EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

7 mars 2022

Avis 5/2022

sur la proposition de directive relative à l'échange d'informations entre les services répressifs des États membres

edps.europa.eu

Le Contrôleur européen de la protection des données (le «CEPD») est une institution indépendante de l'Union 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 leur 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.

En vertu de 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», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'UE sur l'application cohérente et logique des principes de protection des données de l'UE. 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 action future que pourrait entreprendre le CEPD dans l'exercice des pouvoirs que lui confère le règlement (UE) 2018/1725.

Synthèse

La Commission européenne a adopté le 8 décembre 2021 une proposition de directive du Parlement européen et du Conseil relative à l'échange d'informations entre les services répressifs des États membres. La proposition fait partie d'un paquet législatif plus large, appelé «Code de coopération policière de l'UE», qui comprend également une proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil (les «décisions Prüm») et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil (sous réserve d'un avis distinct du CEPD), et une proposition de recommandation du Conseil relative à la coopération policière opérationnelle.

La proposition vise à faciliter un accès équivalent des services répressifs aux informations détenues dans un autre État membre, tout en respectant les droits fondamentaux, y compris les exigences en matière de protection des données, ainsi qu'à garantir que tous les États membres disposent d'un point de contact unique fonctionnant efficacement et à remédier à la prolifération des canaux de communication utilisés pour l'échange d'informations en matière répressive entre les États membres, tout en renforçant le rôle d'Europol en tant que plateforme centrale d'information sur la criminalité dans l'Union.

Bien que le CEPD comprenne que les autorités répressives ont besoin de disposer des meilleurs outils techniques et juridiques possibles pour l'échange d'informations à des fins de prévention et de détection des infractions pénales ainsi que d'enquêtes en la matière, il estime que certains éléments de la proposition doivent être modifiés afin d'assurer la conformité avec les exigences en matière de protection des données.

Tout d'abord, la proposition devrait définir clairement le champ d'application personnel de l'échange d'informations et, en tout état de cause, limiter les catégories de données à caractère personnel qui peuvent être échangées au sujet des témoins et des victimes, conformément à l'article 6 de la directive 2016/680 en matière de protection des données dans le domaine répressif et de manière similaire à l'approche adoptée par l'annexe II du règlement Europol.

Le CEPD estime également que, conformément au principe de limitation de la conservation, la future directive devrait prévoir explicitement que les données à caractère personnel figurant dans les systèmes de gestion des dossiers des points de contact uniques ne devraient être conservées que pendant des périodes très courtes, qui devraient généralement correspondre aux délais en matière de transmission d'informations prévus à l'article 5 de la proposition.

Enfin, le CEPD est d'avis que les États membres devraient être tenus d'évaluer au cas par cas si Europol doit recevoir une copie des informations échangées, et à quelle fin. La proposition devrait également exiger explicitement que cette finalité, ainsi que toute restriction en vertu de l'article 19 du règlement Europol, soient communiquées à Europol.

L'avis analyse et fournit également des recommandations sur un certain nombre d'autres questions spécifiques, telles que la relation entre la proposition de directive et le cadre juridique existant en matière de protection des données, ainsi que l'utilisation de SIENA comme principal canal de communication entre les États membres.

Table des matières

1. Introduction 4

2. Observations générales 5

3. Observations particulières 5

3.1. Lien avec le cadre juridique existant en matière de protection des données 5

3.2. Champ d'application de l'échange de données à caractère personnel 6

3.3. Stockage des données échangées 7

3.4. Le rôle d'Europol 8

4. Conclusions 9

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

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 8 décembre 2021, la Commission européenne a adopté une proposition de directive du Parlement européen et du Conseil relative à l'échange d'informations entre les services répressifs des États membres, abrogeant la décision-cadre 2006/960/JAI du Conseil (la «proposition»)[2].

2. La proposition fait partie d'un paquet législatif plus vaste, appelé «Code de coopération policière de l'UE», qui comprend également:

   - la proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil[3], et

   - la proposition de recommandation du Conseil relative à la coopération policière opérationnelle[4].

