EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

8 février 2023

Avis 6/2023

sur les propositions de règlements relatifs à la collecte et au transfert des informations préalables sur les passagers (API)

edps.europa.eu

Le Contrôleur européen de la protection des données (ci-après 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 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 concerne la proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers (API) en vue de renforcer et de faciliter les contrôles aux frontières extérieures, modifiant le règlement (UE) 2019/817 et le règlement (UE) 2018/1726 et abrogeant la directive 2004/82/CE du Conseil (COM/2022/729 final), et la proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, et modifiant le règlement (UE) 2019/818 (COM/2022/731 final).

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, 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 des deux propositions pertinentes en matière de protection des données.

Résumé

Le 13 décembre 2022, la Commission européenne a présenté deux propositions législatives relatives à la collecte et au transfert des informations préalables sur les passagers («API»): une proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers en vue de renforcer et de faciliter les contrôles aux frontières extérieures (ci-après la «proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières») et une proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière (ci-après la «proposition relative à l'utilisation des données API à des fins répressives») (prises ensemble, les «propositions»).

L'objectif de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières est de renforcer et de faciliter l'efficacité et l'efficience des vérifications aux frontières extérieures et de lutter contre l'immigration clandestine, et de remplacer l'actuelle directive 2004/82/CE du Conseil (ci-après la «directive API»). L'objectif de la proposition relative à l'utilisation des données API à des fins répressives est d'établir de meilleures règles pour la collecte et le transfert de données API par les transporteurs aériens pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, en complément de la directive (UE) 2016/681 existante (ci-après la «directive PNR»).

Compte tenu du fait que les opérations de traitement des données qui résulteraient des propositions correspondent ou complètent des opérations de traitement de données déjà existantes prévues par le droit de l'Union, l'avis se concentre principalement sur la nécessité et la proportionnalité du traitement envisagé des données API provenant de vols intra-UE et sur sa compatibilité avec la directive PNR telle qu'interprétée par l'arrêt de la CJUE dans l'affaire C-817/19.

Bien que le CEPD estime que la solution proposée pour les vols intra-UE est globalement suffisante pour garantir le respect de l'arrêt de la CJUE en ce qui concerne l'article 2 de la directive PNR, il invite néanmoins les colégislateurs à envisager l'élaboration de critères harmonisés pour la sélection des vols intra-UE, à partir desquels les données API devraient être collectées, conformément aux conditions énoncées par la Cour. En outre, le CEPD recommande de renforcer encore la sécurité du traitement des données API dans le routeur avec des garanties supplémentaires, telles que la pseudonymisation et/ou le chiffrement des données API, si cela est techniquement et opérationnellement possible.

L'avis contient également d'autres recommandations spécifiques, telles que la nécessité de préciser explicitement dans les propositions qu'en cas d'impossibilité technique pour le routeur de transmettre les données API transférées par les transporteurs aériens aux autorités nationales compétentes, les données doivent être automatiquement effacées.

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

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 13 décembre 2022, la Commission européenne a présenté deux propositions législatives sur la collecte et le transfert des informations préalables sur les passagers (ci-après les «propositions»):

- une proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers (API) en vue de renforcer et de faciliter les contrôles aux frontières extérieures, modifiant le règlement (UE) 2019/817 et le règlement (UE) 2018/1726 et abrogeant la directive 2004/82/CE du Conseil (ci-après la «proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières»),

- une proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, et modifiant le règlement (UE) 2019/818 (ci-après la «proposition relative à l'utilisation des données API à des fins répressives»).

2. L'objectif de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières est de renforcer et de faciliter l'efficacité et l'efficience des vérifications aux frontières extérieures et de lutter contre l'immigration clandestine[2], remplaçant ainsi l'actuelle directive 2004/82/CE du Conseil (la «directive API»)[3].

3. L'objectif de la proposition relative à l'utilisation des données API à des fins répressives est d'établir de meilleures règles pour la collecte et le transfert des données API par les transporteurs aériens pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière[4], en complément de la directive (UE) 2016/681 existante (ci-après la «directive PNR»)[5].

