Nº 7151

CHAMBRE DES DEPUTES

Session ordinaire 2016-2017

P R O J E T D E L O I

relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

* * *

(Dépôt: le 19.6.2017)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre de la Sécurité intérieure et après délibération du Gouvernement en Conseil;

Arrêtons:

Article unique.– Notre Ministre de la Sécurité intérieure est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Palais de Luxembourg, le 8 juin 2017

Pour le Ministre de la Sécurité intérieure,
La Secrétaire d'Etat,
Francine CLOSENER

HENRI

*

EXPOSE DES MOTIFS

Le présent projet de loi a pour objet de transposer en droit national la directive 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.

*

1. RETROACTES

Le Luxembourg avait inscrit la lutte contre le terrorisme et la criminalité organisée parmi les priorités de sa présidence du Conseil de l'Union européenne au 2e semestre de l'année 2015 et s'était, entre autres, fixé comme objectif de parvenir à un accord politique sur la création d'un système PNR européen.

L'idée de créer un cadre légal européen pour l'utilisation des données passagers à des fins répressives remonte à une proposition de la Commission européenne du 6 novembre 2007. La proposition de décision-cadre n'ayant toutefois pas été adoptée par le Conseil au moment de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne (TFUE) le 1er décembre 2009, elle a dû être remplacée par un nouveau texte. Le 2 février 2011, la Commission européenne a présenté une proposition de directive sur laquelle le Conseil Justice et Affaires intérieures (JAI) a dégagé une orientation générale le 26 avril 2012. Un vote de rejet de la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen du 24 avril 2013 a toutefois bloqué la proposition de directive.

La montée en puissance du phénomène des combattants étrangers a relancé les discussions autour de la mise en place d'un système PNR européen. Après les attenants qui ont frappé Paris en janvier 2015, les chefs d'Etat et de Gouvernement de l'Union européenne ont appelé à adopter d'urgence une directive robuste et efficace relative à un système PNR européen dotée de garanties en matière de protection des données.

Au mois de février 2015, le Parlement européen s'est engagé à travailler sur la finalisation d'une directive jusqu'à la fin de l'année 2015, tout en encourageant le Conseil à faire des progrès sur le paquet protection des données afin de permettre des trilogues en parallèle sur la proposition de directive PNR et la proposition de directive relative à la protection des données à caractère personnel en matière pénale. Le 15 juillet 2015, le Parlement européen a adopté un rapport révisé sur la proposition de directive PNR et un mandat de négociation avec le Conseil.

La Présidence luxembourgeoise du Conseil a réussi à négocier un texte de compromis qui respecte à la fois les principes fondamentaux en matière de protection des données et réponde aux besoins opérationnels des services compétents. Le texte de compromis a été approuvé par le Conseil JAI le 4 décembre 2015 et par le Parlement européen le 14 avril 2016.

Les principaux éléments de discussion entre le Conseil, la Commission et le Parlement étaient l'inclusion des vols intra-communautaires, l'application de la directive aux opérateurs économiques non transporteurs et la durée de conservation des données sous une forme „active".

Pour trouver un compromis entre les Etats membres qui plaidaient pour l'inclusion obligatoire de tous les vols intra-UE et les Etats membres qui étaient opposés à l'inclusion de ces vols, l'orientation générale adoptée en avril 2012 avait laissé le choix aux Etats membres de collecter ou non les données PNR sur tous ou sur certains vols intra-UE. En raison de la menace sécuritaire constituée par les combattants étrangers et des stratégies de contournement entretemps développées, l'inclusion des vols intra-UE n'a plus été en 2015 un sujet controversé au sein du Conseil. L'expérience acquise par les services répressifs montre en effet que les combattants étrangers empruntent des trajets de plus en plus compliqués à travers l'Union européenne pour dissimuler leur point de départ initial et leur destination finale. Le même phénomène est observé à propos des membres d'organisations criminelles.

Le Parlement européen souhaitait voir limiter l'application de la directive aux vols en provenance ou à destination d'Etats non membres de l'Union européenne.

Le texte de la directive tel qu'adopté le 27 avril 2016 retient que les Etats membres sont libres de collecter les données PNR sur tous ou sur certains vols intra-UE. Dans une déclaration commune du 4 décembre 2015, les ministres JAI se sont engagés à faire pleinement usage de la faculté de recueillir des données PNR pour les vols intra-UE dès la mise en application de la directive.

Un autre sujet de négociation était la collecte obligatoire de données PNR auprès d'opérateurs économiques tels que des agences ou des organisateurs de voyages. Il a été retenu que la Commission procède, au plus tard deux ans après le délai de transposition, à un réexamen de tous les éléments de la directive, et notamment la nécessité d'inclure ces opérateurs économiques. Par ailleurs, un considérant de la directive précise que les Etats membres peuvent prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens. Dans la déclaration commune précitée du 4 décembre 2015, les ministres se sont engagés, dans la mesure du possible, à élargir la collecte des données PNR auprès d'opérateurs économiques autres que les transporteurs. Cette inclusion pose cependant des difficultés pratiques dans la mesure où les opérateurs économiques utilisent des systèmes de réservation différents et qu'il n'existe pas de standards en ce qui concerne leurs systèmes informatiques. Le Luxembourg engagera dès à présent des réflexions sur la mise en pratique de l'inclusion des opérateurs économiques, mais attendra les résultats de l'évaluation au sujet de la nécessité de les inclure dans le champ d'application.

Un troisième élément de discussion était la durée de conservation des données PNR. La proposition de la Commission prévoyait une période initiale de conservation de trente jours, suivie d'une période supplémentaire de cinq ans au cours de laquelle les données seraient masquées. Les négociations entre Etats membres ont toutefois fait apparaître qu'une période initiale de trente jours était trop courte d'un point de vue opérationnel et le Conseil a retenu une période de conservation globale de cinq ans, subdivisée en deux périodes, une première période de deux ans au cours de laquelle les données seraient pleinement accessibles, et une seconde période de trois ans où les données servant à identifier le passager seraient masquées et leur divulgation complète serait subordonnée à des conditions strictes. Selon l'avis et les expériences des services répressifs, le système PNR ne permet en effet de lutter de manière efficace contre le terrorisme et la criminalité organisée que si les données restent „actives" pendant une certaine période. Comme les actes de terrorisme se préparent généralement sur une période plus longue, le système PNR doit être conçu de manière à ce qu'il permette de reconstituer l'activité d'un ou de plusieurs individus en remontant sur une période suffisamment longue. Le suivi des groupes terroristes exige d'établir des „patterns of life", procédure qui s'inscrit dans le long terme. La probabilité qu'une information intéressante se trouve dans les données PNR recueillies depuis moins de 30 jours est quasiment nulle. Par ailleurs, concernant le cas particulier des individus se rendant dans des camps d'entraînement en Syrie ou en Irak, selon les renseignements des services spécialisés, ces séjours dépassent généralement 30 jours. Un délai de 30 jours est également trop court pour lutter contre d'autres formes de criminalité telles que le trafic de drogue. Les critères d'évaluation sont en effet établis sur base de l'analyse répétée des données de voyage d'un individu en particulier ou de personnes qui apparaissent régulièrement dans le même dossier de voyage. Or, les trafiquants de drogues sont déployés tous les 4 à 6 mois. Une période de temps avant le masquage suffisamment longue est nécessaire pour découvrir de telles routes et pour comprendre comment les criminels adaptent leurs habitudes.

Le Parlement européen a soutenu la proposition initiale de la Commission. La Présidence luxembourgeoise a toutefois réussi à démontrer, sur base d'exemples concrets fournis par les services compétents des Etats membres de l'Union européenne, qu'une période „active" de 30 jours n'est pas suffisante.

Le texte de compromis retient que les éléments des données qui peuvent servir à identifier directement le passager auquel se rapportent les données doivent être masqués à l'expiration d'une période de 6 mois à compter de leur transfert par les transporteurs aériens.

*

2. OBJET DU PROJET DE LOI

Le présent projet de loi a pour objet de régler le transfert des données PNR des transporteurs aériens vers une unité centrale nationale ayant pour mission la répression et la prévention des infractions terroristes et d'autres formes graves de criminalité ainsi que le traitement ultérieur de ces données.

Les données PNR (Passenger Name Records) sont des informations non vérifiées, communiquées par les passagers, qui sont recueillies et conservées dans le système de réservation et de contrôle des départs des transporteurs aériens pour leur usage commercial. Elles comprennent des informations telles

que les coordonnées du passager, la date du voyage et d'émission du billet, le mode de paiement utilisé et le poids des bagages.

Outre leur usage commercial, les données PNR présentent un intérêt avéré pour les autorités chargées de la prévention et de la répression de la criminalité et sont utilisées depuis des années par les services policiers et douaniers de certains pays. Les activités liées à la criminalité organisée et au terrorisme impliquent souvent des déplacements internationaux. Ces données permettent de contrer la menace que représentent en particulier le terrorisme et certaines autres formes graves de criminalité sous un angle différent que d'autres catégories de données à caractère personnel traitées par les services répressifs.

Les données PNR peuvent être utilisées de différentes manières et à différentes fins. En temps réel, elles aident à trouver des personnes recherchées par la confrontation à des bases de données nationales et internationales ainsi qu'à identifier des personnes pour lesquelles l'analyse de profil indique qu'elles peuvent être impliquées dans une activité criminelle. Les données peuvent également être utilisées de manière réactive pour rassembler des preuves dans le cadre d'enquêtes et, finalement, de manière proactive pour analyser et définir des critères d'évaluation qui peuvent ensuite être appliqués afin d'évaluer le risque que représentent les passagers avant leur arrivée et avant leur départ.

*

3. LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Le considérant 27 de la directive précise que le traitement des données PNR doit être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale et aux exigences spécifiques de protection des données énoncées dans la directive PNR. Il précise par ailleurs que les références faites dans la directive PNR à la décision-cadre 2008/977/JAI doivent s'entendre comme des références à la législation actuellement en vigueur et à la législation qui la remplacera.

Dans la mesure où la décision-cadre 2008/977 a été abrogée par la directive 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, qui est transposée en droit national parallèlement à la directive PNR, le présent projet de loi fait référence aux dispositions pertinentes du projet de loi de transposition de la directive du 27 avril 2016 aux endroits où la directive PNR fait référence à la décision-cadre 2008/977. Il est renvoyé à cette loi de transposition notamment en ce qui concerne les droits des personnes et l'autorité de contrôle en matière de données PNR. En dehors de ces références à la loi de transposition de la directive du 27 avril 2016, le présent projet de loi comporte toute une série de dispositions spéciales qui sont destinées à garantir la protection des données PNR en particulier.

*

TEXTE DU PROJET DE LOI

Chapitre 1er – *Dispositions générales*

Art. 1er. La présente loi règle le transfert, par les transporteurs aériens, des données des dossiers passagers et le traitement de ces données à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité.

Art. 2. Pour l'application de la présente loi, on entend par:

a) „transporteur aérien“: toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes;

b) „passager“: toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

c) „dossier passager“: le dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs utilisés pour contrôler les passagers lors de l'embarquement ou des systèmes équivalents offrant les mêmes fonctionnalités;

d) „système de réservation“: le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

e) „système de contrôle des départs“: le système utilisé pour contrôler les passagers lors de l'embarquement;

f) „données PNR“: les données contenues dans le dossier passager et énumérées à l'annexe I;

g) „méthode push“: la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'information passagers;

h) „infractions terroristes“: les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal;

i) „formes graves de criminalité“: les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans;

j) „dépersonnaliser par le masquage d'éléments des données“: rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

Chapitre 2 – *Unité d'information passagers*

Art. 3. Il est créé au sein de la Police grand-ducale une Unité d'informations passagers, ci-après désignée „UIP“, qui est chargée:

a) de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données;

b) du transfert de ces données et des résultats de leur traitement aux services compétents;

c) de l'échange de ces données et des résultats de leur traitement avec les unités d'information passagers des autres Etats membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4. Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Art. 5. Sans préjudice des obligations imposées en vertu de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, les transporteurs aériens transfèrent à l'UIP, par la méthode push, les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg dont ils disposent.

Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR incombe au transporteur aérien qui assure le vol.

Art. 6. (1) Les transporteurs aériens transfèrent les données PNR à l'UIP à chacune des échéances suivantes:

a) 48 heures avant l'heure de départ programmée du vol;

b) 24 heures avant l'heure de départ programmée du vol;

c) immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer.

Le transfert visé à l'alinéa 1er, point c), peut se limiter à une mise à jour des transferts visés à l'alinéa 1er, points a) et b).

(2) Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP peut demander, au cas par cas, le transfert de données PNR en dehors des délais prévus au paragraphe 1er.

Art. 7. (1) Les données PNR sont transférées à l'UIP par voie électronique au moyen des protocoles communs et des formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la Directive 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. Les actes d'exécution adoptés par la Commission européenne sont applicables au Luxembourg dès leur publication au Journal officiel de l'Union européenne.

Les transporteurs aériens portent à la connaissance de l'UIP le protocole commun et le format de données utilisés pour leurs transferts.

(2) En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union européenne en matière de protection des données soit pleinement respecté.

Chapitre 4 – *Traitement des données PNR*

Art. 8. Le traitement de données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle est interdit.

Lorsque les données PNR transférées par les transporteurs aériens comportent des informations telles que visées à l'alinéa 1er, l'UIP efface ces informations dès réception et de façon définitive.

Art. 9. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données supplémentaires dès réception et de façon définitive.

Art. 10. (1) L'UIP traite les données PNR en vue de réaliser une évaluation des passagers avant leur arrivée prévue sur le territoire national ou leur départ prévu du territoire national afin d'identifier les personnes pour lesquelles un examen plus approfondi par les services compétents et, le cas échéant, par Europol est requis compte tenu du fait qu'elles peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

(2) Pour réaliser cette évaluation l'UIP peut comparer les données PNR:

a) aux banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions;

b) à des critères préétablis.

L'évaluation des passagers au regard de critères préétablis est réalisée de façon non discriminatoire. Les critères sont fixés et réexaminés à des intervalles réguliers par l'UIP en coopération avec les services compétents. Ils doivent être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

(3) L'UIP réexamine individuellement, par des moyens non automatisés, toute concordance positive obtenue à la suite d'un traitement automatisé des données PNR effectué en vertu du présent article.

