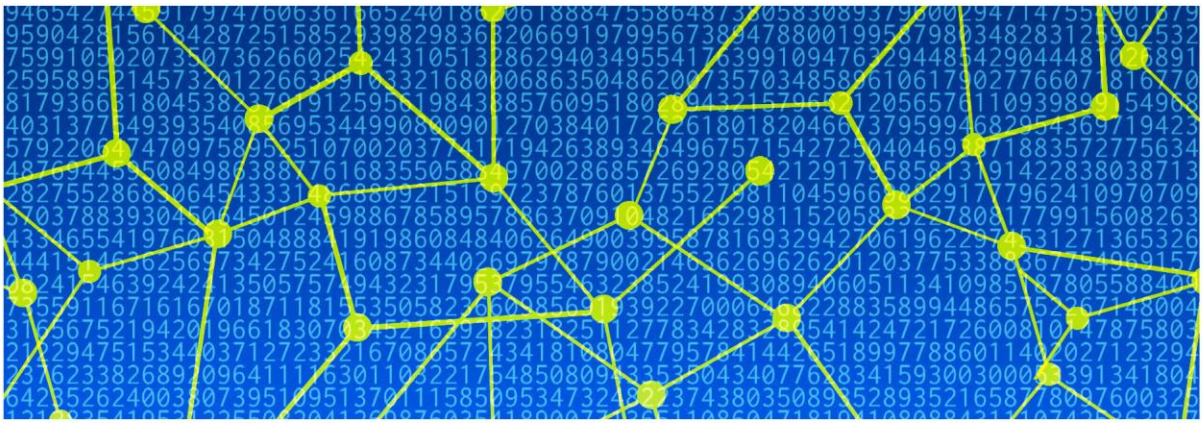

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 1/2020

Avis du CEPD sur le mandat de négociation en vue de la conclusion d'un accord international sur l'échange de données à caractère personnel entre Europol et les autorités répressives néo-zélandaises

EDPS

31 janvier 2020

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

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 se rapporte à la mission du CEPD de conseiller les institutions de l'Union européenne sur l'application cohérente et logique des principes de protection des données de l'Union européenne lors de la négociation d'accords dans le secteur répressif. Il s'appuie sur l'obligation générale exigeant que les accords internationaux soient conformes aux dispositions du traité sur le fonctionnement de l'Union européenne (le «TFUE») et respectent les droits fondamentaux qui forment le noyau du droit de l'Union. En particulier, il convient de veiller au respect des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 16 du TFUE.

Synthèse

Le 30 octobre 2019, la Commission européenne a adopté une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un 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. L'accord envisagé a pour objectif de constituer la base juridique du transfert de données à caractère personnel entre Europol et les autorités compétentes de la Nouvelle-Zélande respectivement, afin d'appuyer et de renforcer leurs actions ainsi que leur collaboration mutuelle dans la prévention des formes graves de criminalité transnationale et du terrorisme et dans la lutte contre ceux-ci, tout en offrant des garanties appropriées en ce qui concerne la protection de la vie privée, des données à caractère personnel et des autres libertés et droits fondamentaux des personnes.

Les transferts de données à caractère personnel collectées dans le cadre d'enquêtes pénales et traitées ensuite par Europol pour produire des renseignements en matière pénale sont susceptibles d'avoir une incidence considérable sur la vie des personnes concernées. C'est pourquoi l'accord international doit garantir que les limitations des droits à la vie privée et à la protection des données dans le cadre de la lutte contre les formes graves de criminalité et le terrorisme s'opèrent dans les limites du strict nécessaire.

Le CEPD note que la Nouvelle-Zélande dispose d'une législation nationale bien établie en matière de protection des données et d'une autorité indépendante chargée de la protection des données, compétente pour superviser également les autorités répressives. En outre, il salue le fait que la Commission ait intégré dans la proposition de mandat de négociation avec la Nouvelle-Zélande un certain nombre de recommandations spécifiques déjà indiquées par le CEPD dans son avis 2/2018 sur huit mandats de négociation en vue de la conclusion d'accords internationaux autorisant l'échange de données entre Europol et des pays tiers.