---

[1] JO L 295 du 21.11.2018, p. 39.
[2] Voir l'article 1er de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.
[3] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261 du 6.8.2004, p. 24).
[4] COM(2022) 731 final, exposé des motifs de la proposition relative à l'utilisation des données API à des fins répressives, page 3.
[5] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *JO L 119 du 4.5.2016, p. 132*.

4. Les propositions sont conformes à la stratégie de Schengen de juin 2021, présentée dans la communication de la Commission intitulée «Stratégie pour un espace Schengen pleinement opérationnel et résilient», qui soulignait spécifiquement la nécessité d'une utilisation accrue des données API en combinaison avec les données PNR afin de sensiblement améliorer la sécurité intérieure, dans le respect du droit fondamental à la protection des données à caractère personnel et du droit fondamental à la libre circulation[6]. En outre, au niveau international, le Conseil de sécurité des Nations unies et l'Organisation pour la sécurité et la coopération en Europe (OSCE) ont également demandé à plusieurs reprises la mise en place et le déploiement mondial de systèmes API et PNR à des fins répressives[7].

5. Le présent avis du CEPD est émis en réponse à une consultation présentée par la Commission européenne le 14 décembre 2022, conformément à l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au considérant 44 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières et au considérant 29 de la proposition relative à l'utilisation des données API à des fins répressives. À cet égard, le CEPD note également avec satisfaction qu'il a déjà été préalablement consulté de manière informelle en ce qui concerne les propositions, conformément au considérant 60 du RPDUE.

6. Compte tenu de la forte concordance entre les propositions[8], y compris les nombreux recoupements entre elles, il semble plus approprié pour le CEPD de les apprécier dans un seul avis.

2. Remarques générales

7. Le CEPD note que les opérations spécifiques de traitement de données prévues dans les propositions correspondent ou complètent des opérations de traitement de données déjà existantes, prévues dans le droit de l'Union. En ce qui concerne la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières, il s'agit du cadre juridique relatif aux vérifications aux frontières extérieures, en particulier le code frontières Schengen[9], et, pour la proposition relative à l'utilisation des données API à des fins répressives, il s'agit de la directive PNR déjà mentionnée.

8. En outre, le CEPD tient compte du fait que la Cour de justice de l'Union européenne (CJUE), dans une récente affaire C-817/19,[10] a confirmé la validité de la directive PNR, tout en apportant d'importantes précisions sur un certain nombre de ses dispositions, y compris, en substance, des limitations supplémentaires au traitement des données à caractère personnel afin de garantir le respect des articles 7 et 8 de la Charte. En particulier, la Cour a fixé un certain nombre de conditions que les législations nationales transposant la

[6] COM(2021) 277 final
[7] Résolutions 2178(2014), 2309(2016), 2396(2017), 2482(2019) du Conseil de sécurité des Nations unies et décision 6/16 du Conseil ministériel de l'OSCE du 9 décembre 2016 sur le renforcement de l'utilisation des renseignements préalables concernant les voyageurs.
[8] Voir le considérant 11 de la proposition relative à l'utilisation des données API à des fins répressives.
[9] Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 77 du 23.3.2016, p. 1).
[10] Arrêt de la CJUE du 21 juin 2022, affaire C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491.

directive PNR doivent respecter en ce qui concerne l'application de la directive PNR aux vols intra-UE.

9. Les exigences définies par la Cour dans son arrêt constituent un point de référence important aux fins de l'appréciation des propositions, notamment en ce qui concerne le traitement des données API provenant des vols intra-UE. Dans ce contexte, le CEPD note avec satisfaction la référence explicite à l'arrêt de la Cour au considérant 14 et dans l'exposé des motifs de la proposition relative à l'utilisation des données API à des fins répressives [11].

10. Dans le même temps, il convient de garder à l'esprit que l'arrêt de la CJUE concerne le traitement des données PNR qui comprend 18 catégories de données[12]. Les données API ne sont qu'un sous-ensemble de ces données. L'incidence du traitement des données API sur les droits fondamentaux des passagers pourrait donc être considérée comme moindre par rapport au traitement des données PNR, malgré l'obligation nouvellement créée au niveau de l'UE de collecter les données API. En outre, il convient de rappeler que les transporteurs aériens collectent déjà des données API lors de l'enregistrement des passagers (enregistrement en ligne et à l'aéroport), alors que parallèlement leurs pratiques sont diverses et incohérentes[13].