(4) L'UIP transmet aux services compétents, au cas par cas, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au présent article ou le résultat du traitement de ces données.

(5) Les conséquences de l'évaluation des passagers ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union européenne à la libre circulation sur le territoire de Luxembourg tel que prévu par la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration.

(6) Lorsque les évaluations sont réalisées pour des vols entre le Luxembourg et un autre Etat membre de l'Union européenne auquel s'applique le règlement No 562/2006 du Parlement européen et du

Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes, les conséquences de ces évaluations doivent respecter ledit règlement.

Art. 11. L'UIP traite les données PNR afin de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations visées à l'article 10.

Art. 12. L'UIP traite les données PNR aux fins de répondre aux demandes des services compétents, dûment motivées et fondées sur des motifs suffisants visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques aux fins visées à l'article 1er, et visant à communiquer aux services compétents ou, le cas échéant, à Europol, le résultat de ce traitement.

Chapitre 5 – *Services compétents*

Art. 13. Sans préjudice des attributions des autorités judiciaires telles que définies par le Code de procédure pénale, sont habilités à demander et à recevoir des données PNR ou le résultat du traitement de ces données, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître:

a) les services de la Police grand-ducale;

b) le Service de Renseignement de l'Etat;

c) les services de l'Administration des Douanes et Accises.

Art. 14. Les services compétents ne peuvent traiter les données PNR et le résultat du traitement de ces données que pour les finalités de la présente loi telles que définies à l'article 1er.

L'alinéa 1er est sans préjudice des compétences de la Police et de l'Administration des Douanes et Accises lorsque d'autres infractions ou indices d'autres infractions sont détectés à la suite de ce traitement.

Art. 15. Les services compétents ne prennent aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Art. 16. Lorsqu'une personne est identifiée conformément à l'article 10, l'UIP communique toutes les données pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP des autres Etats membres de l'Union européenne concernés.

Lorsque l'UIP est destinataire d'informations telles que visées à l'alinéa 1er de la part d'une autre UIP, elle transmet ces informations aux services compétents.

Art. 17. (1) L'UIP transmet, dès que possible, à l'UIP d'un autre Etat membre de l'Union européenne qui en fait la demande, les données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par masquage conformément à l'article 26, et, si nécessaire, le résultat de tout traitement de ces données, s'il a déjà été réalisé conformément à l'article 10.

La demande, dûment motivée, peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière.

Si les données demandées ont été dépersonnalisées par masquage conformément à l'article 26, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que le transfert est nécessaire aux fins visées à l'article 12 et si elle y est autorisée par le procureur d'Etat de Luxembourg ou son délégué.

(2) Dans des cas d'urgence, les autorités compétentes des autres Etats membres, désignées conformément à l'article 7, paragraphe 1er, de la Directive (UE) 2016/661 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 et figurant comme telles au Journal officiel de l'Union européenne, peuvent directement s'adresser à l'UIP pour obtenir communication de données PNR. Les dispositions du paragraphe (1) sont applicables.

(3) A titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un Etat membre a le droit de demander à ce que l'UIP obtienne des données PNR conformément à l'article 6, paragraphe (2), et les communique à l'UIP requérante.

Art. 18. L'UIP et les services compétents visés à l'article 13 peuvent demander aux UIP des autres Etats membres de l'Union européenne des données PNR ou les résultats du traitement de ces données. Les demandes sont introduites et traitées conformément au droit national de l'Etat membre requis.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre Etat membre de l'Union européenne, il transmet copie de sa demande à l'UIP.

Art. 19. L'échange de données effectué en application du présent chapitre peut avoir lieu par l'intermédiaire de tous les canaux de coopération policière existant entre les autorités compétentes des Etats membres de l'Union européenne.

La langue utilisée pour la demande et l'échange des données est celle applicable au canal utilisé.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Art. 20. (1) Dans les limites de ses compétences et pour l'accomplissement de ses missions, Europol peut présenter à l'UIP, au cas par cas, par l'intermédiaire de son unité nationale, une demande électronique dûment motivée visant à obtenir des données PNR spécifiques ou le résultat du traitement de ces données:

a) lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des Etats membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes dans la matière et;

b) dans la mesure où ladite infraction relève de la compétence d'Europol.

(2) La demande énonce les motifs sur lesquels s'appuie Europol pour estimer que la transmission de données PNR ou du résultat de traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée ou à des enquêtes en la matière.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Art. 21. Sans préjudice des dispositions de l'article 35, paragraphe (1), point (d), et des articles 36 à 38 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'UIP peut transférer des données PNR et le résultat de traitement de ces données à un pays non membre de l'Union européenne au cas par cas, et si:

a) l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité;

b) le transfert est nécessaire aux fins telles que définies à l'article 1er;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins telles que définies à l'article 1er;

d) les conditions prévues à l'article 17, paragraphe (1) sont remplies.

Art. 22. (1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre Etat membre de l'Union européenne à un pays non membre de l'Union européenne que si l'Etat membre auprès duquel les données ont été collectées a donné son accord au transfert.

(2) Dans des circonstances exceptionnelles, les données PNR peuvent être transférées à un pays non membre de l'Union européenne sans l'accord du pays membre de l'Union européenne auprès duquel les données ont été collectées si les conditions suivantes sont remplies:

a) ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un Etat membre de l'Union européenne ou un pays tiers;

b) l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'Etat membre de l'Union européenne, qui n'a pas pu donner son accord en temps utile, est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

Art. 23. L'UIP ne peut transférer des données PNR et les résultats du traitement de ces données aux autorités compétentes de pays non membres de l'Union européenne que dans les conditions compatibles avec la présente loi et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

Art. 24. Le délégué à la protection des données est informé de tout transfert de données PNR à un pays non membre de l'Union européenne.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Art. 25. L'UIP conserve les données PNR pendant une durée maximale de cinq ans à compter du transfert par le transporteur aérien.

A l'issue de cette période de cinq ans, elle efface les données PNR de manière définitive. Cette disposition ne s'applique pas si les données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière.

Art. 26. (1) A l'expiration d'une période de six mois à compter du transfert par le transporteur aérien, l'UIP dépersonnalise les données PNR par le masquage des éléments suivants:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations „grands voyageurs“;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte;

f) toute donnée API qui a été recueillie.

(2) A l'expiration de la période de six mois visée au paragraphe (1), la communication de l'intégralité des données PNR n'est autorisée que sous les conditions suivantes:

a) elle est nécessaire aux fins visées à l'article 12;

b) elle a été approuvée par le procureur d'Etat de Luxembourg ou son délégué ou, si les données sont destinées à être communiquées au Service de Renseignement de l'Etat, par la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Art. 27. L'UIP ne conserve le résultat de l'évaluation réalisée en vertu de l'article 10 que le temps nécessaire pour informer les services compétents et, s'il y a lieu, les UIP des autres Etats membres de l'Union européenne de l'existence d'une concordance positive.

Lorsque, à la suite du réexamen individuel par des moyens non automatisés conformément à l'article 10, paragraphe (3), le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées en vertu de l'article 25, de manière à éviter de futures „fausses“ concordances positives.

Chapitre 10 – *Protection des données à caractère personnel*

Art. 28. Sans préjudice de l'article 41 de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, l'autorité de contrôle instituée par l'article 1er de la loi du *jj/mm/aaaa* relative à la création de la Commission nationale pour la protection des données et au régime général sur la protection des données est compétente pour contrôler et vérifier le respect des dispositions de la présente loi en ce qui concerne le traitement des données à caractère personnel. Elle exerce ses missions conformément à l'article 10 de la même loi et elle dispose, à cette fin, des pouvoirs prévus à l'article 16 de la même loi.

Art. 29. (1) Le responsable de l'UIP désigne un délégué à la protection des données.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

(2) Le délégué à la protection des données contrôle le traitement des données PNR et met en œuvre les garanties pertinentes au sein de l'UIP.

Il informe et conseille le responsable et le personnel de l'UIP sur les obligations qui leur incombent en matière de protection des données.

Il fait office de point de contact pour les personnes concernées pour toutes les questions relatives au traitement de leurs données PNR et pour la Commission nationale pour la protection des données.

(3) Le délégué à la protection des données effectue ses missions en toute indépendance.

Il fait directement rapport au responsable de l'UIP.

Par dérogation à l'alinéa 2, et sans préjudice du paragraphe (4), alinéa 2, en cas de problèmes relevant de la protection des données, le délégué à la protection des données rapporte directement au Directeur général de la Police ou, s'il juge nécessaire, au Ministre ayant la Police dans ses attributions.

(4) Le délégué à la protection des données a accès à toutes les données traitées par l'UIP.

Sans préjudice de l'article 23 du Code de procédure pénale, si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, il peut renvoyer l'affaire à la Commission nationale pour la protection des données.

Art. 30. L'UIP met à la disposition du public, par les moyens de communication appropriés, les informations suivantes:

a) ses coordonnées;

b) les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données PNR;

d) le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité;

e) l'existence du droit de demander au responsable de l'UIP l'accès aux données PNR, leur rectification ou leur effacement, et la limitation du traitement des données PNR relatives à une personne concernée.

Art. 31. (1) Les personnes dont les données sont traitées en vertu de la présente loi disposent des mêmes droits d'accès, de rectification ou d'effacement et de limitation du traitement que ceux prévus aux articles 14 à 18 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et peuvent exercer ces droits dans les mêmes conditions et limites.

(2) Elles disposent des mêmes droits de réclamation et de recours juridictionnel que ceux prévus aux articles 45 à 48 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 32. L'UIP conserve, traite et analyse les données PNR en un ou des endroits sécurisés situés sur le territoire du Luxembourg.

Art. 33. Le responsable de l'UIP met en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et la nature des données PNR.

En ce qui concerne le traitement automatisé, le responsable de l'UIP met en œuvre, à la suite d'une évaluation des risques, des mesures telles que prévues à l'article 29, paragraphe (2) de la loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Art. 34. L'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous sa responsabilité.

Cette documentation comprend:

a) Le nom et les coordonnées du service et du personnel chargés du traitement des données PNR au sein de l'UIP et les différentes autorisations d'accès;

b) Les demandes formulées par les services compétents et les UIP des autres Etats membres de l'Union européenne;

c) Toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle, à la demande de celle-ci.

Art. 35. L'UIP tient des registres pour la collecte, la consultation, la communication et l'effacement des données PNR.

Les registres des opérations de consultation et de communication indiquent la finalité, la date et l'heure de l'opération et l'identité de la personne qui a consulté ou communiqué les données PNR ainsi que l'identité des destinataires de ces données.

Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit.

L'UIP met les registres à la disposition de l'autorité de contrôle, à la demande de celle-ci. Les registres sont conservés pendant cinq ans.

Art. 36. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'UIP informe sans retard injustifié la personne concernée et l'autorité de contrôle de cette atteinte.

Chapitre 11 – *Sanctions*

Art. 37. La violation des articles 8, 15 et 36 est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent alinéa sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 49, paragraphe 1er et paragraphes 3 à 5 du projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont applicables en ce qui concerne les violations des règles relatives à la protection des données établies par la présente loi et par les lois auxquelles elle se réfère.

Art. 38. (1) Est puni d'une amende d'un montant maximum de 50.000 euros le transporteur aérien, à raison de chaque vol pour lequel il n'a pas transmis les renseignements y visés, ou ne les a pas transmis dans le délai prévu ou selon les modalités et dans les formats tels que fixés en vertu de l'article 7.

(2) Le manquement est constaté par un procès-verbal établi par la Police grand-ducale. Copie en est transmise au transporteur aérien.

Le transporteur aérien a accès au dossier et est mis à même de présenter ses observations écrites dans un délai d'un mois sur le projet de sanction.

L'amende est prononcée par le Ministre ayant la Police dans ses attributions.

(3) La décision du ministre qui est motivée est susceptible d'un recours en réformation à introduire devant le Tribunal administratif dans un délai d'un mois à compter de la notification.

*

ANNEXE I

Liste des données PNR

a) Code repère du dossier passager;

b) Date de réservation/d'émission du billet;

c) Date(s) prévue(s) du voyage;

d) Nom(s);

e) Adresse et coordonnées (numéro de téléphone, adresse électronique);

f) Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation;

g) Itinéraire complet pour le PNR concerné;

h) Informations „grands voyageurs";

i) Agence de voyages/agent de voyages;

j) Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation;

k) Indications concernant la scission/division du PNR;

l) Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée);

m) Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix;

n) Numéro du siège et autres informations concernant le siège;

o) Informations sur le partage de code;

p) Toutes les informations relatives aux bagages;

q) Nombre et autres noms de voyageurs figurant dans le PNR;

r) Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée);

s) Historique complet des modifications des données PNR énumérées aux points 1 à 18.

*

ANNEXE II

Liste des infractions visées à l'article 2, point (i)

a) Participation à une organisation criminelle;

b) Traite des êtres humains;

c) Exploitation sexuelle des enfants et pédopornographie;

d) Trafic de stupéfiants et de substances psychotropes;

e) Trafic d'armes, de munitions et d'explosifs;

f) Corruption;

g) Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union;

h) Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro;

i) Cybercriminalité;

j) Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;

k) Aide à l'entrée et au séjour irréguliers;

l) Meurtre, coups et blessures graves;

m) Trafic d'organes et de tissus humains;

n) Enlèvement, séquestration et prise d'otage;

o) Vol organisé ou vol à main armée;

p) Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;

q) Contrefaçon et piratage de produits;

r) Falsification de documents administratifs et trafic de faux;

s) Trafic de substances hormonales et d'autres facteurs de croissance;

t) Trafic de matières nucléaires et radioactives;

u) Viol;

v) Infractions graves relevant de la Cour pénale internationale;

w) Détournement d'avion/de navire;

x) Sabotage;

y) Trafic de véhicules volés;

z) Espionnage industriel.