3. L'objectif du code de coopération policière de l'UE est de rationaliser, de renforcer, de développer, de moderniser et de faciliter la coopération en matière répressive entre les agences nationales compétentes[5]. À cet égard, la proposition de directive vise à garantir un accès équivalent des services répressifs de tout État membre aux informations disponibles dans d'autres États membres afin de prévenir et de détecter les infractions pénales, ainsi que de mener des enquêtes pénales ou des opérations de lutte contre la criminalité, ce qui permet de contourner les règles existant actuellement au niveau national, qui entravent la circulation efficace et efficiente des informations[6]. La proposition vise donc à établir un cadre juridique garantissant une convergence des pratiques nationales et permettant un meilleur contrôle et une meilleure application des règles au niveau de l'Union et des États membres. En outre, la proposition vise à rapprocher les normes minimales garantissant un fonctionnement efficace et effectif des points de contact uniques (les «PCU»). Ces exigences minimales communes portent sur la composition, les structures, les responsabilités, les ressources en personnel et les capacités techniques.

4. La proposition, et plus généralement le code de coopération policière de l'UE, est liée aux objectifs politiques de plusieurs documents stratégiques de l'UE dans le domaine de la justice et

des affaires intérieures, notamment la stratégie de l'UE pour l'union de la sécurité[7], la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025)[8] et la stratégie 2021 pour un espace Schengen pleinement opérationnel et résilient[9]. De plus, les propositions établissant le code de coopération policière devraient être examinées à la lumière de la réforme en cours d'Europol et du rôle croissant de l'Agence en tant que plateforme centrale d'information sur la criminalité dans l'Union, qui collecte et traite des volumes toujours plus importants de données[10].

5. La Commission a consulté le CEPD sur la proposition de directive relative à l'échange d'informations entre les services répressifs le 7 janvier 2022, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725. 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.

2. Observations générales

6. Le terrorisme et la grande criminalité constituent une menace importante au sein de l'Union européenne et dans le monde et leur détection, leur prévention et leur poursuite représentent sans aucun doute un objectif important d'intérêt général, qui peut justifier des limitations à l'exercice des droits et libertés fondamentaux des individus, conformément à l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'UE.

7. Le CEPD comprend que les autorités répressives ont besoin de disposer des meilleurs outils techniques et juridiques possibles pour s'acquitter de leurs tâches, à savoir détecter, enquêter et prévenir les infractions et autres menaces à la sécurité publique. À cet égard, l'article 87 TFUE reconnaît la coopération policière, y compris l'échange d'informations pertinentes entre les autorités répressives, comme un instrument important pour la mise en place d'un espace de liberté, de sécurité et de justice.

8. Le présent avis vise à donner une évaluation juste et objective de la nécessité et de la proportionnalité des mesures proposées, ainsi qu'à formuler un certain nombre de recommandations spécifiques en vue d'assurer un juste équilibre entre les valeurs et les intérêts en jeu. À cette fin, une attention particulière est accordée à l'interaction de la proposition avec les dispositions du cadre juridique de l'UE en matière de protection des données, au champ d'application de la proposition et au rôle envisagé pour Europol.

3. Observations particulières

3.1. Lien avec le cadre juridique existant en matière de protection des données

9. Le CEPD accueille favorablement l'engagement pris au considérant 16 de la proposition selon lequel la protection des données à caractère personnel, conformément au droit de l'Union, devrait être garantie dans le cadre de tous les échanges d'informations effectués au titre de la directive proposée. En outre, la deuxième phrase du même considérant prévoit explicitement que les règles de la directive devraient être mises en conformité avec la directive (UE) 2016/680 (la «directive en matière de protection des données dans le domaine répressif», la «DPDR»)[11].

10. Étant donné que la directive (UE) 2016/680 s'appliquerait au traitement envisagé dans la proposition, le CEPD estime que si des garanties supplémentaires étaient nécessaires (par

exemple, en raison de la nature du traitement proposé), ces garanties devraient être incluses dans la proposition, afin de compléter les dispositions générales de la DPDR.

11. Le CEPD rappelle que le cadre législatif actuel est différent de celui qui prévalait lors de l'adoption de la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006[12], dans la mesure où un régime horizontal de protection des données dans le domaine de la justice et des affaires intérieures n'existait pas au niveau de l'Union. La décision-cadre 2008/977/JAI du Conseil[13], dite décision-cadre relative à la protection des données dans le troisième pilier de l'UE, a été adoptée deux ans plus tard.

12. Le CEPD note également que le considérant 16, dernière phrase, dispose que les dispositions de la proposition laissent inchangées les règles de la DPDR et du règlement (UE) 2016/679 (le RGPD)[14]. Cependant, l'objectif de la référence au RGPD reste flou. Selon l'article 2, paragraphe 1, point d), du RGPD, ce dernier ne s'applique pas au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

13. En outre, l'article 2, paragraphe 6, de la proposition renvoie à l'article 4, point 1), du règlement (UE) 2016/679 pour la définition des «données à caractère personnel». Le CEPD rappelle que la DPDR contient une définition identique dans son article 3, paragraphe 1, qui s'applique automatiquement à tout traitement au titre de la proposition.