11. Enfin, en ce qui concerne la relation entre les deux propositions et le cadre juridique de l'UE en matière de protection des données, le CEPD note avec satisfaction la précision apportée selon laquelle les actes généralement applicables du droit de l'Union en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 (RGPD)[14], le RPDUE et la directive (UE) 2016/680 (LED)[15], ne seraient pas affectés par les règlements API envisagés[16]. Toutefois, le CEPD ne juge pas utile, ni exact d'indiquer que la législation proposée «compléterait» les actes généralement applicables en matière de protection des données à caractère personnel, étant donné que l'acte proposé serait simplement conforme à ces législations, comme toute législation sectorielle.

3. Traitement des données API provenant des vols intra□UE

12. À l'instar du cadre juridique actuel – la directive API et la directive PNR –, les deux propositions établissent une distinction entre les vols extra-UE et intra-UE[17]. Les données API des vols extra-UE sont traitées aux fins 1) des vérifications aux frontières extérieures et de la lutte contre l'immigration clandestine (limitée aux seuls vols à destination de l'UE), et 2) de la prévention et de la détection des infractions terroristes et des formes graves de

[11] COM(2022) 731 final, exposé des motifs de la proposition relative à l'utilisation des données API à des fins répressives, page 3.
[12] Voir annexe I de la directive PNR.
[13] COM(2022) 731 final, exposé des motifs de la proposition relative à l'utilisation des données API à des fins répressives, page 1.

[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) (texte présentant de l'intérêt pour l'EEE) (JO L 119 du 4.5.2016, p. 1).
[15] 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 (JO L 119 du 4.5.2016, p. 89).
[16] Voir le considérant 25 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières et le considérant 17 de la proposition relative à l'utilisation des données API à des fins répressives.
[17] Voir l'article 3, point c), de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières et l'article 3, point b), de la proposition relative à l'utilisation des données API à des fins répressives.

criminalité, ainsi que des enquêtes et des poursuites en la matière. Inversement, les données API des vols intra-UE ne peuvent être traitées qu'à des fins de prévention, de détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, telles que définies dans la directive PNR, et non à des fins d'immigration.

13. Le CEPD note que, conformément à l'article 2 et à l'article 4, paragraphes 1 et 6 de la proposition relative à l'utilisation des données API à des fins répressives, les transporteurs aériens seraient tenus de collecter et de transférer ensuite à un «routeur» les données API relatives à [tous] «les vols extra-UE ou intra-UE, réguliers ou non»[18]. Le routeur transmettrait alors aux unités d'informations passagers (UIP) des États membres sur le territoire desquels le vol décollera et atterrira uniquement les données API des vols intra-UE sélectionnés par les États membres conformément à l'article 2 de la directive PNR, tel qu'interprété dans l'arrêt de la CJUE. À cette fin, l'eu-LISA conserverait une liste confidentielle des vols intra-UE sélectionnés, qui serait régulièrement mise à jour[19].

14. Le CEPD note en outre que, conformément à l'article 12, point b), de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières, les données API de vols intra-UE autres que ceux figurant sur la liste seraient effacées du routeur «immédiatement, de manière définitive et automatisée». De même, les transporteurs aériens seraient tenus d'effacer immédiatement et de manière définitive les données API des vols intra-UE lorsque le transfert au routeur a été effectué[20].

15. Selon la Commission, la solution technique proposée vise à limiter la transmission des données API aux UIP pour les seuls vols désignés et sans divulguer d'informations confidentielles concernant les vols intra-UE sélectionnés, compte tenu du risque de contournement par les personnes participant à des formes graves de criminalité ou à des activités terroristes[21].

16. Le CEPD est d'avis que, lors de l'évaluation de la conformité de la solution proposée pour les vols intra-UE, les conditions énoncées dans l'arrêt de la CJUE précité, tout en constituant un point de référence important, doivent être appliquées par analogie (*mutatis mutandis*). La Cour a précisé qu'une ingérence dans les articles 7 et 8 de la Charte peut être justifiée en appréciant la gravité de l'ingérence et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité[22]. Dans le contexte actuel, il convient de tenir compte du fait que l'arrêt concerne un système différent impliquant, entre autres, le traitement de bien plus de catégories de données à caractère personnel que l'API. Par conséquent, le CEPD considère que la proposition entraînerait un niveau d'ingérence dans ces droits fondamentaux inférieur à celui envisagé par la Cour.