*

COMMENTAIRE DES ARTICLES

Chapitre 1er – *Dispositions générales*

Ad article 1er

La présente loi a pour objet d'obliger les transporteurs aériens à transférer les données des dossiers passagers (données PNR) qu'ils recueillent à des fins commerciales, à une unité centrale nationale compétente en matière de prévention et de répression du terrorisme et de la criminalité grave et de fixer les conditions selon lesquelles ces données peuvent être traitées.

L'article 1er, outre de définir l'objet de la loi, précise et limite les finalités pour lesquelles les données PNR peuvent être traitées. Ces finalités sont la prévention et la répression des infractions terroristes et des formes graves de criminalité qui sont énumérées à l'annexe II.

Ad article 2

L'article 2, qui transpose l'article 3 de la directive, définit les notions qui sont essentielles pour la compréhension et l'application de la présente loi.

Le point a) précise ce qu'il y a lieu d'entendre par „transporteur aérien". Il s'agit de toute entreprise de transport aérien qui possède une licence d'exploitation lui permettant d'assurer le transport aérien de personnes. Pour la définition des notions „entreprise de transport" et „licence d'exploitation" il y a lieu de se référer aux définitions figurant dans les textes communautaires relatifs à la navigation aérienne, et en particulier le règlement 1008/2008 du Parlement européen et du Conseil du 24 septembre 2008 qui établit des règles communes pour l'exploitation de services aériens dans la Communauté. L'entreprise y est définie comme une personne physique ou morale, poursuivant ou non un but lucratif, ou tout organisme officiel doté ou non de la personnalité juridique. La licence d'exploitation est une

autorisation délivrée par l'autorité compétente pour l'octroi des licences à une entreprise l'autorisant à fournir des services aériens selon les mentions figurant dans la licence. Le service aérien est défini comme un vol ou une série de vols transportant, à titre onéreux et/ou en vertu d'une location des passagers, du fret et/ou du courrier.

Relèvent du champ d'application de la présente loi toutes les entreprises de transport aérien qui possèdent une licence d'exploitation respectivement, pour les entreprises établies dans des Etats non membres de l'Union européenne, une habilitation équivalente les autorisant à transporter des personnes à titre onéreux ou en vertu d'un contrat de location.

Est ensuite défini, au point b), le terme de „passager". Cette notion est très importante dans la mesure où elle délimite le cercle de personnes dont les données doivent être transmises.

Le point c) précise ce qu'il y a lieu d'entendre par „dossier passager". Cette définition est à voir ensemble avec la définition figurant au point f). Les informations visées dans la définition du dossier passager sont les données PNR. Il s'agit d'informations non vérifiées fournies par les passagers et recueillies par les transporteurs aux fins de la réservation et de la procédure d'enregistrement.

Les points d) et e) n'appellent pas de commentaire particulier.

Le point g) est relatif au mode de transfert des données PNR des transporteurs aériens vers l'autorité publique. Il importe de noter dans ce contexte qu'il existe deux méthodes possibles de transfert, la méthode dite „pull", par laquelle les autorités compétentes peuvent accéder au système de réservation du transporteur aérien et en extraire copie des données PNR requises, et la méthode dite „push", par laquelle les transporteurs aériens transmettent les données PNR à l'autorité requérante, ce qui leur permet de garder le contrôle sur les données. La directive impose aux Etats membres d'adopter la méthode „push" qui est réputée offrir un niveau plus élevé de protection des données.

Les points h) et i) définissent ce qu'il y a lieu d'entendre par „infractions terroristes" et „formes graves de criminalité" au sens de la présente loi. La liste des infractions énumérées à l'annexe II de la directive est reprise telle quelle dans le présent projet de loi. La directive a retenu les seules infractions pour la prévention et l'élucidation desquelles l'exploitation de données PNR a été jugée pertinente. C'est pour cette raison que la liste figurant à l'annexe II du projet de loi, bien que se couvrant largement avec la liste des infractions pour lesquelles un mandat d'arrêt européen est exécuté sans contrôle de la double incrimination, n'est pas identique à la liste du mandat d'arrêt européen qui comprend par ailleurs le racisme et la xénophobie, l'escroquerie, le racket et l'extorsion de fonds et l'incendie volontaire.

Chapitre 2 – *Unité d'information passagers*

Ad article 3

Les Etats membres sont tenus, en vertu de l'article 4 de la directive, d'instituer une „unité d'information passagers", en abrégé „UIP", qui se charge de recueillir les données transférées par les transporteurs aériens, de les traiter, les conserver, les transmettre aux services nationaux compétents et les échanger avec les unités correspondantes des autres Etats membres, avec Europol et avec les pays tiers.

La directive laisse le choix aux Etats membres de mettre en place une autorité compétente en matière de prévention et de répression d'infractions terroristes et de formes graves de criminalité ou de désigner une autorité existante ou une antenne d'une autorité existante, compétente en cette matière, pour assurer le rôle d'unité d'information passagers.

Le Gouvernement a décidé d'intégrer cette unité à la Police grand-ducale, et plus précisément, au Service des Relations internationales. Compte tenu du fait que les détails de l'organisation future de la Police grand-ducale seront, en principe, à l'avenir arrêtés par le Directeur général de la Police, la présente loi se limite à indiquer que l'UIP est mise en place au sein de la Police.

Ad article 4

L'alinéa 1er désigne le responsable de l'UIP comme responsable du traitement des données PNR.

L'alinéa 2 fixe la composition de l'UIP. L'article 4, paragraphe 3, de la directive prévoit la possibilité pour les autorités qui sont habilitées à demander et à recevoir des données PNR, à détacher du personnel à l'UIP. Le Gouvernement a décidé de faire usage de cette faculté en prévoyant le détachement de personnel de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat à l'UIP. Le présent article est ainsi à mettre en relation avec l'article 13 qui énumère les services nationaux compétents pour recevoir et demander des données PNR.

Il importe de préciser que le personnel de l'UIP, qu'il y soit affecté ou détaché, ne traite les données PNR que dans les limites des missions légales de l'Administration pour le compte de laquelle il agit au sein de l'UIP.

A défaut de dispositions particulières dans la présente loi, les détachements à l'UIP sont effectués d'après les règles prévues par la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat en matière de détachements.

Chapitre 3 – *Transfert des données par les transporteurs aériens*

Ad article 5

Le présent article, qui transpose l'article 8, paragraphe 1er de la directive, oblige les transporteurs aériens à transférer leurs données PNR à l'UIP. Le considérant 8 de la directive explique que la directive ne doit pas imposer aux transporteurs de recueillir ou de conserver des données supplémentaires à celles qu'ils recueillent et traitent déjà pour leur propre usage commercial. Il a pour cette raison été précisé que les transporteurs aériens ne sont obligés de transférer que les données *„dont ils disposent"*.

Les transporteurs aériens sont tenus, en vertu de l'article 106 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration et du règlement grand-ducal pris en son exécution, de transmettre au Service de contrôle à l'aéroport de la Police grand-ducale, à des fins de contrôle d'immigration, les données API *(Advanced Passenger Information)* des passagers en provenance d'un pays non membre de l'Union européenne qu'ils débarquent au Luxembourg. Les données API sont les informations biographiques extraites de la partie d'un passeport lisible par machine et contiennent le nom, le lieu de naissance et la nationalité du titulaire, le numéro du passeport et sa date d'expiration. Etant donné que les données API sont énumérées dans la directive et dans le projet de loi parmi les données PNR que les transporteurs aériens sont tenus de transmettre à l'UIP, il a été jugé nécessaire de faire référence à la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration afin de préciser que l'obligation imposée aux transporteurs aériens en vertu de la présente loi ne les dispense pas de transmettre, à des fins de contrôle d'immigration, les données API au service de Contrôle à l'Aéroport de la Police grand-ducale.

L'article 5 précise par ailleurs que les données sont transférées à l'UIP par la méthode „push". Il est renvoyé à ce propos au commentaire de l'article 2, point g.

L'article 5 détermine ensuite les vols pour lesquels les données doivent être transférées à l'UIP. Il s'agit de tous les vols en provenance et à destination de l'aéroport de Luxembourg, que leur origine ou leur destination se situent ou non sur le territoire de l'Union européenne. Cette disposition est à voir ensemble avec l'article 2, point b) qui définit comme passager non seulement les personnes pour lesquelles le Luxembourg est la destination finale, mais également celles qui sont en correspondance ou en transit au Luxembourg.

L'alinéa 2 vient préciser que pour les vols en partage de code, pratique commerciale qui consiste à ce que deux ou plusieurs compagnies aériennes partagent un vol, l'obligation de transfert repose sur le transporteur aérien qui effectue le vol.

Ad article 6

Le paragraphe 1er transpose l'article 8, paragraphe 3 de la directive, et précise à quels moments les données doivent en principe être transférées à l'UIP. En principe, car il peut arriver, pour des achats de billets à la dernière minute, que le transporteur aérien ne dispose pas encore des données PNR d'un passager à l'échéance H-48. Il est évident que le transporteur aérien ne peut transférer que les données dont il dispose et à partir du moment où il en dispose. L'obligation fixée par le présent article est dès lors à mettre en relation avec l'article 5, paragraphe 1er, qui oblige le transporteur aérien à transférer les données „dont il dispose".

L'alinéa 2 précise que, si les données ont déjà été transférées une première fois 48 heures et une seconde fois 24 heures avant le départ d'un vol, le transporteur peut limiter le troisième transfert à une mise à jour des données transmises auparavant. Il ne s'agit toutefois pas d'une obligation, le transporteur étant libre de transférer une nouvelle fois l'ensemble des données.

Si le paragraphe 1er concerne le transfert de données PNR d'office aux échéances y définies, le paragraphe 2 prévoit la possibilité pour l'UIP de solliciter des données PNR en dehors de ces échéances, au cas par cas, lorsqu'il existe une menace précise et réelle d'infraction.

Ad article 7

L'article 7 est relatif au procédé technique par lequel les données doivent être transférées à l'UIP. Ce transfert a lieu de manière électronique au moyen des protocoles communs et des formats de données qui auront été arrêtés par la Commission européenne et publiés au Journal officiel de l'Union européenne.

A titre exceptionnel, en cas de défaillances techniques, les transporteurs peuvent recourir à d'autres moyens techniques qui doivent toutefois assurer la sécurité des données transférées.

Chapitre 4 – *Traitement des données PNR*

Ad article 8

Conformément à l'article 13, paragraphe 4 de la directive, cet article interdit le traitement de données sensibles et oblige l'UIP, pour le cas où de telles données venaient à être transférées par un transporteur aérien, à les effacer dès réception et de manière définitive.

Ad article 9

L'UIP ne peut traiter que les données énumérées à l'annexe I du présent projet de loi et doit effacer, dès réception et de manière définitive, toute donnée supplémentaire qu'elle se verrait transférer.

Ad article 10

Les articles 10, 11 et 12 définissent les différentes manières dont les données PNR peuvent être utilisées dans le cadre de la prévention et la lutte contre le terrorisme et les formes graves de criminalité. Ils portent transposition de l'article 6, paragraphes 1 à 6 et paragraphe 9 de la directive.

Les données PNR peuvent ainsi être utilisées (art. 10) pour réaliser des évaluations de risques des passagers avant leur départ ou leur arrivée sur le territoire luxembourgeois afin de prévenir une infraction, de surveiller ou d'arrêter des personnes avant qu'une infraction ne soit commise ou parce qu'une infraction a été commise ou est en train de l'être.

Cette évaluation des risques est réalisée, d'une part, par la mise en corrélation des données PNR avec les données figurant dans les banques de données pertinentes nationales et internationales, qui sont exploitées par les services compétents ou qui leurs sont accessibles dans le cadre de leurs attributions respectives telles que par exemple le Schengen Information System ou Interpol. Cette mise en corrélation permettra notamment de déceler des personnes à propos desquelles les services compétents disposent d'indices qu'elles se préparent à commettre des actes terroristes ou des infractions graves telles que celles-ci sont définies à l'annexe II du présent projet de loi ou qui sont recherchées dans le cadre d'une procédure judiciaire.

L'évaluation prévue à l'article 10 consiste d'autre part à comparer les données PNR par rapport à des critères préétablis, afin d'identifier des personnes auparavant „inconnues", c'est-à-dire qui jusque-là n'étaient pas soupçonnées de participation à une infraction grave ou à un acte de terrorisme, mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient être soumises à un examen approfondi par les autorités compétentes. La confrontation en temps réel des données PNR à ces critères permet de prévenir ou de détecter des infractions. Ces critères peuvent concerner par exemple le pays de destination ou de départ, combiné à certaines autres informations telles que le mode de paiement, le poids du bagage, ou l'itinéraire choisi.

La comparaison des données par rapport à des critères préétablis est subordonnée à des règles très strictes, qui sont énoncées au paragraphe 2, alinéa 2, à savoir:

1. L'évaluation ne doit pas être réalisée de manière discriminatoire;
2. Les critères doivent être établis en coopération avec les services compétents;
3. Les critères doivent être réexaminés à des intervalles réguliers;
4. Les critères doivent être ciblés, proportionnés et spécifiques par rapport au type d'infraction qu'ils sont supposés révéler;
5. Les critères ne doivent pas être fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

Lorsque l'UIP obtient une correspondance positive, soit après comparaison avec les banques de données ou par rapport à des critères préétablis, elle en informe le ou les services compétents afin qu'ils

prennent les mesures qu'ils jugent appropriées. Si l'UIP estime qu'un autre Etat membre a besoin d'être informé, elle transmet toutes les données qu'elle juge nécessaires et pertinentes à l'unité d'information passagers de cet Etat membre, conformément à ce qui est prévu à l'article 16 du présent projet de loi et exigé par l'article 9, paragraphe 1er de la directive.

Le paragraphe 3 oblige l'UIP à faire réexaminer individuellement, par une personne physique, toute concordance positive obtenue par des moyens automatisés. L'UIP ne peut transmettre des données PNR ou des résultats de traitements de données PNR à des services nationaux compétents et à une UIP étrangère qu'après avoir effectué cette vérification.

Le paragraphe 4 prévoit la transmission spontanée des correspondances positives par l'UIP aux services nationaux compétents. Cette transmission sera en relation avec une personne pour laquelle il existe une raison de croire qu'elle est liée à une activité criminelle rentrant dans le champ d'application de la présente loi, ou parce que son nom apparaît dans une base de données, ou parce que son *„travel pattern"* ou son comportement correspond à un des critères prédéterminés. Il en est de même pour la transmission spontanée de correspondances positives aux UIP des autres Etat membres.