Par conséquent, les recommandations formulées dans le présent avis visent à préciser et, le cas échéant, à développer davantage les garanties et les contrôles en matière de protection des données à caractère personnel, en tenant compte du contexte spécifique de la Nouvelle-Zélande. À cette fin, le CEPD formule les recommandations suivantes:

– la décision du Conseil autorisant l'ouverture de négociations en vertu de l'article 218 du TFUE devrait comporter une référence non seulement à la base juridique procédurale, mais également à la base juridique matérielle pertinente, qui devrait comprendre l'article 16 du TFUE;

– conformément au principe de limitation de la finalité, l'accord envisagé devrait établir explicitement la liste des infractions pénales pour lesquelles des données à caractère personnel pourraient être échangées;

– en vue de la mise en œuvre concrète du principe de limitation de la conservation, le futur accord devrait prévoir expressément un examen périodique de la nécessité de conserver les données à caractère personnel qui ont été transférées;

– étant donné l'importance du droit à l'information pour l'exercice des autres droits en matière de protection des données, l'accord devrait comporter des règles claires et détaillées concernant les informations qui devraient être fournies aux personnes concernées.

Enfin, le CEPD s'attend à être consulté à des stades ultérieurs de la finalisation du projet d'accord, conformément à l'article 42 du règlement (UE) 2018/1725. Il se tient à disposition pour tout conseil complémentaire au cours des négociations

TABLE DES MATIÈRES

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) 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)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[2], et notamment l'article 42, paragraphe 1,

vu la 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[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. Le 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[4] (ci-après le «règlement Europol»), fixe des règles spécifiques concernant les transferts de données effectués par Europol en dehors de l'Union européenne. Son article 25, paragraphe 1, énumère un certain nombre de fondements juridiques sur lesquels Europol pourrait s'appuyer pour transférer en toute légalité des données aux autorités de pays tiers. L'un de ces fondements serait une décision d'adéquation de la Commission adoptée conformément à l'article 36 de la directive (UE) 2016/680, selon laquelle le pays tiers vers lequel Europol transfère des données assure un niveau de protection adéquat. Étant donné qu'il n'existe pas actuellement de telles décisions d'adéquation, un autre fondement sur lequel Europol pourrait s'appuyer pour transférer régulièrement des données vers un pays tiers serait la conclusion d'un accord international contraignant entre l'Union européenne et le pays tiers destinataire offrant des garanties suffisantes au regard de la protection de la vie privée et des autres libertés et des droits fondamentaux des personnes.

2. Aucune base juridique ne permet à l'heure actuelle l'échange régulier et structuré de données à caractère personnel entre les autorités répressives néo-zélandaises et Europol. Europol et la police néo-zélandaise ont signé un arrangement de travail en avril 2019. Celui-ci établit un cadre pour une coopération structurée au niveau stratégique, qui comprend notamment une ligne sécurisée permettant une communication directe sécurisée, et la Nouvelle-Zélande a détaché un officier de liaison auprès d'Europol. Cet arrangement ne constitue toutefois pas une base juridique pour l'échange de données à caractère personnel.

3. La Commission estime que la Nouvelle-Zélande doit être incluse parmi les pays prioritaires avec lesquels entamer des négociations à brève échéance compte tenu de la stratégie politique exposée dans le programme européen en matière de sécurité[5], les conclusions du Conseil sur l'action extérieure de l'UE en matière de lutte contre le terrorisme[6] et la stratégie globale[7] et des besoins opérationnels des autorités répressives dans l'ensemble de l'Union européenne. Elle souligne que les bénéfices potentiels d'une coopération plus étroite ont également été démontrés au travers du suivi de l'attentat de Christchurch de mars 2019. La Nouvelle-Zélande a officiellement demandé, le 23 août 2019, que l'initiative soit prise.

