EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

30 octobre 2023

Avis 47/2023

sur le mandat de négociation d'un accord entre l'Union européenne et la Suisse pour le transfert de données des dossiers passagers

edps.europa.eu

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE, 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, du même règlement, «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 porte sur la recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la Confédération suisse sur le transfert de données des dossiers passagers depuis l'Union vers la Confédération suisse 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[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) 509 final.

Résumé

Le 6 septembre 2023, la Commission européenne a publié une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la Confédération suisse sur le transfert de données des dossiers passagers (PNR) depuis l'Union vers la Confédération suisse 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. L'objectif du futur accord est de permettre à la Suisse de recevoir en toute légalité des données PNR des États membres de l'Union et d'autoriser son autorité compétente désignée à utiliser ces données d'une manière qui garantisse la sécurité des personnes se déplaçant au sein d'un espace commun sans contrôles aux frontières intérieures ainsi que la protection des données à caractère personnel les concernant.

Dans son avis, le CEPD rappelle la situation juridique spécifique de la Suisse en tant que pays associé à l'espace Schengen. Conformément à l'accord d'association de Schengen entre l'Union européenne et la Suisse de 2008, la Suisse est liée par les actes de l'Union qui constituent un développement des dispositions de l'acquis de Schengen. Par conséquent, la Suisse est censée appliquer la directive (UE) 2016/680 de manière similaire aux États membres de l'Union. En outre, il a été considéré en 2000 que la Suisse assurait un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union en vertu de la directive 95/46/CE. Cette décision relative à l'adéquation du niveau de protection des données continue d'être en vigueur dans le cadre du RGPD.

Toutefois, la directive PNR de l'Union ne constitue pas un développement des dispositions de l'acquis de Schengen et, par conséquent, la Suisse n'est pas liée par ses dispositions. Par conséquent, le CEPD souligne la nécessité pour le futur accord PNR entre l'Union et la Suisse d'introduire toutes les garanties appropriées en ce qui concerne le traitement des données PNR, conformément au droit de l'Union applicable, tel qu'il a été interprété par la CJUE.

Outre cette observation générale, le CEPD formule deux recommandations spécifiques. Premièrement, il recommande d'aligner la définition des données sensibles dans le mandat de négociation sur les définitions des catégories particulières de données figurant dans le RGPD et dans la directive (UE) 2016/680. Deuxièmement, le CEPD propose d'introduire dans les directives de négociation les possibilités juridiques de suspendre l'accord en cas de violation de ses dispositions, ainsi que de le résilier si le non-respect est grave et persistant.

Table des matières

1. Introduction 4

2. Remarques d'ordre général 5

3. Données sensibles 7

4. Suspension et résiliation 8

5. Conclusions 8

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»)[2], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 6 septembre 2023, la Commission européenne a publié une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la Confédération suisse sur le transfert de données des dossiers passagers (PNR) depuis l'Union vers la Confédération suisse 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[3] (ci-après la «recommandation»).

2. L'objectif de la recommandation est de permettre à la Suisse de recevoir en toute légalité des données PNR de l'Union et d'autoriser son autorité compétente désignée d'utiliser ces données d'une manière qui garantisse, en même temps, la sécurité des personnes déplaçant au sein d'un espace commun sans contrôles aux frontières intérieures ainsi que la protection des données à caractère personnel les concernant[4].

3. La recommandation s'inscrit dans le cadre plus large des efforts déployés par la Commission pour appliquer une approche cohérente et efficace quant au transfert des données PNR vers des pays tiers, comme annoncé dans la stratégie pour l'Union de la sécurité 2020-2025[5] et demandé par le Conseil dans ses conclusions de juin 2021[6], conformément au droit et à la jurisprudence de l'Union en matière de PNR[7].

4. Le présent avis du CEPD est émis en réponse à une consultation de la Commission européenne du 6 septembre 2023, conformément à l'article 42, paragraphe 1, du RPDUE.