Les paragraphes 5 et 6 visent à préciser que le présent projet de loi ne modifie pas, ni n'affecte les règles de l'UE actuelles définissant les modalités des contrôles aux frontières, pas plus que les règles de l'UE applicables aux entrées sur le territoire de l'Union et aux sorties de celui-ci.

Ad article 11

Outre la réalisation d'évaluations telles que décrites à l'article 10, les données PNR peuvent être traitées pour établir et pour mettre à jour, si nécessaire, les critères utilisés pour l'évaluation des risques. Ainsi par exemple, une analyse de données PNR peut donner des indications sur les itinéraires les plus empruntés, ou de nouveaux itinéraires empruntés pour la traite des êtres humains ou le trafic de drogues, autant d'éléments qui peuvent être intégrés dans les critères d'évaluation.

Ad article 12

Les données PNR peuvent par ailleurs servir comme éléments de preuve dans le cadre d'enquêtes judiciaires. A titre d'exemple, les données PNR peuvent aider à orienter les enquêteurs sur le lieu de séjour d'une personne suspecte au moment où les faits ont été commis.

Chapitre 5 – *Services compétents*

Ad article 13

Cet article dresse la liste des services nationaux qui peuvent solliciter des données PNR auprès de l'UIP et qui sont destinataires, selon leurs compétences respectives, des concordances positives trouvées lors des évaluations des risques. Il ne porte pas préjudice aux compétences des autorités judiciaires telles que celles-ci sont définies par le Code de procédure pénale.

Il échet de préciser que tous les policiers n'ont pas besoin de recourir à des données PNR dans l'exécution de leurs missions, ces informations n'étant destinées qu'à être utilisées dans le cadre de la recherche d'infractions terroristes et d'infractions graves dont la liste figure en annexe de la présente loi. Il en est de même pour les agents du Service de Renseignement de l'Etat et de l'Administration des Douanes et Accises, qui ne peuvent obtenir ou demander des données PNR ou des résultats de traitements de ces données que pour autant qu'ils agissent dans le cadre respectivement de la prévention ou de la recherche des infractions rentrant dans le champ d'application de la présente loi. Il a pour cette raison été précisé que les services compétents énumérés à l'article 13 ne peuvent demander et obtenir des données PNR que dans les limites de leurs attributions légales et du besoin d'en connaître.

Ad article 14

L'article 14 transpose l'article 7, paragraphes 4 et 5 de la directive. Il interdit aux services compétents d'utiliser les données PNR et les résultats de traitements de telles données à des fins autres que la prévention ou la répression des infractions terroristes et des infractions énumérées à l'annexe II du présent projet de loi.

L'alinéa 2 vient toutefois préciser que l'interdiction visée à l'alinéa 1er n'empêche pas la Police ou l'Administration des Douanes d'enquêter sur d'autres infractions qui seraient détectées à la suite d'un traitement de données PNR et qui ne rentreraient pas dans le champ d'application de la présente loi.

Ad article 15

Cet article, qui porte transposition de l'article 7, paragraphe 6, de la directive précise que les autorités compétentes ne peuvent prendre aucune décision ayant des conséquences juridiques pour une personne ou l'affectant gravement sur base du traitement automatisé des données PNR.

Chapitre 6 – *Echange d'informations entre les Etats membres de l'Union européenne*

Ad article 16

Les articles 16 et 17 transposent l'article 9, paragraphes 1 à 4, de la directive.

Lors des négociations en trilogues, une très grande importance avait été accordée à l'échange d'informations entre Etats membres. Les articles 16 et 17 sont ainsi parmi les éléments-clés du système PNR européen.

L'article 16 règle la transmission d'office d'informations aux UIP d'autres Etats membres, tandis que l'article 17 règle la transmission d'informations sur demande.

L'article 16, alinéa 1er prévoit que, lorsque l'UIP luxembourgeoise a identifié une personne susceptible d'être impliquée dans une infraction terroriste ou une forme grave de criminalité, et qu'il existe un lien avec un ou plusieurs autres Etats membres, elle transmet les données qu'elle juge nécessaires et pertinentes à l'unité ou aux unités correspondantes.

Le 2e alinéa envisage le cas de figure où une UIP étrangère transmet à l'UIP luxembourgeoise des informations relatives à des personnes qu'elle a identifiées sur base de l'évaluation des risques comme pouvant être impliquées dans une infraction tombant dans le champ d'application de la directive. Les conditions de transmission de ces données ne relèvent pas de la législation luxembourgeoise, mais des législations respectives des Etats membres qui ont réalisé l'évaluation. La présente disposition vise à préciser que, lorsque l'UIP luxembourgeoise reçoit de telles informations, elle les continue aux services nationaux compétents, conformément à ce qui est prévu à l'article 9, paragraphe 1er, 2e phrase de la directive.

Ad article 17

L'article 17 définit les conditions selon lesquelles les autorités des autres Etats membres peuvent solliciter des données PNR ou des résultats du traitement de ces données auprès de l'UIP luxembourgeoise.

Excepté les circonstances exceptionnelles prévues au paragraphe 2, les demandes et les échanges de données ont toujours lieu par l'intermédiaire des UIP. Autrement dit, un service compétent d'un autre Etat membre ne peut pas, en principe, solliciter directement des données auprès de l'UIP luxembourgeoise, mais doit s'adresser à sa propre UIP.

L'UIP d'un autre Etat membre de l'Union européenne peut demander à l'UIP luxembourgeoise de recevoir des données PNR ou des résultats de traitements de données PNR que cette dernière est tenue de transmettre dès que possible. La dernière partie du paragraphe 1er, alinéa 1er vise à préciser que, dans l'hypothèse où l'évaluation des risques n'aurait pas encore été réalisée par notre UIP, l'UIP étrangère ne peut pas exiger qu'elle le soit.

Le paragraphe 1er distingue entre deux cas de figure envisagés respectivement à l'alinéa 1er (les données demandées n'ont pas encore été masquées) et à l'alinéa 2 (la demande intervient après écoulement des 6 mois au terme desquels certaines données doivent être masquées). L'UIP requérante doit en tout état de cause motiver les raisons de sa demande. Si la demande porte sur des données qui ont déjà été masquées, les données ne seront communiquées que si l'UIP luxembourgeoise estime qu'il existe des motifs raisonnables de croire que le transfert est nécessaire et obtient l'autorisation afférente du procureur d'Etat ou de son délégué.

Le paragraphe 2 prévoit que dans des cas d'urgence, et par exception au principe que les demandes et échanges de données PNR ont lieu par l'intermédiaire de l'UIP, les autorités compétentes des autres Etats membres peuvent directement demander des données PNR à l'UIP luxembourgeoise. La directive oblige les Etats membres à notifier leurs autorités compétentes à la Commission européenne, qui se charge d'en faire la publication au Journal officiel de l'Union européenne. L'UIP luxembourgeoise ne transmettra des données qu'aux autorités compétentes qui figurent sur la liste publiée au Journal officiel de l'Union européenne. A l'instar des demandes introduites par les UIP, les demandes des autorités

compétentes doivent être motivées d'après les circonstances particulières de l'espèce. Par ailleurs, les conditions spéciales prévues pour la communication des données déjà masquées aux UIP s'appliquent également aux demandes formulées directement par les services compétents.

Le paragraphe 3 prévoit la possibilité pour une UIP étrangère de demander à l'UIP luxembourgeoise de solliciter des données auprès d'un transporteur aérien en dehors des délais auxquels les transporteurs sont tenus de transférer les données. Cette faculté est toutefois limitée aux cas où il existe une menace précise et réelle qu'un acte terroriste ou une infraction grave sera commis.

Ad article 18

L'article 18 vise le cas où les autorités luxembourgeoises souhaitent obtenir des données recueillies ou traitées par l'UIP d'un autre Etat membre. Elles doivent dans ce cas s'adresser à l'UIP de l'Etat membre concerné en respectant les conditions fixées par la législation nationale de cet Etat membre.

L'alinéa 2 envisage le cas de figure où un service compétent national s'adresse directement à une UIP étrangère. En effet, si les conditions d'obtention des données sont régies par la législation de l'Etat requis, il importe toutefois de préciser dans notre législation nationale que le service national requérant doit adresser une copie de sa demande à l'UIP luxembourgeoise, conformément à ce qui est exigé par l'article 9, paragraphe 3 de la directive.

Ad article 19

Cet article est relatif aux modalités techniques d'échange des informations entre Etats membres et ne suscite pas de commentaire particulier.

Chapitre 7 – *Conditions d'accès aux données PNR par Europol*

Ad article 20

L'article 20 définit les conditions selon lesquelles Europol peut demander des données à l'UIP et transpose l'article 10 de la directive.

La demande d'Europol doit transiter par son unité nationale, le service de police judiciaire de la Police grand-ducale en l'occurrence, et être motivée. Europol ne peut solliciter des données PNR ou des résultats de traitements que dans les limites de ses compétences et des objectifs qui lui sont assignés. Pour les infractions relevant de la compétence d'Europol, il est renvoyé au règlement 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.

Chapitre 8 – *Transfert de données vers des pays non membres de l'Union européenne*

Ad article 21

L'article 21, transposant l'article 11, paragraphe 1er de la directive, règle les conditions du transfert de données PNR à un pays non membre de l'Union européenne.

Un tel transfert est d'abord subordonné à l'existence d'une décision d'adéquation de la Commission européenne ou, en l'absence d'une telle décision, à l'existence de garanties appropriées.

Les autres conditions, respectivement énoncées aux points a, b et c, sont que la demande émane d'une autorité ayant pour mission la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité, que les données soient sollicitées à ces fins et que l'autorité n'accepte de transférer les données reçues à un autre pays tiers qu'à ces seules fins.

Le point d) précise que les conditions régissant les transferts de données PNR aux UIP des autres Etats membres sont également applicables aux transferts de données aux Etats tiers.

Ad article 22

L'article 22, transposant l'article 11, paragraphe 2 de la directive, envisage le transfert de données recueillies auprès d'un autre Etat membre à un pays tiers. Un tel transfert ne peut avoir lieu que si les

conditions définies à l'article 21 sont remplies et si l'Etat membre auprès duquel les données ont été recueillies a donné son accord (paragraphe 1er).

Le paragraphe 2 prévoit toutefois, à titre exceptionnel, que s'il existe une menace précise et réelle et si l'accord n'a pas pu être obtenu en temps utile, les données puissent être transférées sans l'accord préalable de l'Etat membre d'où proviennent les données.

Ad article 23

L'article 23 pose une condition supplémentaire aux transferts de données vers des pays tiers qui s'applique dans les cas de figure prévus respectivement aux articles 21 et 22.

Ad article 24

Cet article n'appelle pas de commentaire particulier.

Chapitre 9 – *Durée de conservation et dépersonnalisation des données*

Ad article 25

L'article 25 porte transposition de l'article 12, paragraphes 1er et 4 de la Directive. Il fixe la durée maximale de conservation des données PNR.

L'UIP ne peut conserver les données que pendant une période maximale de 5 ans qui commence à courir à partir du moment où les données ont été transférées. Etant donné que la loi prévoit trois transferts consécutifs de données, le premier ayant lieu deux jours avant le départ programmé du vol, le deuxième un jour avant le départ et le dernier immédiatement après la clôture du vol, il importe de préciser que c'est le dernier transfert prévu à l'article 6, paragraphe 1er du présent projet de loi qui fait courir le délai de cinq ans.

Au terme de la période de cinq ans, l'UIP doit effacer les données de façon irrémédiable. Cette disposition ne s'applique toutefois pas aux données qui ont été transmises aux services compétents et qui sont utilisées dans le cadre d'enquêtes ou de poursuites.

Ad article 26

Conformément à l'article 12, paragraphe 2 de la directive, le présent article oblige l'UIP à masquer les informations qui peuvent servir à identifier directement la personne à laquelle se rapportent les données PNR. Le masquage est une technique qui consiste à rendre ces éléments de données invisibles, sans toutefois les altérer. Des recherches automatisées restent ainsi possibles parmi les données masquées et des hits peuvent être générés. Toutefois les informations permettant d'identifier la personne à laquelle les données se rapportent ne sont pas affichées sur l'écran. Pour pouvoir visualiser ces informations, l'UIP doit obtenir l'accord du procureur d'Etat ou de son délégué ou, si la requête émane du Service de Renseignement de l'Etat, l'accord de la Commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat.

Le système technique devra été conçu de manière à ce que les données masquées ne puissent être consultées qu'après que l'accord de l'autorité compétente désignée en vertu du présent article aura été obtenu et qu'il soit possible de retracer les opérations de démasquage effectuées.

Des prescriptions de service interne à l'UIP devront établir une procédure à suivre par l'opérateur lorsqu'un *hit* est généré parmi des données PNR masquées.

Ad article 27

L'article 27, portant transposition de l'article 12, paragraphe 5 de la directive, est relatif à la durée de conservation des résultats des traitements de données PNR obtenus suite à une évaluation réalisée sur base de l'article 10. Ces résultats ne doivent être conservés par l'UIP que le temps nécessaire pour informer les services compétents et les UIP des autres Etats membres concernés de l'existence d'une correspondance positive.

L'alinéa 2 vise l'hypothèse où il s'est avéré, après vérification manuelle, que la concordance positive générée automatiquement était fausse. Pour éviter que les mêmes données ne génèrent d'autres fausses concordances positives à l'avenir, les résultats de ces traitements peuvent être conservés par l'UIP aussi longtemps que les données de base n'ont pas été effacées.

Chapitre 10 – *Protection des données à caractère personnel*

Ad article 28

L'article 15 de la Directive prévoit que dans chaque Etat membre l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les Etats membres en vertu de la présente directive et de surveiller l'application de celles-ci. Etant donné que les références faites à la décision-cadre 2008/977/JAI s'entendent comme des références faites à la législation actuellement en vigueur et à la législation qui la remplacera, que la décision-cadre 2008/977 est remplacée par la directive (UE) 2016/680 DU PARLEMENT EUROPEEN 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 et que la directive 2016/680 est transposée en droit luxembourgeois par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, il échet, pour satisfaire à la directive, de désigner la même autorité de contrôle que celle prévue par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. La Commission nationale pour la protection des données sera ainsi compétente pour contrôler le respect des dispositions de la présente loi en ce qui concerne la protection des données à caractère personnel.

