié par eux, devraient s'efforcer, dans la mesure du raisonnable, de déployer ou de proposer uniquement des mesures de sécurité conformes à l'environnement réglementaire applicable à leurs services et aux mesures proposées, y compris à la législation en matière de protection des données, afin d'être certifiés dans le cadre des schémas européens de certification de cybersécurité pour les services de sécurité gérés. Cela permettrait aux prestataires de services de proposer des mesures juridiquement viables et de réduire les risques de non-conformité pour les petites et moyennes entreprises.

6. Deux dispositions de la proposition contiennent les éléments nécessaires pour étendre les schémas de certification de cybersécurité aux services de sécurité gérés. Par conséquent, le CEPD a examiné tout particulièrement les modifications proposées à l'article 46, paragraphe 2, et l'insertion d'un article 51 *bis* dans le règlement (UE) 2019/881. Le CEPD note que les autres modifications sont des modifications d'ordre rédactionnel.

3. Connaissances appropriées en matière de protection des données

7. Le nouvel article 51 *bis* énumère les objectifs de sécurité des schémas européens de certification de cybersécurité pour les services de sécurité gérés, c'est-à-dire les objectifs garantis, à un niveau élevé, par tout système de certification de ce type. Cette liste est

[7] Avis 7/2022 du CEPD sur la proposition de règlement relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union, publié le 17 mai 2022, points 9 et 10.

fondée sur l'article 51 précédent relatif aux objectifs de sécurité des schémas européens de certification de cybersécurité pour les produits, services et processus TIC, mais est adaptée aux spécificités des services de sécurité gérés. Comme pour les produits, services et processus TIC, les services de sécurité gérés qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui sont consultées, traitées, stockées ou transmises dans le cadre de la fourniture de ces services[8]. En outre, de l'avis du CEPD, la proposition tient compte du fait que la sécurité est gérée en tant que service par les prestataires et que les objectifs doivent donc se concentrer davantage sur les facteurs garantissant la capacité du prestataire potentiel à fournir un tel service. Le CEPD note que ce résultat est atteint en fixant comme objectif que les services soient fournis en permanence avec la compétence, l'expertise et l'expérience requises par un personnel possédant un très haut niveau de connaissances techniques pertinentes et d'intégrité professionnelle.

8. Le CEPD se félicite de l'approche adoptée dans le nouvel article 51 *bis*. Toutefois, comme il l'a déjà indiqué dans ses observations générales, le CEPD est préoccupé par le fait que les aspects liés au respect de la réglementation, notamment à la protection des données, ne figurent pas parmi les objectifs à atteindre dans le cadre des schémas de certification.

9. Le CEPD rappelle que l'une des fonctions de la certification serait de susciter la confiance dans les services et de mettre des services de sécurité gérés de haute qualité à la disposition des entités disposant de peu de ressources. Cette fonction serait neutralisée si toute mesure proposée devait faire l'objet d'une évaluation juridique par le client. Si, en particulier, une petite et moyenne entreprise s'appuie sur la certification de ses fournisseurs, il se pourrait bien qu'elle soit surchargée par la tâche d'évaluer de manière indépendante et critique la légalité des mesures proposées, en dépit de son rôle potentiel de responsable du traitement. Afin d'éviter les situations dans lesquelles les fournisseurs certifiés proposeraient des mesures impliquant un traitement disproportionné ou autrement illégal des données, le CEPD recommande d'exiger une auto-déclaration de conformité des services et des mesures qu'ils proposent avec le cadre réglementaire applicable, y compris celui relatif à la protection des données, comme condition de certification.

4. Autres observations relatives aux objectifs de sécurité (article 51 *bis*)

10. L'article 51 *bis*, point c), prévoit l'obligation pour le prestataire de services de protéger les données traitées par le prestataire en ce qui concerne la fourniture de services de sécurité gérés. Bien que les mots «ou traitées de toute autre façon» fonctionnent comme une disposition générale, le CEPD propose d'ajouter le mot «générées» à la liste. Tel que défini au nouveau point 14 *bis* de l'article 2 du règlement sur la cybersécurité, on entend par «service de sécurité géré», un service consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, y compris la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil. Certains de ces outils de gestion des risques sont en mesure de reconnaître et de

[8] Voir la proposition de modification de l'article 46, paragraphe 2, du règlement sur la cybersécurité.

recueillir des informations qui pourraient être utilisées à des fins malveillantes pour lancer des attaques contre des organisations (par exemple, vulnérabilités des systèmes, informations divulguées publiquement qui peuvent être utilisées pour des attaques d'ingénierie sociale). Les systèmes utilisés pour la gestion des informations et des événements en matière de sécurité (SIEM) agrègent les journaux et corrèlent les événements afin de détecter les menaces et de générer des rapports sur la sécurité des systèmes. De l'avis du CEPD, il conviendrait donc de souligner le caractère critique des informations produites par ces systèmes en les mentionnant explicitement, en plus des termes «consultées, stockées, transmises» qui sont déjà énumérés, et en ajoutant ainsi le terme «générées».

11. Le point d) fixe comme objectif des systèmes de certification de faire en sorte que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident physique ou technique. Le CEPD estime que les deux aspects — physiques ou techniques — sont exhaustifs en ce qui concerne les mesures de sécurité, mais ne couvrent pas l'ensemble des incidents de sécurité possibles. Les incidents de sécurité résultant d'erreurs humaines ou d'actes malveillants de la part de membres du personnel devraient également être visés, même s'ils ne constituent pas une violation de la sécurité technique ou physique. Afin de ne pas exclure de quelconque type d'incident de sécurité, le CEPD propose le libellé suivant: «faire en sorte que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident de sécurité», sans autre qualification de l'incident.

12. Le point e) fixe comme objectif de faire en sorte que les personnes autorisées, les programmes ou les machines ne puissent accéder qu'aux données, services ou fonctions «concernés par leurs droits d'accès». Le CEPD note que les termes «concernés par leurs droits d'accès» sont fondés sur le point correspondant c) de l'article 51 existant. Toutefois, le CEPD propose de saisir l'occasion de rendre ces deux dispositions plus substantielles et axées également sur la protection des données: à l'heure actuelle, elles prévoient que les utilisateurs ne devraient accéder qu'aux ressources pour lesquelles ils ont obtenu un accès. Si, au lieu de cela, l'expression était remplacée par «nécessaires à l'accomplissement de leurs obligations», l'approche formaliste serait remplacée par une position de fond portant à la fois sur des considérations relatives à la sécurité et à la protection des données, selon lesquelles les droits d'accès doivent correspondre au principe du «besoin d'en connaître» ou du «besoin d'accès».

5. Conclusions

13. Eu égard aux considérations qui précèdent, le CEPD formule la recommandation suivante:

    – *établir, dans la proposition, une obligation pour les prestataires de déclarer eux-mêmes que les services et mesures qu'ils proposent sont conformes au cadre réglementaire applicable, y compris celui relatif à la protection des données, comme condition de la certification.*

Bruxelles, le 10 janvier 2024

(signature électronique)
Wojciech Rafał WIEWIÓROWSKI