17. Selon la CJUE, le droit de l'Union, notamment l'article 2 de la directive 2016/681, lu à la lumière de l'article 3, paragraphe 2, TUE, de l'article 67, paragraphe 2, TFUE et de l'article 45 de la Charte, s'oppose à une législation nationale établissant un système de

[18] Il semble y avoir une contradiction (erreur matérielle possible) à l'article 1er, point a), de la proposition relative à l'utilisation des données API à des fins répressives, qui fait référence à certains vols intra-UE. Toutefois, il ressort clairement de l'article 4 et des explications générales des considérants et de l'exposé des motifs (page 10) de cette même proposition que la sélection envisagée doit avoir lieu après le transfert au routeur afin d'éviter de divulguer les vols sélectionnés.
[19] Voir l'article 5 et le considérant 14 de la proposition relative à l'utilisation des données API à des fins répressives.
[20] Article 4, paragraphe 8, point b), de la proposition relative à l'utilisation des données API à des fins répressives.
[21] COM(2022) 731 final, exposé des motifs de la proposition relative à l'utilisation des données API à des fins répressives, page 11.
[22] Voir arrêt de la CJUE du 21 juin 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, point 116, et arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55, et jurisprudence citée.

transfert, par les transporteurs aériens, et de traitement, par les autorités compétentes, des données PNR de tous les vols intra-UE. En revanche, un tel traitement peut être autorisé lorsqu'un État membre est «confronté à une menace terroriste qui s'avère réelle et actuelle ou prévisible»[23].

18. Dans ce contexte, la question pertinente est de savoir si la solution technique proposée conduit ou non, dans la pratique, à un transfert indifférencié des données API de tous les vols intra-UE aux autorités nationales compétentes (UIP), en dehors des situations exceptionnelles de menace terroriste.

19. Selon le CEPD, le traitement automatique envisagé au sein du routeur – le «filtrage» des données API sur la base d'une liste officielle d'aéroports ou de liaisons sélectionnés, la transmission des données des seuls vols présélectionnés et la suppression immédiate des données des vols non sélectionnés, empêche pour les UIP de recevoir et de traiter de quelque manière que ce soit les données API des vols intra-UE pour lesquels elles ne sont pas autorisés.

20. En outre, le CEPD considère que la collecte et le transfert au routeur des données API, d'une part, et le traitement des données API par les autorités nationales compétentes, d'autre part, sont intrinsèquement liés et ne devraient donc pas être considérés isolément. Par conséquent, étant donné qu'il est non seulement juridiquement interdit aux États membres d'accéder aux données API des vols intra-UE qu'ils n'ont pas officiellement sélectionnés et communiqués, mais qu'il leur est également techniquement impossible d'accéder à ces données, le CEPD considère que cet élément des propositions est conforme à la législation européenne pertinente telle qu'interprétée par la CJUE.

21. En outre, le CEPD croit comprendre qu'à ce stade, il n'existe aucune solution alternative satisfaisante (facilement disponible, techniquement viable et économiquement efficace) qui offrirait des garanties comparables pour les vols intra-UE.

22. Par exemple, le transfert des données API par les transporteurs aériens pour tous les vols intra-UE directement aux UIP, en laissant aux États membres le soin de décider quelles données API sont nécessaires et d'effacer le reste, semble problématique. En effet, cela impliquerait un traitement systématique par les autorités nationales des données de tous les vols intra-UE, y compris de ceux qu'elles n'ont pas sélectionnés.

23. De son côté, le «filtrage» des données API au niveau des transporteurs aériens n'offre pas de garanties suffisantes et pourrait créer des difficultés supplémentaires en matière de confidentialité (par exemple, le contournement par des personnes participant à des formes graves de criminalité ou à des activités terroristes), de fiabilité et de cohérence du traitement, puisque les données API seront filtrées par de multiples acteurs sur la base d'instructions provenant de tous les États membres. À cet égard, il convient de noter que, selon l'analyse d'impact jointe aux propositions, il existe actuellement environ 1000 transporteurs aériens opérant dans l'UE, dont environ 150 opèrent exclusivement au sein de l'Union[24].