La référence à l'article 41 du projet de loi de transposition de la Directive 2016/680 vise à préciser que les traitements de données PNR effectués par le ministère public sont soumis au contrôle de l'autorité de contrôle judiciaire.

Ad article 29

L'article 29 transpose l'article 5 et l'article 6, paragraphe 6 de la directive.

La directive qu'il s'agit de transposer prévoit un certain nombre de garanties destinées à assurer la protection des données PNR, parmi lesquelles la désignation obligatoire d'un délégué à la protection des données au sein de l'UIP.

Le présent article, outre de définir les missions du délégué à la protection des données, comporte un certain nombre de dispositions visant à garantir que celui-ci soit mis en mesure d'exercer ses missions de manière indépendante et effective, comme exigé par la directive. Ainsi, la personne qui est appelée à exercer cette fonction doit disposer d'une expertise en matière de protection des données (paragraphe 1er, alinéa 2) et avoir accès à toutes les données traitées par l'UIP.

Le paragraphe 3 consacre expressément l'indépendance du délégué à la protection des données. Cette disposition n'interdit pas que délégué soit issu du cadre du personnel de la Police grand-ducale, mais il appartiendra à la Police de prendre les mesures adéquates pour garantir que l'indépendance soit garantie. Ainsi, quelle que soit la carrière, policière ou civile, dont est issu le délégué et quelle que soit sa position hiérarchique par rapport au personnel de l'UIP, il importe de veiller à ce qu'il n'ait à rapporter qu'au responsable de l'UIP et qu'il ne reçoive d'instructions d'aucun membre du personnel de l'UIP. L'alinéa 3 prévoit que, dans certains cas, le délégué rapporte directement au Directeur général de la Police ou au Ministre. Il n'en reste pas moins que, si le délégué estime nécessaire, dans un cas particulier, de rapporter directement au directeur général ou au Ministre, il dénonce un éventuel traitement illicite parallèlement à l'autorité de contrôle.

Le délégué à la protection des données n'a pas seulement une mission de contrôle (paragraphe 2, alinéa 1er), mais également un rôle d'information et de conseil (alinéa 2). Le délégué fait par ailleurs office de point de contact pour les citoyens et pour la Commission nationale de protection des données (CNPD).

Ad article 30

L'article 30 oblige l'UIP à mettre à disposition du public un certain nombre d'informations dont, notamment, l'information sur les droits des personnes dont les données sont traitées en vertu de la présente loi.

Cette information peut se faire par n'importe quel moyen de communication approprié. En France, par exemple, les informations pertinentes en relation avec le traitement des données PNR et les droits des personnes sont publiée sur le site internet de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Ad article 31

Cet article transpose l'article 13, paragraphe 1er de la directive.

Les droits des personnes sont définis par référence aux articles pertinents du projet de loi portant transposition de la directive sur la protection des données pénales. Il s'agit du droit d'accès (article 14) et du droit de rectification ou d'effacement des données à caractère personnel et de la limitation du traitement prévu à l'article 16. Les limitations au droit d'accès prévues à l'article 15 et les règles relatives à l'exercice des droits fixées par l'article 17 du projet de loi auquel il est fait référence sont applicables aux données PNR.

Les personnes dont les données sont traitées en vertu de la présente loi disposent par ailleurs du droit d'introduire une réclamation auprès de la CNPD (art. 45), d'un droit de recours juridictionnel contre une décision de cette autorité (art. 46), un droit à un recours juridictionnel contre le responsable du traitement (art. 47) et le droit de se faire représenter (art. 48).

Ad article 32

Conformément à l'article 6, paragraphe 8 de la directive, cet article oblige l'UIP à traiter et à analyser les données en des endroits sécurisés situés sur le territoire du Grand-Duché de Luxembourg.

Ad article 33

Cet article, portant transposition de l'article 13, paragraphes 2 et 7 de la directive, impose à l'UIP de prendre des mesures et procédures techniques nécessaires pour assurer un niveau élevé de sécurité des données.

Le paragraphe 2 impose à l'UIP un certain nombre de mesures à prendre en ce qui concerne en particulier le traitement automatisé des données. Il s'agit de mesures destinées à:

(a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations);

(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

(c) empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées (contrôle de la conservation);

(d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

(e) garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation (contrôle de l'accès aux données);

(f) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission);

(g) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

(h) empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);

(i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration);

(j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

Ad article 34

L'article 34 porte transposition de l'article 13, paragraphe 5 de la directive. Il impose l'obligation pour l'UIP de conserver une trace documentaire relative à ses systèmes et procédures de traitement.

L'alinéa 2 énumère les éléments qui doivent figurer dans cette documentation.

Ad article 35

Le traitement des données PNR doit faire l'objet d'une journalisation, conformément à ce qui est prévu à l'article 13, paragraphe 6 de la directive. Il s'agit de permettre le traçage des traitements de données effectués afin qu'il soit possible d'identifier la personne qui a consulté des données, les données consultées, le moment et la finalité de cette consultation ainsi que l'identité des destinataires des données.

L'alinéa 3 précise les finalités de cette journalisation.

Les registres doivent être mis à la disposition de l'autorité de contrôle lorsqu'elle en fait la demande.

L'alinéa dernier oblige l'UIP à conserver les registres pendant une durée de cinq ans.

Ad article 36

L'article 36, portant transposition de l'article 13, paragraphe 8 de la directive, oblige l'UIP à informer la personne concernée et l'autorité de contrôle lorsqu'une atteinte aux données à caractère personnel est susceptible d'engendrer un risque élevé pour la protection de ces données ou d'affecter négativement la vie privée de la personne.

Chapitre 11 – *Sanctions*

Ad article 37

Les articles 37 et 38 transposent l'article 14 de la directive.

L'alinéa 1er de l'article 37 prévoit des sanctions pénales pour les infractions aux dispositions prévues aux articles 8, 15 et 36 de la présente loi. Ainsi, le présent projet de loi prévoit des sanctions pénales pour les mêmes violations que celles pour lesquelles le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale établit des sanctions pénales.

Les violations des autres dispositions applicables en matière de protection des données à caractère personnel sont punies de sanctions administratives telles que prévues par le projet de loi du *jj/mm/aaaa* relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Ad article 38

L'article 38 prévoit des sanctions administratives à l'égard des transporteurs aériens qui ne respectent pas les obligations qui leur sont imposées par la présente loi, à savoir transférer les données à l'UIP à des échéances prédéterminées ou sur demande, selon des modalités précises et dans des formats prédéfinis.

Dans la mesure où la directive impose aux Etats membres de fixer des sanctions effectives, proportionnées et dissuasives à l'égard des transporteurs et s'inspirant des textes français, allemand et belge, le Gouvernement a retenu une amende d'un montant maximal de 50.000 euros.

Le paragraphe 2 décrit la procédure à suivre en cas de manquement par un transporteur aérien. Le manquement est constaté par un procès-verbal adressé au Ministre ayant la Police dans ses attributions. Avant de prononcer une sanction, le Ministre informe le transporteur aérien de son intention de prononcer une amende en indiquant le montant de l'amende. Le transporteur a accès à son dossier et dispose d'un délai d'un mois à compter de la notification du projet de sanction par le Ministre pour présenter des observations écrites.

La décision du Ministre doit être motivée et notifiée à l'intéressé. Ce dernier dispose d'un délai d'un mois à compter de la notification pour introduire un recours en réformation devant le tribunal administratif.

*

TABLEAU DE CORRESPONDANCE

Directive (UE) 2016/681	*Projet de loi*
Art. 1er	
Art. 1	Art. 1
Art. 2	
Art. 2	//
Art. 3	
Art. 3	Art. 2
Art. 4	
Art. 4 paragraphe 1er	Art. 3
Art. 4 paragraphe 2	
Art. 4 paragraphe 3	Art. 4, alinéa 2
Art. 4 paragraphe 4	//
Art. 4 paragraphe 5	
Art. 5	
Art. 5, paragraphe 1er	Art. 29, paragraphe 1, alinéa 1er et paragraphe 2, alinéas 1er et 2
Art. 5, paragraphe 2	Art. 29, paragraphe 1er, alinéa 2 et paragraphe 3
Art. 5, paragraphe 3	Art. 29, paragraphe 2, alinéa 3
Art. 6	
Art. 6, paragraphe 1er	Art. 9
Art. 6, paragraphe 2	Art. 10, paragraphe 1er, art. 11, art. 12
Art. 6, paragraphe 3	Art 10, paragraphe 2
Art. 6, paragraphe 4	Art. 10, paragraphe 2
Art. 6, paragraphe 5	Art. 10, paragraphe 3
Art. 6, paragraphe 6	Art. 10, paragraphes 3 et 4
Art. 6, paragraphe 7	Art. 29, paragraphe 4
Art. 6, paragraphe 8	Art. 32
Art. 6, paragraphe 9	Art. 10, paragraphes 5 et 6
Art. 7	
Art. 7 paragraphe 1er	Art. 13
Art. 7 paragraphe 2	Art. 13
Art. 7 paragraphe 3	//
Art. 7 paragraphe 4	Art. 14, alinéa 1er
Art. 7 paragraphe 5	Art. 14, alinéa 2
Art. 7 paragraphe 6	Art. 15 et art. 8
Art. 8	
Art. 8, paragaphe 1er	Art. 5
Art. 8, paragraphe 2	//
Art. 8, paragraphe 3	Art. 6, paragraphe 1er, alinéa 1er et art. 7
Art. 8, paragraphe 4	Art. 6, paragraphe 1er, alinéa 2
Art. 8, paragraphe 5	Art. 6, paragraphe 2

Directive (UE) 2016/681	*Projet de loi*
Art. 9	
Art. 9, paragraphe 1er	Art. 16
Art. 9, paragraphe 2	Art. 17, paragraphe 1er
Art. 9, paragraphe 3	Art. 17, paragraphe (2) et 18 alinéa 2
Art. 9, paragraphe 4	Art. 17, paragraphe 3
Art. 9, paragraphe 5	Art. 19
Art. 10	
Art. 10, paragraphe 1er	Art. 20, paragraphe 1er
Art. 10, paragraphe 2	Art. 20
Art. 10, paragraphe 3	//
Art. 10, paragraphe 4	//
Art. 11	
Art. 11, paragraphe 1er	Art. 21
Art. 11, paragraphe 2	Art. 22
Art. 11, paragraphe 3	Art. 23
Art. 11, paragraphe 4	Art. 24
Art. 12	
Art. 12, paragraphe 1er	Art. 25, alinéa 1er
Art. 12, paragraphe 2	Art. 26, paragraphe 1er
Art. 12, paragraphe 3	Art. 26, paragraphe 2
Art. 12, paragraphe 4	Art. 25, alinéa 2
Art. 12, paragraphe 5	Art. 27
Art. 13	
Art. 13, paragraphe 1er	Art. 30, point e) at art. 31
Art. 13, paragraphe 2	Art. 33, alinéa 2
Art. 13, paragraphe 3	//
Art. 13, paragraphe 4	Art. 8
Art. 13, paragraphe 5	Art. 34
Art. 13, paragraphe 6	Art. 35
Art. 13, paragraphe 7	Art. 33, alinéa 1er
Art. 13, paragraphe 8	Art. 36
Art. 14	
Art. 14	Art. 37 et 38
Art. 15	
Art. 15, paragraphe 1er	Art. 28
Art. 15, paragraphe 2	
Art. 15, paragraphe 3	
Art. 15, paragraphe 4	
Art. 16	
Art. 16, paragraphe 1er	Art. 7
Art. 16, paragraphe 2	
Art. 16, paragraphe 3	
Art. 16, paragraphe 4r	
Art. 16, paragraphe 5	

Directive (UE) 2016/681	*Projet de loi*
Art. 17	
Art. 17	//
Art. 18	
Art. 18	//
Art. 19	
Art. 19	//
Art. 20	
Art. 20	//
Art. 21	
Art. 21	//
Art. 22	
Art. 22	//
Annexe I	Annexe I
Annexe II	Annexe II

*

FICHE FINANCIERE

Conformément à l'article 79 de la loi modifiée du 8 juin 1999 portant sur le budget, la comptabilité et la trésorerie de l'Etat, le Ministre de la Sécurité Intérieure déclare que le présent projet de loi aura un impact sur le budget de l'Etat.

Remarque préliminaire

Par la transposition de la directive (UE) 2016/681 un nouveau système devra être crée de toutes pièces avec une unité spécifique. Les besoins exprimés ci-dessous reflètent l'état de connaissance des évaluations à l'heure actuelle et sont susceptibles d'être revues au fil du temps.

Le Luxembourg peut bénéficier du cofinancement communautaire par le Fonds pour la Sécurité intérieure 2016-2020 pour la mise en place du PNR, qui s'élève à 292.217 euros.

1. La mise en place d'une Unité d'information passagers (UIP)

a) Infrastructure: Des aménagements dans les immeubles seront nécessaires ainsi que l'équipement des locaux: Investissement: 60.000,00 € au titre de l'article 06.1.12.270 „entretien, exploitation et location d'immeubles, dépenses diverses".

b) Personnel: L'UIP devra être dotée du personnel nécessaire à la réalisation de ses missions. Ce besoin est évalué à 4 personnels de la Police grand-ducale (2 en 2017 et 2 en 2018) dans un premier temps et pour un fonctionnement en semaine sur un horaire en journée. Si une entrée en opération 24/24 heures devait s'avérer nécessaire, un triplement des personnels serait nécessaire.

2. La collecte des données

Pour la collecte des données passagers auprès des transporteurs aériens opérant à l'aéroport de Luxembourg un dispositif technique doit être mis en place et entretenu. Un raccordement avec le système informatique de la quarantaine de transporteurs aériens afin de recueillir la vingtaine de champs d'informations par passagers doit être établi.