14. Par conséquent, **dans un souci de sécurité juridique et de clarté, le CEPD recommande d'expliquer plus clairement dans le préambule la relation de la proposition avec le cadre juridique existant en matière de protection des données, et de s'abstenir de faire des références au RGPD**, car celui-ci ne semble pas pertinent dans le contexte du traitement des données à caractère personnel envisagé par la proposition.

3.2. Champ d'application de l'échange de données à caractère personnel

15. L'article 10, point i), de la proposition limiterait les données à caractère personnel échangées entre les États membres aux catégories visées à l'annexe II, section B, point 2, du règlement (UE) 2016/794 (règlement Europol)[15]. Le catalogue s'applique à des personnes qui, au regard du droit national de l'État membre concerné, sont a) soupçonnées d'avoir commis une infraction ou participé à une infraction relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction, ou b) des personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire, au regard du droit national de l'État membre concerné, qu'elles commettront des infractions pénales relevant de la compétence d'Europol.

16. Le CEPD a toujours exprimé son soutien aux mesures visant à harmoniser et à aligner les règles juridiques applicables au traitement de données opérationnelles à caractère personnel, en particulier dans le contexte d'Europol[16]. Par conséquent, il accueille favorablement l'approche choisie par la Commission pour définir de manière exhaustive les catégories de données qui peuvent être échangées entre les services répressifs (y compris au moyen des PCU).

17. L'utilisation d'une liste fermée de catégories de données apporterait une sécurité juridique supplémentaire et correspond au principe de minimisation des données, énoncé à l'article 4, paragraphe 1, point c), de la DPDR. En outre, elle devrait être considérée conjointement avec l'exigence générale contenue à l'article 4, paragraphe 2, point a), de la proposition, selon laquelle les informations demandées doivent être «nécessaires et proportionnées» à la réalisation de l'objectif mentionné à l'article 1er, paragraphe 1, de la proposition, à savoir la prévention ou la

détection des infractions pénales et les enquêtes en la matière. En outre, le CEPD estime que le choix d'une technique législative, à savoir par référence à la liste existante de catégories de données à l'annexe II du règlement Europol, pourrait contribuer à assurer la conformité d'Europol avec les règles applicables au traitement des données à caractère personnel dans les cas où l'Agence est mise en copie dans un échange bilatéral d'informations.

18. Dans le même temps, le CEPD note une différence substantielle entre la proposition et le règlement Europol en ce qui concerne le champ d'application, matériel et personnel des données traitées. En particulier, l'annexe II, section B, du règlement Europol établit plusieurs listes de catégories de données autorisées, chacune d'entre elles étant différenciée et étroitement liée à une certaine catégorie de personnes concernées. Par conséquent, le champ d'application et la quantité de données à caractère personnel concernant des criminels condamnés ou suspectés, qui pourraient être stockées et traitées, sont beaucoup plus importants que le champ d'application et la quantité de données concernant des victimes ou des témoins. Selon le CEPD, l'approche de l'annexe II, section B, du règlement Europol pourrait être considérée comme une expression pratique de l'obligation, en vertu de l'article 6 de la DPDR, «d'établir une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernée».

19. Le CEPD regrette que la proposition ne prévoie pas une telle distinction. Étant donné que le champ d'application personnel des échanges d'informations en vertu de la proposition ne serait pas limité uniquement aux criminels condamnés ou soupçonnés, les services répressifs peuvent demander et communiquer des données à caractère personnel concernant également d'autres parties à une enquête pénale, telles que les témoins et les victimes. Par conséquent, l'article 10, point i), de la proposition pourrait être interprété comme autorisant l'échange de catégories très larges de données (qui, dans le contexte d'Europol, n'est autorisé qu'en ce qui concerne les criminels et les suspects), également sur les témoins et les victimes. Le CEPD considère que ce résultat serait disproportionné et non conforme aux principes de protection des données.

20. Par conséquent, **le CEPD estime que la proposition devrait définir clairement le champ d'application personnel de l'échange d'informations et, en tout état de cause, devrait limiter les catégories de données à caractère personnel qui peuvent être échangées au sujet des témoins et des victimes en vertu de la proposition, conformément à l'article 6 de la DPDR, et de manière similaire à l'approche adoptée par l'annexe II du règlement Europol**.