[23] Arrêt de la CJUE du 21 juin 2022, affaire C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491, p. 7 de l'arrêt et points 171 et 173.
[24] SWD(2022) 422 final, rapport d'analyse d'impact, annexe 4, page 71.

24. Il s'ensuit que le traitement de toutes les données API ayant lieu au niveau du routeur, compte tenu du niveau d'ingérence dans les droits fondamentaux concernés, des garanties prévues, notamment l'impossibilité juridique et technique pour les UIP des États membres de recevoir et de traiter d'une autre manière des données API non liées aux vols sélectionnés, reste proportionné à l'objectif poursuivi.

25. Enfin, le CEPD rappelle que, conformément à l'arrêt de la CJUE, la sélection des vols intra-UE doit être limitée au strict nécessaire. À cette fin, le choix des États membres doit être justifié sur la base d'indications [objectives] et faire l'objet de réexamens réguliers[25]. Par conséquent, afin d'éviter des pratiques divergentes, le CEPD invite les colégislateurs à envisager d'introduire des dispositions, y compris une délégation spécifique à la Commission conformément aux articles 290 et/ou 291 du TFUE si cela est jugé approprié, pour l'élaboration de critères et de méthodes harmonisés aux fins de la sélection des vols intra-UE, à partir desquels les données API devraient être collectées.

4. Sécurité des données API

26. Compte tenu de l'ampleur du traitement et du nombre de personnes concernées, la collecte et le transfert envisagés de données API peuvent potentiellement engendrer des risques et doivent donc s'accompagner de garanties efficaces assurant un niveau élevé de sécurité. À cet égard, le CEPD note que la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières prévoit une disposition détaillée sur la sécurité des données API et du routeur, en plus des obligations générales relatives à la sécurité des données à caractère personnel conformément à l'article 33 du RPDUE et à l'article 32 du RGPD[26]. Dans le même temps, la disposition correspondante de la proposition relative à l'utilisation des données API à des fins répressives[27] est très générale et ne prévoit aucune mesure spécifique, ni ne fait référence aux règles pertinentes de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.

27. Par ailleurs, le CEPD rappelle l'obligation des autorités des États membres, des transporteurs aériens et de l'eu-LISA de mettre en œuvre des mesures techniques et organisationnelles appropriées conformément aux exigences en matière de protection des données dès la conception et par défaut, en vertu de l'article 27 du RPDUE, de l'article 25 du RGPD et à l'article 20 de la directive en matière de protection des données dans le domaine répressif.

28. Le CEPD recommande donc que la proposition relative à l'utilisation des données API à des fins répressives prévoie des mesures spécifiques garantissant la sécurité des données API traitées aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, ou, à défaut, qu'elle fasse référence aux règles pertinentes de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.

[25] Voir arrêt de la CJUE du 21 juin 2022, affaire C-817/19, Ligue des droits humains, point 174.
[26] Article 17 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.
[27] Article 8 de la proposition relative à l'utilisation des données API à des fins répressives.

29. En outre, le CEPD recommande à l'eu-LISA, lors de la conception et du développement du routeur, d'envisager l'utilisation de la pseudonymisation et/ou du chiffrement des données API, si cela est techniquement et opérationnellement possible.

5. Rôles et responsabilités

30. Les propositions désigneraient les transporteurs aériens comme responsables du traitement, au sens de l'article 4, paragraphe 7, du RGPD, des données API constituant des données à caractère personnel en ce qui concerne la collecte de ces données et leur transfert vers le routeur[28].

31. En outre, les autorités frontalières compétentes sont désignées comme responsables du traitement des données API constituant des données à caractère personnel par l'intermédiaire du routeur, y compris la transmission, ainsi qu'en ce qui concerne leur traitement des données API constituant des données à caractère personnel en vertu de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières. De même, les UIP seraient des responsables du traitement, au sens de l'article 3, paragraphe 8, de la directive (UE) 2016/680, en ce qui concerne le traitement des données API constituant des données à caractère personnel par l'intermédiaire du routeur, y compris la transmission, en vertu de la proposition relative à l'utilisation des données API à des fins répressives.

32. Enfin, l'eu-LISA est désignée comme sous-traitant au sens de l'article 3, paragraphe 12, du règlement (UE) 2018/1725 pour le traitement des données API constituant des données à caractère personnel par l'intermédiaire du routeur[29].