- Investissement: 540.000,00 € au titre de l'article 06.1.74.051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 215.000,00 € /an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

- Frais d'exploitation: 503.000,00 € /an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

Des synergies européennes pourraient permettre de réduire le coût net par transaction par des économies d'échelle.

3. Le traitement des données

Un logiciel pour l'analyse et l'exploitation des données passagers recueillies doit être installé. Pour l'heure le Luxembourg a repris à titre gratuit le système d'un partenaire européen. Si un développement propre devait s'avérer comme indispensable au cours des premières années d'opération les coûts suivants seraient à prévoir:

- Investissement: 500.000,00 € au titre de l'article 06.1.74. 051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 100.000,00 €/an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

4. Le système de gestion des échanges entre les Etats membres de l'Union Européenne

Un projet européen devrait voir le jour pour gérer les échanges entre les Unités Informations Passagers des 28 Etats membres. Sur besoin un développement propre serait nécessaire.

- Investissement: 150.000,00 € au titre de l'article 06.1.74.051 „Coopération policière européenne: développement de nouveaux systèmes d'information"
- Maintenance: 30.000,00 €/an au titre de l'article 06.1.12.071 „Coopération policière européenne: développement de nouveaux systèmes d'information"

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet:	**Projet de loi relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave**
Ministère initiateur:	**Ministère de la Sécurité intérieure**
Auteur(s):	**Martine Schmit**
Tél:	**247-84687**
Courriel:	**martine.schmit@msi.etat.lu**
Objectif(s) du projet:	**transposition de la directive 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**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):	
Ministère d'Etat (Service de Renseignement de l'Etat) **Ministère des Finances (Administration des Douanes et Accises)** **Ministère du Développement durable et des Infrastructures (Direction de l'Aviation civile)** **Ministère de la Justice/autorités judiciaires**	
Date:	**1.6.2016**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s): Oui ☒ Non ☐

   Si oui, laquelle/lesquelles:
   Ministère d'Etat (Service de renseignement)
   Ministère des Finances (Administration des Douanes et accises)
   Ministère du Développement durable et des Infrastructures (Direction de l'aviation civile)
   Ministère de la Justice / autorités judiciaires
   Commissaire du gouvernement à la protection des banques de données

   Remarques/Observations:

2. Destinataires du projet:
   - Entreprises/Professions libérales: Oui ☒ Non ☐
   - Citoyens: Oui ☒ Non ☐
   - Administrations: Oui ☒ Non ☐

3. Le principe „Think small first" est-il respecté? Oui ☐ Non ☐ N.a.[1] ☒

   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité?)

   Remarques/Observations:

4. Le projet est-il lisible et compréhensible pour le destinataire? Oui ☒ Non ☐

   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière? Oui ☐ Non ☒

   Remarques/Observations:

1 N.a.: non applicable.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures? Oui ☐ Non ☒

   Remarques/Observations:

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s)? (un coût imposé pour satisfaire à une obligation d'information émanant du projet?) Oui ☒ Non ☐

   Si oui, quel est le coût administratif[3] approximatif total? (nombre de destinataires x coût administratif par destinataire) Le coût des transferts des données PNR (0,04 € par „push" par passager)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire? Oui ☐ Non ☒ N.a. ☐

   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?

   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4]? Oui ☒ Non ☐ N.a. ☐

   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il? Des données à caractère personnel contenues au niveau des dossiers passagers

8. Le projet prévoit-il:
   - une autorisation tacite en cas de non-réponse de l'administration? Oui ☐ Non ☐ N.a. ☒
   - des délais de réponse à respecter par l'administration? Oui ☐ Non ☐ N.a. ☒
   - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois? Oui ☐ Non ☒ N.a. ☐

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p. ex. prévues le cas échéant par un autre texte)? Oui ☐ Non ☐ N.a. ☒

   Si oui, laquelle:

10. En cas de transposition de directives communautaires, le principe „la directive, rien que la directive" est-il respecté? Oui☒ Non ☐ N.a. ☐

    Si non, pourquoi?

11. Le projet contribue-t-il en général à une:
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire? Oui ☐ Non ☒

    Remarques/Observations:

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)? Oui ☒ Non ☐
Si oui, quel est le délai pour disposer du nouveau système?
25 mai 2018 (= délai de transposition)

14. Y a-t-il un besoin en formation du personnel de l'administration concernée? Oui ☒ Non ☐ N.a. ☐
Si oui, lequel? formation des agents de l'unité d'information passagers
Remarques/Observations:

Egalité des chances

15. Le projet est-il:
- principalement centré sur l'égalité des femmes et des hommes? Oui ☐ Non ☒
- positif en matière d'égalité des femmes et des hommes? Oui ☐ Non ☒
  Si oui, expliquez de quelle manière:
- neutre en matière d'égalité des femmes et des hommes? Oui ☒ Non ☐
  Si oui, expliquez pourquoi:
- négatif en matière d'égalité des femmes et des hommes? Oui ☐ Non ☒
  Si oui, expliquez de quelle manière:

16. Y a-t-il un impact financier différent sur les femmes et les hommes? Oui ☐ Non ☒ N.a. ☐
Si oui, expliquez de quelle manière:

Directive „services"

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5]? Oui ☐ Non ☐ N.a. ☒
Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6]? Oui ☐ Non ☐ N.a. ☒
Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur:
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

5 Article 15, paragraphe 2 de la directive „services" (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive „services" (cf. Note explicative, p. 10-11)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) Le 6 novembre 2007, la Commission a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives. Cependant, n'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, la proposition de la Commission est devenue obsolète.

(2) «Le programme de Stockholm — Une Europe ouverte et sûre qui sert et protège les citoyens» ([3]) invite la Commission à présenter une proposition concernant l'utilisation des données PNR 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.

(3) Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, la Commission a décrit un certain nombre d'éléments essentiels d'une politique de l'Union dans ce domaine.

(4) La directive 2004/82/CE du Conseil ([4]) régit la transmission aux autorités nationales compétentes, par les transporteurs aériens, d'informations préalables relatives aux passagers (ci-après dénommées «données API»), en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration illégale.

(5) Les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes.

(6) L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels.

(7) L'évaluation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être

([1]) JO C 218 du 23.7.2011, p. 107.
([2]) Position du Parlement européen du 14 avril 2016 (non encore parue au Journal officiel) et décision du Conseil du 21 avril 2016.
([3]) JO C 115 du 4.5.2010, p. 1.
([4]) 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).

soumises à un examen plus approfondi par les autorités compétentes. L'utilisation des données PNR permet de contrer la menace que représentent les infractions terroristes et les formes graves de criminalité sous un angle autre que par le traitement d'autres catégories de données à caractère personnel. Cependant, pour veiller à ce que le traitement de données PNR reste limité à ce qui est nécessaire, la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente. Par ailleurs, les critères d'évaluation devraient être définis d'une manière qui réduise au minimum le nombre d'identifications erronées de personnes innocentes par le système.

(8) Les transporteurs aériens recueillent et traitent déjà des données PNR de leurs passagers pour leur propre usage commercial. La présente directive ne devrait pas leur imposer l'obligation de recueillir ou de conserver des données supplémentaires des passagers et ne devrait pas non plus contraindre les passagers à communiquer des données en sus de celles qui sont déjà transmises aux transporteurs aériens.

(9) Certains transporteurs aériens conservent les données API qu'ils recueillent en les regroupant avec les données PNR, alors que d'autres ne le font pas. L'utilisation combinée des données PNR et des données API présente une valeur ajoutée en ce qu'elle aide les États membres à vérifier l'identité d'une personne, renforçant ainsi la valeur du résultat en termes de prévention, de détection et de répression des infractions et réduisant au minimum le risque de soumettre des personnes innocentes à des vérifications et à des enquêtes. C'est pourquoi il est important de veiller à ce que, lorsque les transporteurs aériens recueillent des données API, ils les transfèrent, que les données API soient conservées ou non par des moyens techniques différents de ceux utilisés pour d'autres données PNR.

(10) 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, il est essentiel que tous les États membres adoptent des dispositions obligeant les transporteurs aériens qui assurent des vols extra-UE à transférer les données PNR qu'ils recueillent, y compris les données API. Les États membres devraient également avoir la possibilité d'étendre cette obligation aux transporteurs aériens qui assurent des vols intra-UE. Ces dispositions devraient s'entendre sans préjudice de la directive 2004/82/CE.

(11) Le traitement des données à caractère personnel devrait être proportionné aux objectifs de sécurité spécifiques poursuivis par la présente directive.

(12) La définition des infractions terroristes appliquée dans le cadre de la présente directive devrait être la même que celle figurant dans la décision-cadre 2002/475/JAI du Conseil ([1]). La définition des formes graves de criminalité devrait englober les catégories d'infractions énumérées à l'annexe II de la présente directive.

(13) Il convient que les données PNR soient transmises à une seule unité d'information passagers désignée (UIP) dans l'État membre concerné, de manière à garantir la clarté et à réduire les coûts supportés par les transporteurs aériens. L'UIP peut avoir plusieurs antennes dans un même État membre et les États membres peuvent également mettre en place conjointement une seule UIP. Les États membres devraient échanger leurs informations par l'intermédiaire de réseaux d'échange d'informations appropriés afin de faciliter le partage des informations et de garantir l'interopérabilité.

(14) Les États membres devraient assumer les coûts liés à l'utilisation, à la conservation et à l'échange de données PNR.

(15) Une liste des données PNR à transmettre à une UIP devrait être établie dans le but de refléter les exigences légitimes des pouvoirs publics en matière de prévention et de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, renforçant par là la sécurité intérieure de l'Union et la protection des droits fondamentaux, notamment le respect de la vie privée et la protection des données à caractère personnel. À cette fin, il convient d'appliquer des normes élevées conformément à la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée «convention n° 108») et la convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). Une telle liste ne devrait pas être fondée sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne. Les données PNR ne devraient comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers qui permettent aux autorités compétentes d'identifier les passagers aériens représentant une menace pour la sécurité intérieure.

(16) Actuellement, deux méthodes de transfert des données sont possibles: la méthode «pull», par laquelle les autorités compétentes de l'État membre qui requièrent les données PNR peuvent accéder au système de réservation du transporteur aérien et en extraire («pull») une copie des données PNR requises, et la méthode «push», par laquelle les transporteurs aériens transmettent («push») les données PNR requises à l'autorité requérante, ce qui permet aux transporteurs aériens de garder le contrôle sur les données transmises. La méthode «push» est réputée offrir un niveau plus élevé de protection des données et devrait être obligatoire pour tous les transporteurs aériens.

([1]) Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

(17) La Commission soutient les lignes directrices de l'organisation de l'aviation civile internationale (OACI) relatives aux données PNR. Ces lignes directrices devraient, par conséquent, servir de base pour l'adoption des formats de données reconnus pour les transferts des données PNR par les transporteurs aériens aux États membres. Afin d'assurer des conditions uniformes d'exécution des formats de données reconnus et des protocoles correspondants applicables au transfert des données provenant des transporteurs aériens, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([1]).

(18) Les États membres devraient prendre toutes les mesures nécessaires pour permettre aux transporteurs aériens de remplir leurs obligations au titre de la présente directive. Il y a lieu que les États membres prévoient des sanctions effectives, proportionnées et dissuasives, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne respectent pas leurs obligations en matière de transfert de données PNR.

(19) Chaque État membre devrait être responsable de l'évaluation des menaces potentielles liées aux infractions terroristes et aux formes graves de criminalité.

(20) En tenant pleinement compte du droit à la protection des données à caractère personnel et du droit à la non-discrimination, aucune décision qui produit des effets juridiques préjudiciables à une personne ou l'affecte de manière significative ne devrait être prise sur la seule base du traitement automatisé des données PNR. Par ailleurs, conformément aux articles 8 et 21 de la Charte, aucune décision de cette nature ne devrait introduire de discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. La Commission devrait également prendre en compte ces principes lors du réexamen de l'application de la présente directive.

(21) Le résultat du traitement des données PNR ne devrait en aucun cas être utilisé par les États membres comme motif pour se soustraire à leurs obligations internationales au titre de la convention du 28 juillet 1951 relative au statut des réfugiés, telle qu'amendée par le protocole du 31 janvier 1967, ni être invoqué pour refuser aux demandeurs d'asile des voies sûres et effectives d'entrée légales sur le territoire de l'Union afin d'y exercer leur droit à la protection internationale.

(22) En tenant pleinement compte des principes mis en évidence par la récente jurisprudence pertinente de la Cour de justice de l'Union européenne, l'application de la présente directive devrait garantir le plein respect des droits fondamentaux et du droit au respect de la vie privée ainsi que du principe de proportionnalité. Elle devrait aussi véritablement remplir les objectifs de nécessité et de proportionnalité afin de répondre aux intérêts généraux reconnus par l'Union et à la nécessité de protéger les droits et libertés d'autrui dans la lutte contre les infractions terroristes et les formes graves de criminalité. L'application de la présente directive devrait être dûment justifiée et les garanties nécessaires devraient être mises en place afin d'assurer la légalité de tout stockage, de toute analyse, de tout transfert ou de toute utilisation des données PNR.

(23) Les États membres devraient échanger entre eux et avec Europol les données PNR qu'ils reçoivent, lorsque cela est jugé nécessaire 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. Les UIP devraient, le cas échéant, transmettre sans tarder le résultat du traitement des données PNR aux UIP des autres États membres en vue d'un complément d'enquête. Les dispositions de la présente directive devraient s'entendre sans préjudice d'autres instruments de l'Union relatifs à l'échange d'informations entre les services de police et d'autres services répressifs et les autorités judiciaires, y compris la décision 2009/371/JAI du Conseil ([2]) et la décision-cadre 2006/960/JAI du Conseil ([3]). Il convient que les échanges de données PNR soient régis par les règles relatives à la coopération policière et judiciaire et ne portent pas atteinte au niveau élevé de protection de la vie privée et des données à caractère personnel exigé par la Charte, la convention nº 108 et la CEDH.

(24) L'échange sécurisé d'informations relatives aux données PNR entre les États membres devrait être assuré par l'intermédiaire de tout canal de coopération existant entre les autorités compétentes des États membres, et en particulier avec Europol, par l'intermédiaire de son application de réseau d'échange sécurisé d'informations (SIENA).