3.3. Stockage des données échangées

21. L'un des objectifs de la proposition, selon l'exposé des motifs, est de remédier à l'absence de pratique commune dans l'utilisation des canaux de communication existants par les services répressifs. La proposition vise *notamment* à réduire la fragmentation en demandant aux États membres de regrouper un certain nombre de points de contact existants de la police dans une structure commune – un point de contact unique (PCU). À cette fin, et conformément à l'article 14, paragraphe 3, point a), de la proposition, le PCU devrait avoir accès à toutes les informations dont disposent les services répressifs nationaux, dans la mesure où cela est nécessaire à l'exécution des tâches qui lui incombent en vertu de la directive.

22. En outre, conformément à l'article 16 de la proposition, les États membres devraient veiller à ce que leur PCU déploie et exploite un système électronique unique de gestion des dossiers (SGD). Le système de gestion des dossiers servirait de répertoire et enregistrerait les demandes entrantes et sortantes, les informations communiquées, ainsi que les communications internes entre le PCU et les services répressifs nationaux.

23. Le CEPD note que le SGD stockerait non seulement les métadonnées liées à l'échange d'informations, mais aussi les données de contenu. Par conséquent, des données à caractère personnel de différents types provenant de différents services répressifs pourraient être stockées dans le SGD des PCU nationaux. Les principaux objectifs du stockage des données, selon l'article 16, paragraphe 1, points d) et e), de la proposition, seraient le recoupement des demandes entrantes avec les informations déjà disponibles et le suivi adéquat et rapide des demandes entrantes.

24. Le CEPD estime que plusieurs aspects liés au traitement des données dans le SGD, et en particulier le stockage des données de contenu, y compris les données à caractère personnel, doivent être clarifiés. En particulier, le texte de l'article 16, paragraphe 3, «[...] *les données à caractère personnel traitées par leur point de contact unique ne figurent dans le système de gestion des dossiers que pour la durée nécessaire et proportionnée aux fins pour lesquelles ces données sont traitées, puis à ce qu'elles soient irrévocablement supprimées*» pourrait laisser entendre que le stockage ne serait que temporaire, dans le but de faciliter l'échange d'informations. Dans le même temps, l'expression «*pour la durée nécessaire et proportionnée aux fins pour lesquelles ces données sont traitées*» n'est pas suffisamment spécifique pour limiter de manière significative les durées de conservation applicables. Le CEPD estime que le rôle du répertoire du SGD devrait être plus explicitement défini dans la proposition afin d'éviter la duplication des mêmes données dans des bases de données parallèles, ou du moins de la limiter au strict minimum.

25. À cet égard, le CEPD attire l'attention sur le risque d'une éventuelle désynchronisation en cas de stockage prolongé des données de contenu dans le SGD. Par exemple, lorsque le PCU est copié dans les messages initiaux identifiant une personne comme suspecte, mais que les États membres ne copient pas leur PCU dans une correction ultérieure, une classification incorrecte de la personne peut être diffusée dans le système répressif. En outre, la proposition ne précise pas quelles devraient être les conséquences du recoupement avec les informations disponibles, par exemple si le PCU doit fournir immédiatement et de sa propre initiative les informations à l'État membre requérant.

26. Par conséquent, **le CEPD estime que, conformément au principe de limitation de la conservation, la proposition devrait être modifiée de manière à prévoir explicitement que les données à caractère personnel ne peuvent être stockées dans le SGD que pendant des périodes très courtes, qui devraient généralement correspondre aux délais en matière de transmission d'informations prévus à l'article 5 de la proposition.**

3.4. Le rôle d'Europol

27. L'article 12 de la proposition obligerait les États membres à envoyer des copies des demandes d'information, des informations fournies en réponse à une demande, ou des informations transmises de leur propre initiative, à Europol, si ces informations concernent des infractions relevant des objectifs de l'Agence conformément au règlement Europol.

28. Le CEPD note que le considérant 18, dernière phrase, va encore plus loin et suggère que «*[d]ans la pratique, cela peut se faire en cochant par défaut la case "application SIENA" correspondante*». Dans ce contexte, le CEPD rappelle qu'en vertu de l'article 7, paragraphe 6, point a), du règlement Europol, les États membres doivent communiquer «à Europol des informations nécessaires à la réalisation de ses objectifs, y compris des informations relatives aux formes de criminalité à l'égard desquelles la prévention et la lutte sont considérées comme des priorités de l'Union». En outre, conformément à l'article 19 du règlement Europol, les États membres ont la possibilité juridique et en même temps l'obligation de déterminer les finalités du traitement d'informations par Europol et les limitations en la matière.