[2] JO L 295 du 21.11.2018, p. 39.
[3] COM(2023) 509 final.
[4] Voir COM(2023) 509 final, exposé des motifs, p. 4.
[5] Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final.
[6] Conclusions du Conseil du 7 juin 2021 sur le transfert de données des dossiers passagers (données PNR) à des pays tiers, document 9605/21 du Conseil du 8 juin 2021.
[7] Voir COM(2023) 509 final, exposé des motifs, p. 3.

2. Remarques d'ordre général

5. Les données PNR sont des informations fournies par les passagers, collectées et conservées dans les systèmes de contrôle des réservations et des départs des transporteurs aériens à leurs propres fins commerciales. Bien qu'utiles pour la lutte antiterroriste et la lutte contre les formes graves de criminalité, le transfert de données PNR vers des pays tiers et le traitement ultérieur de celles-ci par les autorités de ces pays constituent une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la charte des droits fondamentaux (ci-après la «charte»). C'est la raison pour laquelle le transfert exige une base juridique en vertu du droit de l'Union et doit être nécessaire, proportionné et soumis à des limitations strictes et à des garanties efficaces.

6. Outre la charte, les règles juridiques applicables en cas de transfert et de traitement de données PNR comprennent également le cadre juridique horizontal de l'Union sur la protection des données, à savoir le règlement (UE) 2016/679 (le RGPD)[8] et la directive (UE) 2016/680 (la directive sur la protection des données dans le domaine répressif)[9], ainsi que la directive spécifique (UE) 2016/681 (la directive relative à l'utilisation des données PNR de l'UE)[10].

7. En outre, comme souligné dans la recommandation[11], la Cour de justice de l'Union européenne (CJUE) a, à deux reprises, interprété le cadre juridique relatif aux dossiers passagers et fourni des orientations en ce qui concerne la proportionnalité et la nécessité du traitement des données PNR, à savoir dans l'avis 1/15 du 26 juillet 2017[12] et dans l'arrêt rendu le 21 juin 2022 dans l'affaire C-817/2019[13]. Les exigences définies par la CJUE dans la jurisprudence citée constituent un point de référence important pour l'évaluation de la présente recommandation et de tout futur accord de l'Union sur le transfert de données PNR.

8. Le CEPD rappelle également que, en plus d'être soumises à la législation de l'Union, les données PNR sont soumises à des règles et normes internationales. La résolution 2396 (2017) du Conseil de sécurité des Nations unies sur les menaces contre la paix et la sécurité internationales causées par les combattants terroristes étrangers qui reviennent vers leur pays, adoptée le 21 décembre 2017, et la résolution 2482 (2019) ultérieure du Conseil de sécurité des Nations unies du 19 juillet 2019, ont appelé les États membres des Nations unies à développer la capacité de collecter et d'utiliser les données PNR, sur la base des normes et pratiques recommandées en matière de PNR (SARP) de l'Organisation de l'aviation civile internationale (OACI) à partir de 2020, adoptées au moyen de l'amendement 28 à l'annexe 9 de la convention relative à l'aviation civile

[8] 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) (JO L 119 du 4.5.2016, p. 1).

[9] 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. 89–131).

[10] 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. 132-149.

[11] Voir COM(2023) 509 final, p. 2 et 5.

[12] Avis 1/15 de la Cour (grande chambre) du 26 juillet 2017, EU:C:2017:592.

[13] Arrêt de la Cour (grande chambre) du 21 juin 2022 «Ligue des droits humains», C-817/19, EU:C:2022:491.

internationale (convention de Chicago)[14]. Tous les États membres de l'Union, ainsi que la Suisse, sont parties à la Convention de Chicago.