([1]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

([2]) Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (JO L 121 du 15.5.2009, p. 37).

([3]) Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (JO L 386 du 29.12.2006, p. 89).

(25) Les données PNR ne devraient être conservées que pour la durée nécessaire et proportionnée aux objectifs de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière. En raison de leur nature et de leurs utilisations, il est indispensable que les données PNR soient conservées pendant une période suffisamment longue pour permettre leur analyse et leur utilisation dans le cadre d'enquêtes. Pour éviter toute utilisation disproportionnée, il convient que, après le délai initial de conservation, les données PNR soient dépersonnalisées par le masquage d'éléments des données. Afin de garantir le niveau le plus élevé de protection de données, l'accès à l'intégralité des données PNR, qui permettent l'identification directe de la personne concernée, ne devrait être accordé que dans des conditions très strictes et limitées après ce délai initial.

(26) Lorsque des données PNR spécifiques ont été transmises à une autorité compétente et servent dans le cadre d'enquêtes ou de poursuites pénales spécifiques, leur durée de conservation par cette autorité devrait être fixée par le droit national, indépendamment des périodes de conservation de données prévues par la présente directive.

(27) Dans chaque État membre, le traitement de données PNR effectué par l'UIP et par les autorités compétentes devrait être soumis à une norme de protection des données à caractère personnel du droit national conforme à la décision-cadre 2008/977/JAI du Conseil [1] et aux exigences spécifiques de protection des données énoncées dans la présente directive. Les références à la décision-cadre 2008/977/JAI devraient s'entendre comme des références faites à la législation actuellement en vigueur ainsi qu'à la législation qui la remplacera.

(28) Compte tenu du droit à la protection des données à caractère personnel, il convient que les droits des personnes concernées en ce qui concerne le traitement de leurs données PNR, tels que les droits d'accès, de rectification, d'effacement et de limitation, ainsi que le droit à réparation et le droit à un recours juridictionnel, soient conformes à la décision-cadre 2008/977/JAI et au niveau de protection élevé conféré par la Charte et la CEDH.

(29) Eu égard au droit des passagers d'être informés du traitement des données à caractère personnel les concernant, les États membres devraient veiller à ce que les passagers reçoivent des informations précises, aisément accessibles et facilement compréhensibles, sur la collecte des données PNR, le transfert de celles-ci à l'UIP et leurs droits en tant que personnes concernées.

(30) La présente directive s'applique sans préjudice du droit de l'Union et du droit national concernant le principe de l'accès du public aux documents officiels.

(31) Les États membres ne devraient être autorisés à transférer des données PNR vers des pays tiers qu'au cas par cas et dans le plein respect des dispositions adoptées par les États membres en vertu de la décision-cadre 2008/977/JAI. Pour assurer la protection des données à caractère personnel, ces transferts devraient être soumis à des exigences supplémentaires relatives à leur finalité. Ils devraient également être soumis aux principes de nécessité et de proportionnalité et au niveau de protection élevé conféré par la Charte et la CEDH.

(32) Les autorités de contrôle nationales mises en place en application de la décision-cadre 2008/977/JAI devraient également être chargées de fournir des conseils sur l'application des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci.

(33) La présente directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

(34) La présente directive est sans préjudice des règles actuelles de l'Union sur les modalités des contrôles aux frontières ou des règles de l'Union régissant l'entrée sur le territoire de l'Union et la sortie de celui-ci.

(35) Comme les dispositions nationales relatives au traitement des données à caractère personnel, y compris des données PNR, divergent sur le plan juridique et technique, les transporteurs aériens doivent et devront faire face à des exigences différentes en ce qui concerne le type d'informations à transmettre et les conditions dans lesquelles

[1] 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).

ces informations doivent être communiquées aux autorités nationales compétentes. Ces divergences peuvent nuire à une coopération efficace entre ces autorités aux fins de la prévention et de la détection des infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Il est dès lors nécessaire d'établir, au niveau de l'Union, un cadre juridique commun pour le transfert et le traitement des données PNR.

(36) La présente directive respecte les droits fondamentaux et les principes énoncés dans la Charte, en particulier le droit à la protection des données à caractère personnel, le droit au respect de la vie privée et le droit à la non-discrimination consacrés par ses articles 8, 7 et 21; elle devrait dès lors être mise en œuvre en conséquence. La présente directive est compatible avec les principes de la protection des données et ses dispositions sont conformes à la décision-cadre 2008/977/JAI. En outre, afin de respecter le principe de proportionnalité, la présente directive prévoit, pour des points spécifiques, des règles de protection des données plus strictes que celles prévues dans la décision-cadre 2008/977/JAI.

(37) Le champ d'application de la présente directive est aussi limité que possible dès lors que: il prévoit que la conservation des données PNR dans les UIP est autorisée pendant une période n'excédant pas cinq ans au terme de laquelle les données devraient être effacées; il prévoit que les données sont dépersonnalisées par le masquage d'éléments des données après une période initiale de six mois; et il interdit la collecte et l'utilisation des données sensibles. Pour garantir l'efficacité et un niveau élevé de protection des données, les États membres sont tenus de veiller à ce qu'une autorité de contrôle nationale indépendante et, notamment, un délégué à la protection des données soient chargés de fournir des conseils et de surveiller la manière dont les données PNR sont traitées. Tout traitement de données PNR devrait être consigné ou faire l'objet d'une trace documentaire à des fins de vérification de sa licéité et d'autocontrôle et pour garantir de manière adéquate l'intégrité des données et la sécurité du traitement. Les États membres devraient également veiller à ce que les passagers reçoivent des informations claires et précises sur la collecte des données PNR et sur leurs droits.

(38) Étant donné que les objectifs de la présente directive — à savoir le transfert de données PNR par les transporteurs aériens et leur traitement aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière — ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(39) Conformément à l'article 3 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, ces États membres ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive.

(40) Conformément aux articles 1er et 2 du protocole n° 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(41) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil [1] et a rendu son avis le 25 mars 2011,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier

Objet et champ d'application

1. La présente directive prévoit:

a) le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE;

b) le traitement des données visées au point a), notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

[1] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

2. Les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière, comme prévu à l'article 6, paragraphe 2, points a), b) et c).

Article 2

Application de la présente directive aux vols intra-UE

1. Si un État membre décide d'appliquer la présente directive aux vols intra-UE, il le notifie à la Commission par écrit. Un État membre peut adresser ou révoquer une telle notification à tout moment. La Commission publie cette notification et la révocation éventuelle de celle-ci au *Journal officiel de l'Union européenne*.

2. Lorsqu'une notification visée au paragraphe 1 est adressée, toutes les dispositions de la présente directive s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE et aux données PNR des vols intra-UE comme s'il s'agissait de données PNR de vols extra-UE.

3. Un État membre peut décider d'appliquer la présente directive uniquement à certains vols intra-UE. Lorsqu'il prend une telle décision, l'État membre sélectionne les vols qu'il juge nécessaires afin de poursuivre les objectifs de la présente directive. L'État membre peut décider à tout moment de modifier la sélection des vols intra-UE.

Article 3

Définitions

Aux fins de la présente directive, on entend par:

1) «transporteur aérien», une entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de passagers;

2) «vol extra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance d'un pays tiers et devant atterrir sur le territoire d'un État membre ou en provenance du territoire d'un État membre et devant atterrir dans un pays tiers, y compris, dans les deux cas, les vols comportant d'éventuelles escales sur le territoire d'États membres ou de pays tiers;

3) «vol intra-UE», tout vol, régulier ou non, effectué par un transporteur aérien en provenance du territoire d'un État membre et devant atterrir sur le territoire d'un ou de plusieurs États membres, sans escale sur le territoire d'un pays tiers;

4) «passager», toute personne, y compris une personne en correspondance ou en transit et à l'exception du personnel d'équipage, transportée ou devant être transportée par un aéronef avec le consentement du transporteur aérien, lequel se traduit par l'inscription de cette personne sur la liste des passagers;

5) «dossier(s) passager(s)» ou «PNR», un dossier relatif aux conditions de voyage de chaque passager, qui contient les informations nécessaires pour permettre le traitement et le contrôle des réservations par les transporteurs aériens concernés qui assurent les réservations, pour chaque voyage réservé par une personne ou en son nom, que ce dossier figure dans des systèmes de réservation, des systèmes de contrôle des départs (utilisés pour contrôler les passagers lors de l'embarquement) ou des systèmes équivalents offrant les mêmes fonctionnalités;

6) «système de réservation», le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations;

7) «méthode push», la méthode par laquelle les transporteurs aériens transfèrent les données PNR énumérées à l'annexe I vers la base de données de l'autorité requérante;

8) «infractions terroristes», les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI;

9) «formes graves de criminalité», les infractions énumérées à l'annexe II qui sont passibles d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale d'au moins trois ans au titre du droit national d'un État membre;

10) «dépersonnaliser par le masquage d'éléments des données», rendre invisibles pour un utilisateur les éléments des données qui pourraient servir à identifier directement la personne concernée.

CHAPITRE II

Responsabilités des états membres

Article 4

Unité d'informations passagers

1. Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne une antenne d'une telle autorité, en tant que son UIP.

2. L'UIP est chargée:

a) de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes visées à l'article 7;

b) de l'échange à la fois des données PNR et du résultat de leur traitement avec les UIP d'autres États membres et avec Europol, conformément aux articles 9 et 10.

3. Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Les États membres dotent les UIP des ressources adéquates pour l'accomplissement de leurs missions.

4. Deux États membres ou plus (ci-après dénommés «États membres participants») peuvent mettre en place ou désigner une autorité unique en tant qu'UIP. Cette UIP est établie dans l'un des États membres participants et est considérée comme l'UIP nationale de tous les États membres participants. Ces derniers conviennent conjointement des modalités de fonctionnement de l'UIP et respectent les exigences prévues dans la présente directive.

5. Chaque État membre notifie à la Commission la mise en place de son UIP dans un délai d'un mois à compter de cette mise en place et peut, à tout moment, modifier sa notification. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

Article 5

Délégué à la protection des données au sein de l'UIP

1. L'UIP nomme un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes.

2. Les États membres dotent les délégués à la protection des données des moyens pour accomplir leurs missions et obligations, conformément au présent article, de manière effective et en toute indépendance.

3. Les États membres veillent à ce que la personne concernée ait le droit de s'adresser au délégué à la protection des données, en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant.

Article 6

Traitement des données PNR

1. Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

2. L'UIP ne traite les données PNR qu'aux fins suivantes:

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

3. Lorsqu'elle réalise l'évaluation visée au paragraphe 2, point a), l'UIP peut:

a) confronter les données PNR aux bases de données utiles 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, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

4. L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

5. Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

6. L'UIP d'un État membre transmet, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au paragraphe 2, point a), ou le résultat du traitement de ces données aux autorités compétentes visées à l'article 7 de ce même État membre. Ces transferts ne sont effectués qu'au cas par cas et, en cas de traitement automatisé des données PNR, après un réexamen individuel par des moyens non automatisés.

7. Les États membres veillent à ce que le délégué à la protection des données ait accès à toutes les données traitées par l'UIP. Si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, le délégué à la protection des données peut renvoyer l'affaire à l'autorité de contrôle nationale.

8. Le stockage, le traitement et l'analyse des données PNR par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

9. Les conséquences des évaluations des passagers visées au paragraphe 2, point a), du présent article ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union à la libre circulation sur le territoire de l'État membre concerné prévu dans la directive 2004/38/CE du Parlement européen et du Conseil ([1]). En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) nº 562/2006 du Parlement européen et du Conseil ([2]), les conséquences de ces évaluations doivent respecter ledit règlement.

Article 7

Autorités compétentes

1. Chaque État membre arrête une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données en vue de procéder à un examen plus approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

2. Les autorités visées au paragraphe 1 sont des autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière.

3. Aux fins de l'article 9, paragraphe 3, chaque État membre notifie à la Commission la liste de ses autorités compétentes au plus tard 25 mai 2017 et peut modifier sa notification à tout moment. La Commission publie cette notification et toute modification y afférente au *Journal officiel de l'Union européenne*.

4. Les données PNR et le résultat du traitement de ces données reçus par l'UIP ne peuvent faire l'objet d'un traitement ultérieur par les autorités compétentes des États membres qu'aux seules fins spécifiques de la prévention ou de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi que des enquêtes ou des poursuites en la matière.

5. Le paragraphe 4 s'applique sans préjudice des compétences des autorités répressives ou judiciaires nationales, lorsque d'autres infractions, ou des indices d'autres infractions, sont détectés dans le cadre d'actions répressives menées à la suite de ce traitement.

6. Les autorités compétentes ne peuvent prendre aucune décision produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR. Ces décisions ne peuvent pas être fondées sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

Article 8

Obligations imposées aux transporteurs aériens concernant les transferts de données

1. Les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent, par la «méthode push», les données PNR énumérées à l'annexe I, pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités, vers la base de données de l'UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel il décollera. Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR de tous les passagers du vol incombe au transporteur aérien qui assure le vol. Lorsqu'un vol extra-UE comporte une ou plusieurs escales dans des aéroports des États membres, les transporteurs aériens transfèrent les données PNR de tous les passagers aux UIP de tous les États membres concernés. Il en est de même lorsqu'un vol intra-UE comporte une ou plusieurs escales dans les aéroports de différents États membres, mais uniquement en ce qui concerne les États membres qui recueillent les données PNR des vols intra-UE.

([1]) Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) nº 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

([2]) Règlement (CE) nº 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 105 du 13.4.2006, p. 1).

2. Dans l'hypothèse où les transporteurs aériens ont recueilli des informations préalables sur les passagers (ci-après dénommées «données API») énumérées à l'annexe I, point 18, mais ne les conservent pas par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, les États membres adoptent les mesures nécessaires pour veiller à ce que les transporteurs aériens transfèrent également ces données, par la «méthode push», à l'UIP des États membres visés au paragraphe 1. Dans le cas d'un tel transfert, toutes les dispositions de la présente directive s'appliquent à ces données API.