33. Compte tenu de la répartition des responsabilités entre les différents acteurs, interprétée à la lumière des dispositions pertinentes du RGPD, du RPDUE et de la directive en matière de protection des données dans le domaine répressif, et compte tenu également des lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement en vertu du règlement (UE) 2018/1725[30] ainsi que les lignes directrices 07/2020 du comité européen de la protection des données (EDPB) sur les notions de responsable du traitement et de sous-traitant dans le RGPD[31], le CEPD considère que cette attribution des rôles est appropriée, pour les raisons suivantes.

34. Le CEPD note que les autorités des États membres, agissant en tant que responsables du traitement, déterminent les finalités et les moyens essentiels du traitement par l'intermédiaire du routeur, dans le cadre juridique établi par les propositions. Selon les lignes directrices du comité européen de la protection des données, les «moyens essentiels» sont étroitement liés à la finalité et à la portée du traitement. En ce qui concerne les finalités, bien que l'eu-LISA traite toutes les données API, en définitive les données traitées par les autorités des États membres sont uniquement les données relatives aux vols sélectionnés

[28] Voir l'article 15 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières et l'article 7 de la proposition relative à l'utilisation des données API à des fins répressives.
[29] Article 16 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.
[30] https://edps.europa.eu/sites/default/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf
[31] https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

par les États membres. Ces derniers déterminent donc quels sous-ensembles spécifiques de données ils recevront et «pourquoi» au sens des lignes directrices 7/2020 du comité européen de la protection des données précitées[32]. En ce qui concerne les moyens essentiels, ils sont déterminés par la loi: les données API qui sont présentées à l'eu-LISA; la durée du traitement; les catégories de destinataires (les UIP compétentes et les autorités frontalières) et les catégories de personnes concernées dont les données à caractère personnel seront traitées (voyageurs aériens qui relèvent du champ d'application des règlements API).

35. Les «moyens non essentiels» concernent des aspects plus pratiques de la mise en œuvre, tels que le choix d'un type particulier de matériel ou de logiciel ou les mesures de sécurité concrètes – ce que l'eu-Lisa est censée faire – qui pourraient être laissés à la discrétion du sous-traitant. En outre, selon l'EDPB, il n'est pas nécessaire que le responsable du traitement ait effectivement accès aux données qui sont traitées (c'est-à-dire aux données du routeur).

36. Dans la pratique, l'eu-LISA offre un canal de communication entre les transporteurs aériens et les responsables du traitement des États membres, plutôt qu'une base de données autonome (il n'y a pas de véritable stockage des données API dans le routeur). L'Agence n'a pas d'autres finalités pour le traitement des données API que de les transmettre aux responsables du traitement compétents dans les États membres.

37. Nonobstant la désignation de l'eu-LISA en tant que sous-traitant pour le compte des autorités des États membres, les propositions confèrent à l'Agence une responsabilité importante pour garantir un traitement licite et sécurisé des données API dans le routeur. L'eu-LISA doit garantir, entre autres, que seules les données API correctement sélectionnées concernant les vols intra-UE parviendront aux unités d'informations passagers, l'effacement des données API restantes, ainsi qu'un niveau élevé de sécurité pour empêcher tout accès non autorisé aux données[33].

38. À cet égard, le CEPD rappelle que le RPDUE ne fait pas de distinction entre les responsables du traitement et les sous-traitants en ce qui concerne les pouvoirs de contrôle du CEPD au titre de l'article 58 ou les éventuelles sanctions en cas d'infraction au titre de l'article 66 dudit règlement. En tout état de cause, le CEPD prévoit de contrôler de près l'exercice des tâches de l'eu-LISA dans le cadre des propositions, conformément à son mandat en vertu du RPDUE.

6. Établissement de rapports et de statistiques

39. Le CEPD note que, conformément à l'article 31 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières, l'eu-LISA serait chargée de stocker les statistiques journalières provenant du traitement des données dans le routeur dans le répertoire central des rapports et statistiques (CRRS) créé par l'article 39 du

[32] Lignes directrices 07/2020 de l'EDPB sur les notions de responsable du traitement et de sous-traitant dans le RGPD, paragraphe 35.
[33] Voir les articles 17 et 22 à 24 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.

règlement (UE) 2019/817 (règlement sur l'interopérabilité)[34] ainsi que de produire divers rapports statistiques. À cette fin, l'eu-LISA disposerait d'un droit d'accès à certaines données API transmises au routeur, «sans toutefois que cet accès permette l'identification des voyageurs concernés».

