

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

2011/0023(COD) - 27/04/2016 - Acte final

OBJECTIF : permettre le transfert des 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.

ACTE LÉGISLATIF : Directive (UE) 2016/681 du Parlement européen et du Conseil 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.

CONTENU : la directive vise à **réglementer le transfert vers les États membres, par les compagnies aériennes, des données PNR des passagers des vols internationaux** (vols extra-UE), ainsi que le traitement de ces données par les autorités compétentes.

Si un État membre décide d'appliquer la directive aux **vols intra-UE**, il devra le notifier à la Commission par écrit. Un État membre pourra également décider d'appliquer la directive uniquement à certains vols intra-UE. Dans ce cas, il devra sélectionner les vols qu'il juge nécessaires afin de poursuivre les objectifs de la directive.

Unité d'informations passagers (UIP) : pour garantir l'efficacité et un niveau élevé de protection des données, les États membres seront 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.

- Toute personne concernée aura 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.
- Le délégué à la protection des données **aura accès à toutes les données traitées par l'UIP** et pourra, s'il estime que traitement de certaines données n'était pas licite, renvoyer l'affaire à l'autorité de contrôle nationale.
- **Europol** pourra également présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une demande électronique motivée de transmission de données PNR spécifiques ou du résultat du traitement de ces données.

Traitement des données : les données PNR recueillies ne pourront 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.

Ainsi, l'UIP ne pourra traiter les données PNR que pour réaliser une **évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ** prévu de celui-ci. Cette évaluation aura pour finalité d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités

compétentes et, le cas échéant, par Europol, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité.

Lorsqu'il réalise cette évaluation, l'UIP pourra : a) confronter les données PNR aux bases de données utiles et b) traiter les données PNR au regard de critères préétablis.

L'évaluation des passagers au regard de **critères préétablis** devra être réalisée de façon **non discriminatoire**. Ces critères devront être ciblés, proportionnés et spécifiques, et être réexaminés à intervalles réguliers.

Transfert de données vers des pays tiers : les États membres ne seront autorisés à transférer des données PNR vers des pays tiers qu'au **cas par cas** et dans le respect des dispositions adoptées par les États membres en vertu 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 seront autorisés que dans des circonstances exceptionnelles.

Conservation et dépersonnalisation des données : la directive 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 devront être effacées.

Après une période de six mois suivant le transfert initial des données PNR, les données devront être dépersonnalisées par le **masquage** des éléments pouvant servir à identifier directement le passager tels que le nom, l'adresse et les coordonnées, mais également les informations sur tous les modes de paiement, y compris l'adresse de facturation, ou les informations «grands voyageurs».

À l'expiration de cette période de six mois, la communication de l'intégralité des données PNR ne sera autorisée que dans des conditions strictement définies.

Protection des données à caractère personnel : tout traitement de données PNR devra 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.

L'UIP devra tenir des **registres** au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Ces registres devront être conservés pendant **cinq ans**.

La directive **interdit explicitement le traitement des données PNR sensibles** révélant 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 recevrait des données PNR révélant de telles informations, elle devrait les effacer immédiatement.

Protocoles communs et formats de données reconnus : 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, tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP devront se faire par voie électronique à l'aide de méthodes sécurisées respectant ces protocoles communs.

ENTRÉE EN VIGUEUR : 24.5.2016.

TRANSPOSITION : 25.5.2018.