4. Le 30 octobre 2019, la Commission européenne a adopté une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un 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[8] (ci-après la «recommandation»). L'annexe de la recommandation (ci-après l'«annexe») établit les directives de négociation du Conseil à l'intention de la Commission, c'est-à-dire les objectifs que celle-ci devrait s'efforcer d'atteindre au nom de l'Union européenne au cours des négociations.

5. L'accord a pour objectif de constituer la base juridique du transfert de données à caractère personnel entre Europol et les autorités compétentes de la Nouvelle-Zélande respectivement, afin d'appuyer et de renforcer l'action des autorités compétentes de ce pays et des États membres ainsi que leur collaboration mutuelle dans la prévention des formes graves de criminalité transnationale et du terrorisme et dans la lutte contre ceux-ci, tout en offrant des garanties appropriées en ce qui concerne la protection de la vie privée, des données à caractère personnel et des libertés et droits fondamentaux des personnes[9].

6. Conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, la Commission doit consulter le CEPD à la suite de l'adoption de propositions de recommandations au Conseil en vertu de l'article 218 du TFUE en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.

7. Par ailleurs, le considérant 35 du règlement Europol dispose que «[l]e cas échéant et conformément au règlement [(UE) 2018/1725], la Commission devrait pouvoir consulter le Contrôleur européen de la protection des données (CEPD) avant et pendant la négociation d'un accord international» entre l'Union européenne et un pays tiers afin d'autoriser l'échange de données entre Europol et les autorités de ce pays tiers.

8. Le CEPD se réjouit d'avoir été consulté par la Commission européenne sur la recommandation et espère qu'une référence au présent avis sera intégrée dans le préambule de la décision du Conseil. Le présent avis est sans préjudice des observations supplémentaires que le CEPD pourrait formuler ultérieurement sur la base des informations disponibles.

2. OBSERVATIONS GÉNÉRALES

9. Les transferts de données à caractère personnel collectées dans le cadre d'enquêtes pénales et traitées ensuite par Europol pour produire des renseignements en matière pénale envisagés dans l'accord sont susceptibles d'avoir une incidence considérable sur la vie des personnes concernées car ils serviront éventuellement dans le cadre de poursuites engagées dans le pays destinataire en vertu de son droit national.

10. Étant donné que les transferts de données à caractère personnel vers des pays tiers constituent une ingérence dans le droit des personnes à la vie privée et à la protection des données garanti par les articles 7 et 8 de la charte, les exigences en matière de nécessité et de proportionnalité du traitement envisagé doivent être évaluées conformément à l'article 52, paragraphe 1, de la charte[10]. Par conséquent, l'accord international doit garantir que les limitations des droits à la vie privée et à la protection des données dans le cadre de la lutte contre les formes graves de criminalité et le terrorisme s'opèrent dans les limites du strict nécessaire[11].

11. Si le règlement Europol prévoit des règles autonomes en matière de protection des données spécifiques à Europol, son considérant 40 précise qu'elles devraient rester *«cohérentes avec d'autres instruments pertinents en matière de protection des données applicables au domaine de la coopération policière dans l'Union. [...] en particulier, la directive (UE) 2016/680 [...]»*. À cet égard, le considérant 68 de la directive (UE) 2016/680 énonce parmi les différents facteurs qui devraient être pris en considération dans le cadre de l'évaluation des transferts de données à caractère personnel vers des autorités répressives dans des pays tiers, les *«engagements internationaux»* de ces derniers et *toute décision d'adéquation pertinente [que la Commission] aurait adoptée conformément à l'article 45 du règlement (UE) 2016/679»*.

12. À cette fin, le CEPD souligne que la Nouvelle-Zélande dispose depuis 1993 d'une législation nationale en matière de protection des données, le «Privacy Act», et d'une autorité indépendante chargée de la protection des données, le commissaire à la protection de la vie privée, compétente pour superviser les organismes privés et publics, y compris les services répressifs[12]. En outre, la Commission a adopté en décembre 2012 une décision constatant, conformément à la directive 95/46/CE, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande[13]. La Nouvelle-Zélande a un statut d'observateur au sein du comité de la convention 108 du Conseil de l'Europe[14]. En outre, le commissariat néo-zélandais à la protection de la vie privée a fait office, il y a peu encore, de secrétariat de la conférence internationale des Commissaires à la protection des données et à la vie privée (ICDPPC), désormais appelée «Global Privacy Assembly (GPA)».