29. Le CEPD est préoccupé par le fait que, dans la pratique, les PCU et les services répressifs peuvent rencontrer des difficultés pour évaluer dans des cas individuels s'ils doivent envoyer une copie des informations à Europol et dans quelles conditions, et que cette évaluation serait sujette à des erreurs. Il pourrait en résulter qu'Europol reçoive plus d'informations qu'elle n'est autorisée à en traiter en vertu du règlement Europol.

30. Par ailleurs, l'article 13 de la proposition imposerait l'utilisation du réseau SIENA d'Europol pour tous les échanges prévus par la proposition. Par cet article, l'application SIENA d'Europol deviendrait le canal de communication obligatoire par défaut pour la coopération policière entre les États membres de l'UE (à l'exception des situations où d'autres canaux sont requis par le droit de l'Union, par exemple dans le contexte du système d'information Schengen).

31. Le CEPD note que les moyens de communication établis peuvent améliorer la sécurité des données et également renforcer et faciliter la supervision. Étant donné que, selon la Commission, actuellement, l'application SIENA n'est pas systématiquement utilisée comme canal privilégié, la transformation de l'application SIENA en un canal obligatoire pour les échanges entre services répressifs semble appropriée pour offrir les avantages susmentionnés du point de vue de la protection des données et remédier à la fragmentation.

32. Compte tenu de ce qui précède, **le CEPD estime que la proposition devrait être modifiée afin d'imposer explicitement aux États membres d'évaluer au cas par cas s'il convient d'envoyer une copie des informations échangées à Europol, et à quelle fin. La proposition devrait également prévoir explicitement que cette finalité, ainsi que toute limitation éventuelle en vertu de l'article 19 du règlement Europol, soit communiquée à l'Agence, afin qu'Europol sache comment elle pourrait traiter les données à caractère personnel.** Sauf indication contraire, la directive pourrait aboutir à la création d'une vaste base de données d'anciennes copies d'informations échangées qui serait gérée par Europol, agissant en tant que responsable du traitement, pour les nouvelles finalités fixées par l'Agence. Le CEPD recommande également de supprimer la dernière phrase du considérant 18.

4. Conclusions

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

– Le lien avec le cadre juridique existant en matière de protection des données devrait être expliqué plus clairement dans les considérants. En outre, la proposition devrait s'abstenir de toute référence au RGPD, car celui-ci ne semble pas pertinent dans le contexte du traitement des données à caractère personnel envisagé par la proposition.

– La proposition devrait définir clairement le champ d'application personnel des échanges d'informations envisagés et limiter les catégories de données à caractère personnel qui pourraient être échangées au sujet des témoins et des victimes, conformément à l'article 6 de la DPDR et de manière similaire à l'approche adoptée par l'annexe II du règlement Europol (UE).

– Le CEPD estime également que, conformément au principe de limitation de la conservation, la proposition devrait prévoir explicitement que les données à caractère personnel ne peuvent être stockées dans le SGD du PCU que pendant des périodes très courtes, qui devraient généralement correspondre aux délais en matière de transmission d'informations prévus à l'article 5 de la proposition.

– Le CEPD estime que la proposition devrait imposer explicitement aux États membres d'évaluer au cas par cas s'il convient d'envoyer une copie des informations échangées à Europol, et à quelle fin. La proposition devrait également prévoir explicitement que cette finalité, ainsi que les limitations éventuelles en vertu de l'article 19 du règlement Europol, soient communiquées à Europol. Le CEPD recommande également de supprimer la dernière phrase du considérant 18.

Bruxelles, le 7 mars 2022

[signature électronique]
Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 295 du 21.11.2018, p. 39.
[2] COM (2021) 782 final.
[3] COM(2021) 784 final.
[4] COM(2021) 780 final.
[5] Exposé des motifs, p. 2.
[6] Exposé des motifs, p. 3.
[7] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final.
[8] Communication de la Commission relative à la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025), COM(2021) 170 final.
[9] Communication de la Commission, «Stratégie pour un espace Schengen pleinement opérationnel et résilient», COM(2021) 277 final.
[10] Pour plus d'informations, voir l'avis 4/2021 du CEPD,https://edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf
[11] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
[12] Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, *JO L 386 du 29.12.2006, p. 89*JO L 386 du 29.12.2006, p. 89.
[13] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *JO L 350 du 30.12.2008, p. 60.*
[14] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[15] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI.
[16] Voir, par exemple, l'avis 4/2021 du CEPD, point 40.