9. Un autre aspect important qui mérite une attention particulière est la situation juridique de la Suisse en tant que pays associé à l'espace Schengen. Conformément à l'article 7 de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen de 2008[15], la Suisse est liée par les actes de l'Union qui constituent un développement des dispositions de l'acquis de Schengen. Bien que le processus ne soit pas automatique et nécessite l'acceptation par la Suisse du contenu des actes et mesures respectifs de l'Union et, le cas échéant, le respect des exigences constitutionnelles nationales, il crée néanmoins des obligations juridiques claires pour la Suisse en ce qui concerne la mise en œuvre et l'application de la législation de l'Union en question. En outre, conformément à l'article 7, paragraphe 4, de l'accord d'association à Schengen de 2008, si la Suisse n'acceptait pas le contenu de l'acte de l'Union concerné ou ne procédait pas à la transposition dans son ordre juridique interne, ledit accord devrait être considéré comme résilié. En outre, conformément à l'article 9 de l'accord d'association à Schengen de 2008, la Suisse doit présenter des rapports annuels sur la manière dont ses autorités administratives et ses juridictions appliquent et interprètent les dispositions de l'acquis de Schengen, telles qu'interprétées par la CJUE, le cas échéant.

10. Le CEPD rappelle également que la Suisse est juridiquement liée par le cadre de l'Union en matière de protection des données applicable au traitement des données à caractère personnel par les autorités compétentes aux fins de prévention, de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Le considérant 102 de la *directive sur la protection des données dans le domaine répressif* indique explicitement que cette directive «constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen». Par conséquent, comme nous l'avons déjà expliqué ci-dessus, la Suisse a l'obligation de transposer la directive sur la protection des données dans le domaine répressif dans son ordre juridique interne et de l'appliquer dans la pratique.

11. En ce qui concerne la protection des données en général, y compris les transferts par les transporteurs aériens, le CEPD rappelle qu'il a été considéré que la Suisse assurait un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union en 2000[16], en vertu de la directive 95/46/CE[17]. Conformément à l'article 45, paragraphe 9, du RGPD, cette décision reste en vigueur jusqu'à sa modification, son remplacement ou son abrogation par une décision de la Commission adoptée conformément au paragraphe 3 ou 5 de l'article 45 du RGPD.

12. À l'inverse, le CEPD rappelle que la directive relative à l'utilisation des données PNR ne constitue pas un développement des dispositions de l'acquis de Schengen et que, par

[14] Voir https://www.icao.int/safety/airnavigation/nationalitymarks/annexes_booklet_en.pdf
[15] JO L 53 du 27.2.2008, pp. 52-79.
[16] Décision 2000/518/CE de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, JO L 215 du 25.8.2000, p. 1.
[17] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31.

conséquent, la Suisse n'est pas liée par ses dispositions. Par conséquent, le futur accord PNR entre l'Union et la Suisse devrait prévoir toutes les garanties appropriées en ce qui concerne le traitement des données PNR, conformément au droit de l'Union applicable, tel qu'il est interprété par la CJUE.

13. Outre ces observations générales, le CEPD formule deux recommandations spécifiques concernant le mandat de négociation en ce qui concerne le transfert de données sensibles et la suspension et la résiliation de l'accord.

3. Données sensibles

14. La directive de négociation figurant au point 10 de l'annexe de la recommandation dispose que le futur accord doit veiller à ce que les «données sensibles au sens du droit de l'Union» ne soient pas traitées. À cet égard, les «données sensibles» sont définies comme des «données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, ou qui concernent sa santé ou sa vie ou son orientation sexuelle». Toutefois, les définitions des catégories particulières de données (données sensibles) dans le RGPD et la directive sur la protection des données dans le domaine répressif comprennent deux catégories supplémentaires: «données génétiques et données biométriques aux fins d'identifier une personne physique de manière unique».

15. Le CEPD note que la définition des données sensibles figurant dans le mandat de négociation est identique à celle figurant à l'article 13, paragraphe 4, de la directive relative à l'utilisation des données PNR. Dans ce contexte, le CEPD rappelle que si la directive relative à l'utilisation des données PNR a été adoptée en même temps que le RGPD et la directive sur la protection des données dans le domaine répressif, pour des raisons de technique juridique, elle fait référence aux prédécesseurs abrogés de ces actes juridiques, à savoir la directive 95/46/CE[18] et la décision-cadre 2008/977/JAI[19]. Conformément à l'article 94 du RGPD et à l'article 59 de la directive sur la protection des données dans le domaine répressif, à compter de mai 2018, les références aux actes abrogés relatifs à la protection des données dans la directive relative à l'utilisation des données PNR s'entendent comme des références aux actes juridiques actuels respectifs. En d'autres termes, la nouvelle norme plus élevée de l'Union en matière de protection des données à caractère personnel s'applique également dans le cadre du traitement des données PNR.