13. Le CEPD a déjà eu la possibilité de formuler des observations sur l'échange de données à caractère personnel entre Europol et les autorités répressives des huit pays tiers sur la base de l'article 25, paragraphe 1, point b), du règlement Europol[15]. Il se félicite que la Commission ait intégré dans la proposition de mandat de négociation avec la Nouvelle-Zélande un certain nombre de recommandations énoncées dans l'avis de 2018, parmi lesquelles figurent la présentation d'une liste exhaustive des autorités compétentes de la Nouvelle-Zélande auxquelles Europol peut transférer des données à caractère personnel, ainsi qu'une brève description de leurs compétences [directive 3, point c), de l'annexe][16]; l'autorisation de transferts ultérieurs d'informations des autorités compétentes de la Nouvelle-Zélande qu'aux fins initiales du transfert par Europol [directive 3, point i), de l'annexe][17]; l'obligation pour les autorités compétentes de la Nouvelle-Zélande de respecter les limitations fixées par Europol concernant les données à caractère personnel qui ont été transférées et de préciser les modalités pratiques de leur mise en œuvre [directive 3, point c), de l'annexe][18]; ou la précision des possibilités juridiques pour poursuivre le traitement des données déjà transférées en cas de suspension ou de dénonciation de l'accord (directive 6 de l'annexe)[19].

14. Dans ce contexte, les recommandations formulées dans le présent avis visent à préciser et, le cas échéant, à développer davantage les garanties et les contrôles prévus dans le futur accord en ce qui concerne la protection des données à caractère personnel. Elles sont sans préjudice des éventuelles recommandations supplémentaires que le CEPD pourrait formuler sur la base de

nouvelles informations disponibles et des dispositions des projets d'accords au cours des négociations.

15. En outre, le CEPD estime qu'il serait particulièrement utile de renforcer la coopération internationale dans le domaine de la protection des données à caractère personnel entre les autorités de contrôle respectives de l'Union européenne et de la Nouvelle-Zélande, conformément à l'article 51 du règlement (UE) 2018/1725 et à l'article 40 de la directive (UE) 2016/680. Par ailleurs, cette coopération peut contribuer à éviter d'éventuels conflits et interprétations erronées au cours de l'application de l'accord et, si nécessaire, faciliter le fonctionnement du mécanisme de règlement des différends prévu à la directive 4 de l'annexe.

3. RECOMMANDATIONS

3.1. Base juridique matérielle de la décision du Conseil

16. L'exposé des motifs de la recommandation indique que celle-ci est fondée sur l'article 218 du TFUE. Le préambule du projet de décision du Conseil renvoie plus précisément à l'article 218, paragraphes 3 et 4, du TFUE. Toutefois, le préambule ne fait référence à aucune base juridique matérielle pour l'accord envisagé.

17. Conformément à l'article 296, deuxième alinéa, du TFUE et à la jurisprudence constante de la CJUE[20], le CEPD s'interroge sur le fait que les visas cités dans le préambule de la décision du Conseil font certes référence aux bases juridiques procédurales appropriées, mais ne font pas de la même manière référence aux bases juridiques matérielles pertinentes. Le CEPD rappelle que, dans un contexte répressif similaire, la CJUE a conclu que «*la décision du Conseil relative à la conclusion de l'accord envisagé [entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers] doit être fondée conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), TFUE*»[21].

