Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Fiche d'information *Passenger Name Record* (PNR) Analyse d'impact relative à la protection des données personnelles (AIPD)

État : juillet 2024

Contexte

Lors de sa séance du 15 mai 2024, le Conseil fédéral a approuvé le message relatif à la loi sur les données relatives aux passagers aériens et l'a transmis au Parlement. Cette base légale permettra à la Suisse de mettre en place un système PNR (*Passenger Name Record*) national. Ce dernier contribuera à la lutte contre le terrorisme et la grande criminalité et à la protection de la place économique suisse.

Protection des données et respect des droits de la personnalité

La loi garantit la protection des données et des droits de la personnalité des passagers. Elle régit de façon stricte l'accès aux données PNR et la finalité poursuivie.

Le Conseil fédéral a renforcé les aspects liés à la protection des données par rapport au projet mis en consultation. Il a par exemple réduit la durée de conservation des données : par conséquent, les données ne présentant aucun indice objectif d'infraction terroriste ou d'une autre infraction pénale grave ne peuvent pas être enregistrées pendant plus de six mois. En outre, ces données sont pseudonymisées un mois déjà après leur introduction dans le système PNR, ce qui signifie que les informations personnelles identifiables (nom, coordonnées, date de naissance, etc.) ne sont plus directement visibles dans le système. En revanche, les données présentant des indices objectifs d'infraction terroriste ou d'une autre infraction pénale grave peuvent être conservées pendant une durée maximale de cinq ans.

Toutes les étapes de traitement importantes seront consignées dans un procès-verbal électronique, qui permettra au Préposé fédéral à la protection des données et à la transparence (PFPDT) de veiller au respect de la protection des données.

Une analyse d'impact relative à la protection des données personnelles (AIPD) a été réalisée pour la première fois conformément à la nouvelle loi sur la protection des données et les demandes du PFPDT ont été prises en compte lors de l'élaboration du projet législatif.

Résumé de l'AIPD pour le projet PNR Suisse

Le projet PNR Suisse concerne la collecte et le traitement de données relatives aux passagers aériens par l'Office fédéral de la police (fedpol) dans le but de lutter contre le terrorisme et la grande criminalité. L'AIPD sert à identifier et à évaluer à un stade préalable les risques potentiels pour la protection des données. L'objectif de l'AIPD ne se résume pas à la prévisibilité et à l'évaluation des risques "élevés". Son intérêt pratique réside aussi et surtout dans

le fait qu'elle permet, d'une part, de documenter de façon claire l'origine et l'analyse des risques systémiques et relevant des techniques de sécurité et, d'autre part, de réduire les risques à un niveau acceptable du point de vue du droit de la protection des données par des mesures appropriées.

Les contenus essentiels de l'AIPD sont résumés ci-après :

Traitement de données

Les données relatives aux passagers aériens collectées au moment de la réservation d'un vol comprennent le nom, les coordonnées et les détails sur le voyage des passagers. Les compagnies aériennes ont besoin de ces données pour assurer le bon déroulement du vol et doivent les communiquer à l'unité d'information passagers (UIP).

Il s'agit d'un ensemble de 19 catégories de données figurant à l'annexe 1 de la loi sur les données relatives aux passagers aériens (LDPa).

Personnes particulièrement vulnérables concernées

Les personnes décrites dans cette section de l'AIPD sont considérées comme particulièrement vulnérables en raison de leur situation spéciale :

- **enfants** : les enfants voyageant seuls ou avec un accompagnant qui n'est pas l'un de leurs deux parents sont particulièrement vulnérables. Les mineurs non accompagnés de moins de 18 ans, pour lesquels sont saisies des informations détaillées telles que le nom, l'âge, la langue et les coordonnées de la personne présente au départ et à l'arrivée, sont aussi inclus ;
- **personnes en situation de handicap**: si les données PNR ne donnent généralement aucune information directe sur un handicap, certaines circonstances pourraient en présumer un, comme le fait d'embarquer une chaise roulante. Cette information n'est toutefois que spéculation et n'est pas saisie systématiquement.

Étapes de traitement

L'utilité principale du traitement de données par l'État est la possibilité de prendre rapidement des mesures préventives et répressives pour prévenir et poursuivre le terrorisme et les autres infractions pénales graves.