40. Dans son avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité[35], le CEPD a déjà mis en garde contre le fait que la création du CRRS proposée imposerait une lourde charge à l'eu-LISA. Le CEPD a exprimé cette position à plusieurs reprises dans ses avis sur l'EES[36], l'ETIAS[37], le SIS[38], le VIS[39] et l'agence eu-LISA[40]. Dans ce contexte, le CEPD a émis un certain nombre de recommandations relatives au CRRS, y compris la nécessité de réaliser une évaluation approfondie des risques dans le domaine de la sécurité de l'information, de mettre en œuvre des mesures de sécurité adéquates et d'appliquer le respect de la vie privée dès la conception. Ces recommandations restent pleinement valables dans le contexte des propositions.

7. Effacement des données API du routeur

41. L'article 12 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières prévoirait deux situations qui entraîneraient l'effacement automatique des données API du routeur:
a) lorsque la transmission des données API aux autorités frontalières compétentes ou aux UIP concernées, selon le cas, a été achevée;
b) en ce qui concerne la proposition relative à l'utilisation des données API à des fins répressives, lorsque les données API se rapportent à d'autres vols intra-UE que ceux figurant sur les listes visées à l'article 5, paragraphe 2, dudit règlement (c'est-à-dire non sélectionnées par un État membre).

42. Le CEPD note également que l'article 14 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières décrit les mesures à prendre en cas d'impossibilité technique d'utiliser le routeur. En général, dans de telles situations, les transporteurs aériens n'auraient aucune obligation de transférer les données API au routeur. Toutefois, les propositions ne mentionnent pas explicitement ce qui devrait se passer si un transporteur aérien a transféré des données API au routeur avant de prendre connaissance d'une impossibilité technique pour le routeur de transmettre ultérieurement les données API en raison d'une défaillance des systèmes ou de l'infrastructure d'un ou des États membres.

43. Le CEPD recommande donc de préciser à l'article 12 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières qu'en cas d'impossibilité

[34] Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil (JO L 135 du 22.5.2019, p. 27).
[35] https://edps.europa.eu/sites/default/files/publication/2018-04-16_interoperability_opinion_en.pdf
[36] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf
[37] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf
[38] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf
[39] https://edps.europa.eu/sites/default/files/publication/18-12-13_opinion_vis_en.pdf
[40] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf

technique du routeur de transmettre ultérieurement les données API aux autorités nationales compétentes, les données sont automatiquement effacées.

8. Autres observations

44. Le CEPD note que l'article 4, paragraphe 1, deuxième phrase, de la proposition relative à l'utilisation des données API à des fins répressives indique spécifiquement à qui incombe l'obligation de transférer les données API lorsqu'il s'agit d'un vol en partage de code entre plusieurs transporteurs aériens. Toutefois, la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières ne contient pas de règle similaire. Par conséquent, le CEPD recommande d'ajouter une disposition similaire sur les vols en partage de code également dans la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières.

9. Conclusions

45. À la lumière des considérations qui précèdent, le CEPD recommande aux colégislateurs:

(1) d'envisager l'élaboration de critères et d'une méthodologie harmonisés pour la sélection des vols intra-UE, à partir desquels les données API devraient être collectées;

(2) de prévoir des mesures spécifiques dans la proposition relative à l'utilisation des données API à des fins répressives garantissant la sécurité des données API traitées aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, ou, à défaut, faire référence aux règles pertinentes en matière de sécurité dans la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières;

(3) de préciser à l'article 12 de la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières qu'en cas d'impossibilité technique pour le routeur de transmettre ultérieurement les données API aux autorités nationales compétentes, les données devront être automatiquement effacées;

(4) de préciser, dans la proposition relative à la collecte et au transfert des données API aux fins de la gestion des frontières, à qui incombe l'obligation de transférer les données API lorsqu'il s'agit d'un vol en partage de code entre plusieurs transporteurs aériens.

Bruxelles, le 8 février 2023

(signature électronique)
Wojciech Rafał WIEWIÓROWSKI