18. Conformément aux directives de négociation, la Commission devrait poursuivre plusieurs objectifs simultanément lors des négociations en vue de l'accord envisagé, parmi lesquels: autoriser le transfert de données à caractère personnel et garantir le respect des droits fondamentaux inscrits dans la charte, notamment les droits au respect de la vie privée et à la protection des données à caractère personnel. De cette manière, l'accord envisagé serait directement en rapport avec les objectifs visés à l'article 16 du TFUE. **Par conséquent, le CEPD recommande d'ajouter, dans le préambule de la décision du Conseil, une référence à la base juridique matérielle appropriée pour le futur accord, qui devrait comprendre l'article 16 du TFUE.**

3.2. Limitation de la finalité

19. La limitation de la finalité est l'un des principes fondamentaux du cadre de l'Union en matière de protection des données. Elle exige, d'une part, que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et, d'autre part, qu'elles ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. À cet égard, le règlement Europol établit qu'«*elle contribue notamment à la transparence, à la sécurité juridique et à la prévisibilité, et revêt une importance particulièrement grande dans le domaine de la coopération entre services répressifs, dans lequel les personnes concernées ignorent habituellement que leurs données à caractère personnel sont collectées et traitées et où l'utilisation de données à caractère personnel peut avoir une incidence considérable sur la vie*

et les libertés des personnes physiques»[22]. Plus précisément, l'article 18 du règlement Europol établit une liste exhaustive de finalités des activités de traitement de données effectuées par Europol, considérées comme légitimes.

20. Le CEPD se félicite que la directive 2 de l'annexe ne limite l'échange de données dans le cadre du futur accord qu'aux formes de criminalité et aux infractions pénales connexes relevant de la compétence d'Europol conformément à l'article 3 du règlement Europol, en particulier la prévention du terrorisme et la lutte contre celui-ci, la désorganisation de la criminalité organisée et la lutte contre la cybercriminalité, et estime également que l'accord devrait préciser son champ d'application et les finalités pour lesquelles Europol peut transférer des données à caractère personnel aux autorités compétentes de la Nouvelle-Zélande. En outre, dans la directive 3, point b), de l'annexe, le principe de spécificité est mis en évidence, principe selon lequel les données ne devraient pas être traitées à des fins autres que celles pour lesquelles elles ont été transférées.

21. Étant donné que le règlement Europol porte principalement sur la limitation de la finalité et sur une plus grande sécurité juridique, **le CEPD recommande que le futur accord établisse explicitement la liste des infractions pénales pour lesquelles des données à caractère personnel pourraient être échangées. En outre, les données à caractère personnel qui sont transférées devraient être liées à des affaires individuelles.**

3.3. Limitation de la conservation

22. La directive 3, point c), de l'annexe dispose que les données à caractère personnel «*ne devraient pas être conservées plus longtemps que ce qui est nécessaire aux finalités pour lesquelles elles auront été transférées*». La directive 3, point f), exige en outre que les accords définissent les règles de conservation, de réexamen, de correction et d'effacement de données à caractère personnel. À cet égard, le CEPD tient à souligner que le règlement Europol prévoit un régime bien établi pour la conservation des données assorti de garanties techniques et procédurales, garantissant que les obligations de conservation et d'effacement sont respectées dans la pratique. L'article 31 impose à Europol de réexaminer la nécessité et la proportionnalité de la conservation des données tous les trois ans. Cette obligation est sans préjudice des différents délais de conservation communiqués par les fournisseurs de données lors de l'envoi des données à Europol, qui sont obligatoires pour cette dernière. Toute décision de conserver les données au-delà des trois premières années doit être dûment justifiée et les raisons doivent être consignées. Europol est également tenue d'effacer les données qui ont été effacées dans les systèmes du fournisseur de données dès qu'elle en est informée.