16. Compte tenu de ce qui précède, le CEPD recommande d'aligner la définition des données sensibles figurant au paragraphe 10 de l'annexe de la recommandation sur les définitions des catégories particulières de données figurant à l'article 9, paragraphe 1, du RGPD et à l'article 10 de la directive sur la protection des données dans le domaine répressif, en remplaçant la liste des catégories de données considérées comme sensibles par une référence aux dispositions respectives de la législation de l'Union en matière de protection

[18] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31.
[19] 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.

des données ou, à défaut, en ajoutant «données génétiques et données biométriques aux fins d'identifier une personne physique de manière unique».

4. Suspension et résiliation

17. La directive de négociation figurant au point 18 de l'annexe de la recommandation dispose que l'accord doit être conclu pour une durée déterminée, mais comporte une disposition en vertu de laquelle l'accord doit être renouvelé pour des périodes similaires, à moins qu'une partie ne notifie sa décision de le résilier. Toutefois, le mandat de négociation ne fait pas référence à la possibilité juridique de suspendre ou de résilier l'accord avant l'expiration de ce délai déterminé, en cas de violation substantielle ou de non-respect des obligations découlant dudit accord par la partie contractante. Le CEPD tient à rappeler que ce type de clause de suspension n'est pas seulement un élément standard des accords internationaux[20] et fait généralement également partie des accords internationaux de l'Union[21], mais il s'agit aussi d'une garantie importante pour les droits des personnes concernées par le transfert de données à caractère personnel conformément à l'accord.

18. Le CEPD recommande donc d'introduire dans les directives de négociation la possibilité juridique de suspendre l'accord en cas de violation de ses dispositions, ainsi que de le résilier si le non-respect est grave et persistant. La disposition correspondante du futur accord devrait également préciser la procédure applicable en ce qui concerne les données à caractère personnel transférées vers la Suisse avant sa suspension ou sa résiliation.

5. Conclusions

19. Eu égard aux considérations qui précèdent, le CEPD formule les recommandations suivantes:

(1) introduire dans le futur accord PNR entre l'Union et la Suisse toutes les garanties appropriées concernant le traitement des données PNR, conformément au droit de l'Union applicable, tel qu'interprété par la CJUE, en tenant compte du fait que la directive relative à l'utilisation des données PNR ne constitue pas un développement des dispositions de l'acquis de Schengen et que, par conséquent, la Suisse n'est pas liée par ses dispositions;

(2) aligner la définition des données sensibles figurant au paragraphe 10 de l'annexe de la recommandation sur les définitions des catégories particulières de données figurant à l'article 9, paragraphe 1, du RGPD et à l'article 10 de la directive en matière de protection des données dans le domaine répressif, en remplaçant la liste des catégories de données considérées comme sensibles par une référence aux dispositions respectives de la législation de l'Union en matière

[20] Voir la section 3 de la convention de Vienne sur le droit des traités, Vienne, 23 mai 1969.
[21] Voir, par exemple, plus récemment, l'article 19 de l'accord entre l'Union européenne et la Nouvelle-Zélande sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités néo-zélandaises compétentes pour lutter contre les formes graves de criminalité et le terrorisme, JO L 51 du 20.2.2023, p. 4.

de protection des données ou, à défaut, en ajoutant «données génétiques et données biométriques aux fins d'identifier une personne physique de manière unique»;

(3) *introduire dans les directives de négociation la possibilité juridique de suspendre l'accord en cas de violation de ses dispositions, ainsi que de le résilier si le non-respect est grave et persistant.*

Bruxelles, le 30 octobre 2023

(signature électronique)
Wojciech Rafał WIEWIÓROWSKI