JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 690 du 16 août 2018

Loi du 1er août 2018 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 et portant modification de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

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

Notre Conseil d'État entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 26 juillet 2018 et celle du Conseil d'État du 27 juillet 2018 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

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 :

1° « 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 ;
2° « 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 ;
3° « 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 ;
4° « système de réservation » : le système interne du transporteur aérien, dans lequel les données PNR sont recueillies aux fins du traitement des réservations ;
5° « système de contrôle des départs » : le système utilisé pour contrôler les passagers lors de l'embarquement ;
6° « données PNR » : les données contenues dans le dossier passager et énumérées à l'annexe I ;
7° « méthode push » : la méthode par laquelle les transporteurs aériens transfèrent les données PNR vers la base de données de l'Unité d'informations passagers telle que créée à l'article 3 ;
8° « infractions terroristes » : les infractions visées au Livre II, Titre 1ier, Chapitre III-1 du Code pénal ;
9° « 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 ;
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 ;

11° « services compétents » : les services visés à l'article 13.

Chapitre 2 - Unité d'informations 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 :

1° de la collecte des données PNR transférées par les transporteurs aériens ainsi que de la conservation et du traitement de ces données ;
2° du transfert de ces données et des résultats de leur traitement aux services compétents ;
3° de l'échange de ces données et des résultats de leur traitement avec les unités d'informations passagers des autres États membres de l'Union européenne, avec Europol et avec les pays tiers.

Art. 4.

(1) Le responsable de l'UIP a la qualité de responsable du traitement des données PNR.

Il est désigné parmi les membres de la catégorie de traitement A1 du cadre policier de la Police grand-ducale.

(2) Outre le personnel de la Police grand-ducale, l'UIP peut comprendre du personnel de l'Administration des douanes et accises et du Service de renseignement de l'État. Chaque membre du personnel de l'UIP agit dans les limites des attributions légales de l'administration dont il relève.

Les membres du personnel de l'Administration des douanes et accises et du Service de renseignement de l'État sont désignés à l'UIP par une décision conjointe du ministre ayant la Police grand-ducale dans ses attributions et du ministre du ressort. Ils continuent de relever de l'autorité hiérarchique de leur chef d'administration et sont placés sous l'autorité fonctionnelle du responsable de l'UIP.

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 en provenance de, à destination de ou transitant par le Luxembourg pour autant qu'ils aient déjà recueilli de telles données dans le cours normal de leurs activités de transport aérien.

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 :

1° 48 heures avant l'heure de départ programmée du vol ;
2° 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 2°, peut se limiter à une mise à jour du transfert visé à l'alinéa 1er, point 1°.

(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 de protocoles communs et de formats de données reconnus, adoptés par la Commission européenne conformément à l'article 16, paragraphe 3, de la 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.

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.

(3) Dans l'hypothèse où un transporteur aérien ne conserve pas les données API énumérées à l'annexe I, point 18, par les mêmes moyens techniques que ceux utilisés pour d'autres données PNR, il transfère également ces données par la méthode « push » à l'UIP. Dans le cas d'un tel transfert, toutes les dispositions de la présente loi s'appliquent à ces données API.

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 :

1° aux traitements de données à caractère personnel mis en œuvre par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;
2° 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 du Grand-Duché 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 Grand-Duché de Luxembourg et un autre État membre de l'Union européenne auquel s'applique le règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), 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.

Sont habilités à demander à l'UIP ou à recevoir de celle-ci des données PNR ou le résultat du traitement de ces données, en vue de procéder à un examen approfondi de ces informations ou de prendre les mesures appropriées aux fins de la prévention et de la détection d'infractions terroristes ou des formes graves de criminalité, ainsi que des enquêtes et poursuites en la matière :

1° la Police grand-ducale ;
2° le Service de renseignement de l'État conformément à l'article 5, paragraphe 4, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
3° l'Administration des douanes et accises.

En recherchant les crimes et délits visés à l'article 2, points 8° et 9°, le procureur d'État peut, par une décision écrite et motivée, charger un officier de police judiciaire de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 12.

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 grand-ducale 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.

Les décisions produisant des effets juridiques préjudiciables à une personne ou l'affectant de manière significative 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.

Chapitre 6 - Échange d'informations entre les États 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 États 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 État 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 général d'État ou son délégué.

Les dispositions du présent paragraphe ne portent pas atteinte aux dispositions tant internationales que nationales sur l'entraide judiciaire internationale en matière pénale.

(2) Dans des cas d'urgence, les autorités compétentes des autres États 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 1er sont applicables.

(3) 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 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 États membres de l'Union européenne des données PNR ou les résultats du traitement de ces données.