23. **Le CEPD recommande que le futur accord prévoie un examen périodique de la nécessité de conserver les données à caractère personnel qui ont été transférées et d'autres mesures appropriées qui garantissent que les délais sont respectés, par exemple, l'obligation pour Europol d'informer les autorités néo-zélandaises, à qui les données ont été communiquées ou transférées, du moment où les données seront effacées de ses systèmes.**

3.4. Droit à l'information

24. Le CEPD salue le fait que la directive 3, point e), de l'annexe exige que le futur accord international garantisse «*des droits opposables pour les personnes physiques dont les données à caractère personnel sont traitées, en définissant des règles relatives au droit d'accès, de rectification et d'effacement, y compris les motifs spécifiques pouvant autoriser d'éventuelles*

limitations nécessaires et proportionnées». En outre, la directive 3, point f), prévoit que l'accord fixe des règles, entre autres, «*sur les informations devant être mises à la disposition des personnes physiques*».

25. Le droit à l'information est de la plus haute importance, car il permet l'exercice des autres droits en matière de protection des données, y compris le droit à un recours, et garantit un traitement loyal des données[23]. Les personnes concernées n'ont généralement aucune connaissance du fait que leurs données sont traitées et transférées à des fins répressives. Dans le cas d'Europol, le règlement Europol ne prévoit aucune obligation pour elle d'informer à l'avance les personnes concernées qu'elle traite des informations à caractère personnel les concernant. Les personnes concernées doivent exercer leur droit d'accès pour savoir si Europol traite des données les concernant. Néanmoins, dans son avis 1/15, la CJUE a conclu qu'«*il importe que les passagers aériens soient informés du transfert de leurs données PNR vers le Canada et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques*», considérant qu'«*une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données PNR les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la [c]harte, un recours effectif devant un tribunal*»[24].

26. **Le CEPD recommande que le futur accord international fixe des règles claires et détaillées concernant les informations qui devraient être fournies aux personnes concernées, qui devraient inclure des informations sur le régime applicable aux personnes concernées de l'Union afin d'exercer leurs droits d'accès, de rectification et d'effacement en Nouvelle-Zélande.**

4. CONCLUSIONS

27. Les transferts de données à caractère personnel collectées dans le cadre d'enquêtes pénales et traitées ensuite par Europol pour produire des renseignements en matière pénale sont susceptibles d'avoir une incidence considérable sur la vie des personnes concernées car ils serviront éventuellement dans le cadre de poursuites engagées dans le pays destinataire en vertu de son droit national. Par conséquent, l'accord international doit garantir que les limitations des droits à la vie privée et à la protection des données dans le cadre de la lutte contre les formes graves de criminalité et le terrorisme s'opèrent dans les limites du strict nécessaire.

28. Le CEPD se félicite de l'objectif du mandat de négociation visant à garantir le respect des droits fondamentaux et à observer les principes qui sont reconnus par la charte, en particulier le droit à la vie privée et familiale, prévu à l'article 7 de la charte, le droit à la protection des données à caractère personnel, prévu à l'article 8 de la charte, et le droit à un recours effectif et à accéder à un tribunal impartial, prévu à l'article 47 de la charte. En outre, le CEPD salue le fait que la Commission ait intégré dans la proposition de mandat de négociation avec la Nouvelle-Zélande un certain nombre de recommandations spécifiques déjà indiquées par le CEPD dans son avis 2/2018 sur huit mandats de négociation en vue de la conclusion d'accords internationaux autorisant l'échange de données entre Europol et des pays tiers.

29. Les recommandations du CEPD formulées dans le présent avis visent à préciser et, le cas échéant, à développer davantage les garanties et les contrôles prévus dans le futur accord en ce qui concerne la protection des données à caractère personnel dans le contexte spécifique de la

Nouvelle-Zélande. Elles sont sans préjudice des éventuelles recommandations supplémentaires que le CEPD pourrait formuler sur la base de nouvelles informations disponibles au cours des négociations.