Dès que l'UIP reçoit des données PNR, elle les compare automatiquement avec celles issues de systèmes d'information de police ainsi qu'avec des profils de risque et des listes d'observation, dans le but d'identifier des menaces potentielles de terrorisme et de grande criminalité, ou des personnes recherchées au niveau international ou national qui sont soupçonnées d'avoir commis de tels actes ou qui ont été condamnées à de longues peines privatives de liberté pour de tels actes. Si la comparaison n'aboutit à aucune concordance, les données sont pseudonymisées au bout d'un mois et effacées automatiquement après cinq mois supplémentaires. Les données qui produisent une concordance sont communiquées aux autorités compétentes (police, autorités de poursuite pénale et services de renseignement de la Confédération et des cantons) et marquées. Les données marquées peuvent être conservées pendant cinq ans au plus.

Après la comparaison automatique, les données PNR ne sont plus traitées que dans des cas isolés, lorsqu'une autorité compétente demande qu'elles lui soient communiquées.

Les personnes impliquées dans le traitement sont les collaborateurs de l'UIP et les autorités fédérales et cantonales compétentes. Comme les données de plusieurs millions de passagers sont traitées chaque année, le nombre de processus de traitement est très élevé. Par conséquent, des technologies de pointe et le système PNR éprouvé de l'ONU sont utilisés pour le traitement des données. Le recours à l'intelligence artificielle n'est pas prévu dans ce domaine, et toutes les mesures sont strictement mises en œuvre selon les dispositions légales et les normes en matière de protection des données.

Par ailleurs, l'UIP transmet au Service de renseignement de la Confédération les données PNR des liaisons aériennes à risque définis par le Conseil fédéral pour qu'il puisse les traiter de manière autonome.

Risques identifiés

Au total, l'AIPD identifie 14 risques systémiques pour les droits fondamentaux des personnes concernées, notamment les suivants :

- l'accès non autorisé aux données PNR;
- la classification erronée de personnes et le marquage erroné de leurs données en raison d'informations incomplètes et de données de qualité insuffisante;
- le traitement de données personnelles sensibles non autorisé.

Mesures visant à réduire les risques

Au total, l'AIPD présente 22 mesures permettant de réduire efficacement les risques identifiés à un niveau résiduel acceptable.

Ces mesures sont de nature juridique, organisationnelle et technique et visent à réduire la probabilité de survenance et l'étendue des dommages.

Voici quelques exemples de l'influence des mesures sur les risques résiduels :

- **le renforcement des contrôles d'accès et des mesures techniques de sécurité**, par exemple l'amélioration des procédures de vérification et des procès-verbaux, aide à empêcher l'accès non autorisé aux données PNR et réduit ainsi le risque de violation de la protection des données;
- **des formations régulières dispensées aux collaborateurs accroissent la prise de conscience et les compétences concernant la gestion de données sensibles**, contribuant ainsi à réduire au maximum les erreurs humaines pouvant engendrer une violation de la protection des données;
- **le progrès technologique et la vérification régulière des systèmes**, y compris les tests d'intrusion et la vérification de l'intégrité des données, garantissent que les systèmes sont sûrs et fonctionnent correctement, ce qui réduit le risque de pannes techniques;
- **des directives juridiques et organisationnelles claires** permettent une meilleure conformité et renforcent l'obligation de rendre compte au sein de l'organisation, contribuant ainsi à réduire les risques juridiques et opérationnels;
- **la minimisation des données et l'amélioration des pratiques en matière de protection des données** telles que l'effacement et la pseudonymisation automatiques des données après expiration des délais fixés aident à réduire le risque d'utilisation abusive de données anciennes ou de celles qui ne sont plus nécessaires.

La mise en œuvre de ces mesures est décisive pour garantir la sécurité et la protection des données personnelles traitées.

Évaluation du PFPDT

Le PFPDT a évalué la présente AIPD et constate, dans sa prise de position d'avril 2024, que:

- l'AIPD a été soigneusement établie;
- les informations nécessaires à l'évaluation sont disponibles;
- les risques exposés pour la personnalité ou les droits fondamentaux des personnes concernées couvrent l'ensemble du processus de traitement des données prévu dans la LDPa;

- des mesures appropriées et visant à réduire les risques sont prévues pour plusieurs risques élevés constatés.

Informations complémentaires

Le document complet *Datenschutzfolgeabschätzung PNR Schweiz* est disponible sur demande à l'adresse suivante: pnr@fedpol.admin.ch.