Lorsqu'un service compétent demande directement des données PNR auprès de l'UIP d'un autre État 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 existant entre les services compétents des États 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 :

1° 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 dans la matière et ;
2° 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.

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 :

1° l'une des conditions prévues à l'article 34, paragraphe 1er, point d) de la loi du 1er août 2018 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 est remplie ;
2° l'autorité destinataire est chargée de la prévention, recherche, constatation et poursuite d'infractions terroristes ou de formes graves de criminalité ;
3° le transfert est nécessaire aux fins telles que définies à l'article 1er ;
4° 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 ;
5° les conditions prévues à l'article 17, paragraphe 1er sont remplies.

Les dispositions du présent article ne portent pas atteinte aux dispositions légales sur l'entraide judiciaire internationale en matière pénale.

Art. 22.

(1) Sans préjudice des conditions prévues à l'article 21, l'UIP ne peut transférer des données PNR obtenues d'un autre État membre de l'Union européenne à un pays non membre de l'Union européenne que si l'État 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 :

1° 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 de l'Union européenne ou un pays tiers ;
2° l'accord préalable n'a pas pu être obtenu en temps utile.

L'UIP de l'État 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 à posteriori.

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 qu'après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte les conditions et garanties de la présente loi.

Art. 24.

Le délégué à la protection des données visé à l'article 29 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.

À 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) À 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 :

1° 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 ;
2° l'adresse et les coordonnées ;
3° 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 ;
4° les informations « grands voyageurs » ;
5° les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte ;
6° toute donnée API qui a été recueillie.

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

1° elle est nécessaire aux fins visées à l'article 12 ;
2° elle a été approuvée par le procureur général d'État ou son délégué ou, si les données sont destinées à être communiquées au Service de renseignement de l'État, par la commission spéciale prévue à l'article 7 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

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 États 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.

L'autorité de contrôle visée à l'article 39 de la loi du 1er août 2018 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 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 8 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et elle dispose, à cette fin, des pouvoirs prévus à l'article 14 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 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 grand-ducale ou, s'il juge nécessaire, au ministre ayant la Police grand-ducale 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 conformément à la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Art. 30.

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

1° ses coordonnées ;
2° les coordonnées du délégué à la protection des données ;
3° les finalités du traitement auquel sont destinées les données PNR ;
4° le droit d'introduire une réclamation auprès de la Commission nationale pour la protection des données et les coordonnées de cette autorité ;
5° 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 13 à 17 de la loi du 1er août 2018 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 44 à 46 de la loi du 1er août 2018 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 Grand-Duché de 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 28, paragraphe 2 de la loi du 1er août 2018 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 :

1° 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 ;
2° les demandes formulées par les services compétents et les UIP des autres États membres de l'Union européenne ;
3° 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 la Commission nationale pour la protection des données de cette atteinte.

Chapitre 11 - Sanctions

Art. 37.

La violation intentionnelle de l'article 8, alinéa 1er et de l'article 15 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 prononce la cessation du traitement contraire aux dispositions de l'article 8, alinéa 1er et de l'article 15 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Pour le surplus, les dispositions de l'article 47, paragraphes 1er, 2, 4, 5 et 6 de la loi du 1er août 2018 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 visés à l'article 3, 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 grand-ducale 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.

Chapitre 12 - Dispositions modificatives

Art. 39.

Dans l'article 5 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, il est inséré un paragraphe 4 libellé comme suit :

« (4) Pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées, le SRE peut demander la communication des données PNR visées à l'article 10, paragraphe 4, et à l'article 12, de la loi du 1er août 2018 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.

Le directeur du SRE rapporte tous les mois par écrit au Comité la liste des consultations des données des passagers ainsi que les motifs spécifiques pour lesquels l'exercice des missions a exigé la demande de communication.

En cas d'urgence, la demande de communication des données PNR peut être mise en œuvre sur autorisation verbale du directeur, à confirmer par écrit dans un délai de quarante-huit heures. »

Art. 40.

À l'article 8, paragraphe 1er de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, la lettre a) est supprimée.

Chapitre 13 - Disposition finale

Art. 41.

La référence à la présente loi peut se faire sous une forme abrégée en recourant à l'intitulé suivant : « Loi du 1er août 2018 relative au traitement des données des dossiers passagers ».

ANNEXE I

Liste des données PNR

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 2, 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.

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

Le Ministre de la Sécurité intérieure,
Étienne Schneider

Cabasson, le 1er août 2018.
Henri

Doc. parl. 7151 ; sess. ord. 2016-2017 et 2017-2018 ; Dir. (UE) 2016/681.