30. À cet effet, le CEPD réaffirme sa position, déjà exprimée dans ses avis précédents[25], selon laquelle la décision du Conseil autorisant l'ouverture de négociations en vertu de l'article 218 du TFUE devrait comporter une référence non seulement à la base juridique procédurale, mais également à la base juridique matérielle pertinente, qui devrait comprendre l'article 16 du TFUE. Par ailleurs, conformément au principe de limitation de la finalité, le futur accord devrait établir explicitement la liste des infractions pénales pour lesquelles des données à caractère personnel pourraient être échangées. En outre, pour assurer la mise en œuvre concrète du principe de limitation de la conservation, le futur accord devrait prévoir expressément un examen périodique de la nécessité de conserver les données à caractère personnel qui ont été transférées. Enfin, étant donné l'importance particulière du droit à l'information pour l'exercice des autres droits en matière de protection des données, le CEPD souligne la nécessité d'établir des règles claires et détaillées concernant les informations qui devraient être fournies aux personnes concernées.

31. Le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus. Les observations présentées dans le présent avis sont sans préjudice des observations supplémentaires que le CEPD pourrait formuler ultérieurement, notamment si de nouveaux problèmes étaient soulevés et abordés à la lumière d'informations complémentaires. À cette fin, le CEPD s'attend à être ultérieurement consulté à propos des dispositions du projet d'accord avant que celui-ci ne soit finalisé.

Bruxelles, le 31 janvier 2020

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3]JO L 119 du 4.5.2016, p. 89.
[4] JO L 135 du 24.5.2016, p. 53.
[5] COM(2015) 185 final.
[6] Document 10384/17 du Conseil du 19 juin 2017.
[7] Vision partagée, action commune: Une Europe plus forte – une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne, http://europa.eu/globalstrategy/fr
[8] COM(2019) 551 final.
[9] Voir la directive 1 de l'annexe.
[10] Pour de plus amples informations, veuillez consulter les lignes directrices du CEPD portant sur l'évaluation du caractère proportionnel des mesures qui limitent les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, disponibles à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf.
[11] Voir les arrêts rendus dans les affaires jointes C-293/12 et C-594/12, DRI, point 52; l'affaire C-73/07, Satakunnan Markkinapörssi/Satamedia, point 56; les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke/Eifert, points 77 et 86.
[12] https://www.privacy.org.nz/
[13] Décision d'exécution de la Commission du 19 décembre 2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande, JO L 28 du 30.1.2013, p. 12.
[14] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE nº 108.
[15] Voir l'avis 2/2018 du CEPD sur huit mandats de négociation en vue de la conclusion d'accords internationaux autorisant l'échange de données entre Europol et des pays tiers, adopté le 14 mars 2018, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_international_agreements_europol_fr.pdf.
[16] Voir le point 4.1. de l'avis 2/2018 du CEPD.
[17] Voir le point 4.2. de l'avis 2/2018 du CEPD.
[18] Voir le point 4.3. de l'avis 2/2018 du CEPD.
[19] Voir le point 4.8. de l'avis 2/2018 du CEPD.
[20] Arrêts de la CJUE rendus dans l'affaire C-43/12, Commission/Parlement et Conseil, point 29, et l'affaire C-263/14, Parlement/Conseil, point 43.
[21] Avis 1/15 de la CJUE, Accord PNR UE-Canada, EU:C:2017:592, point 232.
[22] Considérant 26 du règlement Europol.
[23] Affaire C-201/14, Smaranda Bara e.a./Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală, EU:C:2015:638, en particulier les points 32 et 33, dans lesquels la Cour a conclu que «*cette exigence d'information des personnes concernées par le traitement de leurs données personnelles est d'autant plus importante qu'elle est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées [...] et de leur droit d'opposition au traitement desdites données*» et que «*[c]es informations concernent l'identité du responsable du traitement de ces données, les finalités de ce traitement ainsi que toute information supplémentaire nécessaire pour assurer un traitement loyal des données*».
[24] Avis 1/15 de la CJUE, Accord PNR UE-Canada, EU:C:2017:592, point 220.
[25] Voir l'avis 6/2019 du CEPD sur le mandat de négociation d'un accord entre l'UE et le Japon pour le transfert et l'utilisation de données des dossiers passagers, l'avis 2/2019 du CEPD sur le mandat de négociation d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques et l'avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité, disponibles à l'adresse suivante: https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_fr.