3. Les transporteurs aériens transfèrent les données PNR par voie électronique au moyen de protocoles communs et de formats de données reconnus à adopter en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2, ou, en cas de défaillance technique, par tout autre moyen approprié garantissant un niveau de sécurité des données approprié:

a) 24 à 48 heures avant l'heure de départ programmée du vol; et

b) immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'ils ne peuvent plus embarquer ou débarquer.

4. Les États membres autorisent les transporteurs aériens à limiter le transfert visé au paragraphe 3, point b), aux mises à jour des transferts visés au point a) dudit paragraphe.

5. Lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, les transporteurs aériens transfèrent, au cas par cas, des données PNR à d'autres moments que ceux mentionnés au paragraphe 3, à la demande d'une UIP conformément au droit national.

Article 9

Échange d'informations entre États membres

1. Les États membres veillent à ce que, en ce qui concerne les personnes identifiées par une UIP conformément à l'article 6, paragraphe 2, toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États membres. Les UIP des États membres destinataires transmettent les informations reçues à leurs autorités compétentes, conformément à l'article 6, paragraphe 6.

2. L'UIP d'un État membre a le droit de demander, si nécessaire, à l'UIP de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par le masquage d'éléments des données au titre de l'article 12, paragraphe 2, ainsi que, si nécessaire, le résultat de tout traitement de ces données, si celui-ci a déjà été réalisé en vertu de l'article 6, paragraphe 2, point a). Cette demande est dûment motivée. Elle peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. Les UIP transmettent dès que possible les informations demandées. Si les données demandées ont été dépersonnalisées par le masquage d'éléments des données conformément à l'article 12, paragraphe 2, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), et uniquement si elle y est autorisée par une autorité visée à l'article 12, paragraphe 3, point b).

3. Les autorités compétentes d'un État membre ne peuvent demander directement à l'UIP d'un autre État membre de leur communiquer des données PNR qui sont conservées dans sa base de données que lorsque cela est nécessaire dans les cas d'urgence et dans les conditions fixées au paragraphe 2. Les demandes des autorités compétentes sont motivées. Une copie de la demande est toujours envoyée à l'UIP de l'État membre requérant. Dans tous les autres cas, les autorités compétentes canalisent leurs demandes par l'intermédiaire de l'UIP de leur propre État membre.

4. À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP d'un autre État membre obtienne des données PNR conformément à l'article 8, paragraphe 5, et les communique à l'UIP requérante.

5. L'échange d'informations au titre du présent article peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération existant entre les autorités compétentes des États membres. La langue utilisée pour la demande et l'échange

d'informations est celle applicable au canal utilisé. Lorsqu'ils procèdent aux notifications conformément à l'article 4, paragraphe 5, les États membres communiquent également à la Commission les coordonnées des points de contact auxquels les demandes peuvent être adressées en cas d'urgence. La Commission communique lesdites coordonnées aux États membres.

Article 10

Conditions d'accès aux données PNR par Europol

1. Europol est habilité à demander aux UIP des États membres des données PNR ou le résultat du traitement de ces données dans les limites de ses compétences et pour l'accomplissement de ses missions.

2. Europol peut présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une demande électronique dûment motivée de transmission de données PNR spécifiques ou du résultat du traitement de ces données. Europol peut présenter cette demande lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des États membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes en la matière, dans la mesure où ladite infraction ou ladite forme de criminalité relève de la compétence d'Europol en vertu de la décision 2009/371/JAI. Cette demande énonce les motifs raisonnables sur lesquels se fonde Europol pour estimer que la transmission des données PNR ou du résultat du traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée, ou à des enquêtes en la matière.

3. Europol informe le délégué à la protection des données nommé conformément à l'article 28 de la décision 2009/371/JAI de chaque échange d'informations au titre du présent article.

4. Les échanges d'information au titre du présent article ont lieu par l'intermédiaire de SIENA et conformément à la décision 2009/371/JAI. La langue utilisée pour la demande et l'échange d'informations est celle applicable à SIENA.

Article 11

Transfert de données vers des pays tiers

1. Un État membre peut transférer à un pays tiers des données PNR et le résultat du traitement de ces données, qui sont conservés par l'UIP conformément à l'article 12, uniquement au cas par cas et si:

a) les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies;

b) le transfert est nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2, et uniquement avec l'accord exprès dudit État membre; et

d) les mêmes conditions que celles prévues à l'article 9, paragraphe 2, sont remplies.

2. Nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI, les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne sont autorisés que dans des circonstances exceptionnelles et uniquement si:

a) ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un État membre ou un pays tiers; et

b) l'accord préalable ne peut pas être obtenu en temps utile.

L'autorité chargée de donner son accord est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

3. Les États membres ne transfèrent des données PNR aux autorités compétentes de pays tiers que dans des conditions compatibles avec la présente directive et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

4. Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé.

Article 12

Période de conservation et dépersonnalisation des données

1. Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient conservées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol.

2. À l'expiration d'une période de six mois suivant le transfert des données PNR visé au paragraphe 1, toutes les données PNR sont dépersonnalisées par le masquage des éléments des données suivants qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations «grands voyageurs»;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte; et

f) toute donnée API qui a été recueillie.

3. À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que:

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par:

   i) une autorité judiciaire; ou

   ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

4. Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.

5. Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de manière à éviter de futures «fausses» concordances positives.

Article 13

Protection des données à caractère personnel

1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel effectué au titre de la présente directive, chaque passager dispose du même droit à la protection de ses données à caractère personnel, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national et en application des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI. Lesdits articles sont par conséquent applicables.

2. Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre 2008/977/JAI concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive.

3. La présente directive est sans préjudice de l'applicabilité de la directive 95/46/CE du Parlement européen et du Conseil ([1]) au traitement des données à caractère personnel par les transporteurs aériens, en particulier en ce qui concerne leurs obligations de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.

4. Les États membres interdisent le traitement des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. Dans l'hypothèse où l'UIP reçoit des données PNR révélant de telles informations, elle les efface immédiatement.

5. Les États membres veillent à ce que l'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous leur responsabilité. Cette documentation comprend au minimum:

a) le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données PNR au sein de l'UIP et les différents niveaux d'autorisation d'accès;

b) les demandes formulées par les autorités compétentes et les UIP d'autres États membres;

c) toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

6. Les États membres veillent à ce que l'UIP tienne des registres au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Les registres des opérations de consultation et de communication indiquent, en particulier, la finalité, la date et l'heure de ces opérations et, dans la mesure du possible, l'identité de la personne qui a consulté ou communiqué les données PNR, ainsi que l'identité des destinataires de ces données. Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit. L'UIP met les registres à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

Ces registres sont conservés pendant cinq ans.

7. Les États membres veillent à ce que leur UIP mette en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et à la nature des données PNR.

8. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, les États membres veillent à ce que l'UIP fasse part de cette atteinte à la personne concernée et à l'autorité de contrôle nationale sans retard injustifié.

Article 14

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.

En particulier, les États membres déterminent le régime des sanctions, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne transmettent pas de données comme le prévoit l'article 8, ou ne les transmettent pas dans le format requis.

Les sanctions prévues doivent être effectives, proportionnées et dissuasives.

([1]) 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).

Article 15

Autorité de contrôle nationale

1. Chaque État membre prévoit que l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci. L'article 25 de ladite décision-cadre s'applique.

2. Ces autorités de contrôle nationales exercent les activités au titre du paragraphe 1 en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel.

3. Chaque autorité de contrôle nationale:

a) traite les réclamations introduites par toute personne concernée, enquête sur l'affaire et informe la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable;

b) vérifie la licéité du traitement des données, effectue des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation visée au point a).

4. Chaque autorité de contrôle nationale conseille, sur demande, toute personne concernée quant à l'exercice des droits que lui confèrent les dispositions adoptées en vertu de la présente directive.

CHAPITRE III

Mesures d'exécution

Article 16

Protocoles communs et formats de données reconnus

1. Tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive sont effectués par des moyens électroniques qui offrent des garanties suffisantes en ce qui concerne les mesures de sécurité techniques et les mesures organisationnelles régissant le traitement à effectuer. En cas de défaillance technique, les données PNR peuvent être transférées par tout autre moyen approprié, pour autant que le même niveau de sécurité soit maintenu et que le droit de l'Union en matière de protection des données soit pleinement respecté.

2. À partir de l'année qui suit la date à laquelle la Commission adopte pour la première fois des protocoles communs et des formats de données reconnus conformément au paragraphe 3, tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP aux fins de la présente directive se font par voie électronique à l'aide de méthodes sécurisées respectant ces protocoles communs. Ces protocoles sont identiques pour tous les transferts afin d'assurer la sécurité des données PNR pendant le transfert. Les données PNR sont transférées sous un format de données reconnu afin d'en assurer la lisibilité par toutes les parties concernées. Tous les transporteurs aériens sont tenus de choisir et de préciser à l'UIP le protocole commun et le format de données qu'ils ont l'intention d'utiliser pour leurs transferts.

3. La Commission dresse la liste des protocoles communs et des formats de données reconnus et, si nécessaire, l'adapte au moyen d'actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 17, paragraphe 2.

4. Tant que les protocoles communs et les formats de données reconnus visés aux paragraphes 2 et 3 ne sont pas disponibles, le paragraphe 1 s'applique.

5. Dans un délai d'un an à compter de la date d'adoption des protocoles communs et des formats de données reconnus visés au paragraphe 2, chaque État membre veille à ce que les mesures techniques nécessaires soient adoptées pour pouvoir utiliser ces protocoles communs et formats de données.

Article 17

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) nº 182/2011 s'applique.

CHAPITRE IV

Dispositions finales

Article 18

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 25 mai 2018. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 19

Réexamen

1. Sur la base des informations communiquées par les États membres, y compris les informations statistiques visées à l'article 20, paragraphe 2, la Commission procède, au plus tard le 25 mai 2020, au réexamen de tous les éléments de la présente directive et communique et présente un rapport au Parlement européen et au Conseil.

2. Dans le cadre de son réexamen, la Commission accorde une attention particulière:

a) au respect des normes applicables de protection des données à caractère personnel;

b) à la nécessité et à la proportionnalité de la collecte et du traitement des données PNR au regard de chacune des finalités énoncées dans la présente directive;

c) à la durée de la période de conservation des données;

d) à l'efficacité de l'échange d'informations entre les États membres; et

e) à la qualité des évaluations, y compris en ce qui concerne les informations statistiques recueillies en vertu de l'article 20.

3. Le rapport visé au paragraphe 1 examine également s'il est nécessaire, proportionné et efficace d'inclure dans le champ d'application de la présente directive la collecte et le transfert des données PNR, à titre obligatoire, pour l'ensemble des vols intra-UE ou une sélection de ceux-ci. La Commission tient compte de l'expérience acquise par les États membres, en particulier ceux qui appliquent la présente directive aux vols intra-UE conformément à l'article 2. Le rapport examine également s'il est nécessaire d'inclure des opérateurs économiques autres que les transporteurs, tels que des agences et des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, dans le champ d'application de la présente directive.

4. Le cas échéant, au vu du réexamen effectué au titre du présent article, la Commission soumet une proposition législative au Parlement européen et au Conseil en vue de modifier la présente directive.

Article 20

Données statistiques

1. Les États membres fournissent chaque année à la Commission une série de statistiques sur les données PNR communiquées aux UIP. Ces statistiques ne contiennent pas de données à caractère personnel.

2. Les statistiques concernent au moins:

a) le nombre total de passagers dont les données PNR ont été recueillies et échangées;

b) le nombre de passagers identifiés en vue d'un examen plus approfondi.

Article 21

Rapports avec d'autres instruments

1. Les États membres peuvent continuer d'appliquer les accords ou arrangements bilatéraux ou multilatéraux en matière d'échange d'informations entre les autorités compétentes qu'ils ont conclus entre eux et qui sont en vigueur au 24 mai 2016, dans la mesure où ceux-ci sont compatibles avec la présente directive.

2. La présente directive s'applique sans préjudice de l'applicabilité de la directive 95/46/CE au traitement des données à caractère personnel par les transporteurs aériens.

3. La présente directive s'applique sans préjudice des obligations et engagements d'États membres ou de l'Union qui découlent d'accords bilatéraux ou multilatéraux avec des pays tiers.

Article 22

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Bruxelles, le 27 avril 2016.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

ANNEXE I

Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens

1. Code repère du dossier passager
2. Date de réservation/d'émission du billet
3. Date(s) prévue(s) du voyage
4. Nom(s)
5. Adresse et coordonnées (numéro de téléphone, adresse électronique)
6. Toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation
7. Itinéraire complet pour le PNR concerné
8. Informations «grands voyageurs»
9. Agence de voyages/agent de voyages
10. Statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation
11. Indications concernant la scission/division du PNR
12. Remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée)
13. Informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix
14. Numéro du siège et autres informations concernant le siège
15. Informations sur le partage de code
16. Toutes les informations relatives aux bagages
17. Nombre et autres noms de voyageurs figurant dans le PNR
18. Toute information préalable sur les passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée)
19. Historique complet des modifications des données PNR énumérées aux points 1 à 18.

ANNEXE II

Liste des infractions visées à l'article 3, point 9)

1. Participation à une organisation criminelle
2. Traite des êtres humains
3. Exploitation sexuelle des enfants et pédopornographie
4. Trafic de stupéfiants et de substances psychotropes
5. Trafic d'armes, de munitions et d'explosifs
6. Corruption
7. Fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union
8. Blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro
9. Cybercriminalité
10. Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
11. Aide à l'entrée et au séjour irréguliers
12. Meurtre, coups et blessures graves
13. Trafic d'organes et de tissus humains
14. Enlèvement, séquestration et prise d'otage
15. Vol organisé ou vol à main armée
16. Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
17. Contrefaçon et piratage de produits
18. Falsification de documents administratifs et trafic de faux
19. Trafic de substances hormonales et d'autres facteurs de croissance
20. Trafic de matières nucléaires et radioactives
21. Viol
22. Infractions graves relevant de la Cour pénale internationale
23. Détournement d'avion/de navire
24. Sabotage
25. Trafic de véhicules volés
26. Espionnage industriel.

Impression: CTIE – Division Imprimés et Fournitures de bureau