



Factsheet «Passenger Name Record» (PNR) – Valutazione d’impatto sulla protezione dei dati (VIPD)

Stato: luglio 2024

Contesto

Nella seduta del 15 maggio 2024 il Consiglio federale ha adottato e trasmesso al Parlamento il messaggio concernente la legge sui dati dei passeggeri aerei. Questa base legale permetterà alla Svizzera di creare un sistema nazionale per il trattamento dei dati dei passeggeri aerei («Passenger Name Record», PNR). Il PNR contribuisce a combattere il terrorismo e altre gravi forme di criminalità nonché a proteggere la piazza economica svizzera.

Protezione dei dati e rispetto dei diritti della personalità

La legge garantisce la protezione dei dati e dei diritti della personalità dei passeggeri aerei. L’accesso ai dati PNR e la finalità del loro utilizzo sono soggetti a una rigorosa regolamentazione.

Rispetto all’avamprogetto posto in consultazione, il Consiglio federale ha rafforzato la protezione dei dati. La durata di conservazione dei dati è stata ridotta. I dati che non presentano indizi concreti di terrorismo o di altre gravi forme di criminalità non possono essere quindi conservati per più di sei mesi. Questi dati sono inoltre pseudonimizzati dopo un mese. Ciò significa che i dati identificativi, quali il nome, i dati di contatto e la data di nascita, non sono più direttamente visibili nel sistema. Per contro, i dati che presentano indizi concreti di terrorismo o di gravi forme di criminalità possono essere conservati per un periodo massimo di cinque anni.

Tutte le fasi importanti del trattamento sono documentate all’interno di un verbale elettronico. I verbali servono all’Incaricato federale della protezione dei dati e della trasparenza (IFPDT) per vigilare sul rispetto della protezione dei dati.

Nell’elaborare il disegno di legge è stata eseguita per la prima volta una valutazione d’impatto sulla protezione dei dati (VIPD) ai sensi della nuova legge sulla protezione dei dati. Le richieste formulate dall’IFPDT sono state considerate al momento dell’elaborazione del disegno.

Riassunto della valutazione d’impatto sulla protezione dei dati (VIPD) per il progetto PNR Svizzera

Il progetto PNR («Passenger Name Record») Svizzera riguarda la raccolta e il trattamento dei dati dei passeggeri aerei da parte dell’Ufficio federale di polizia (fedpol) ai fini della lotta al terrorismo e alle gravi forme di criminalità. La valutazione d’impatto sulla protezione dei

dati (VIPD) mira a individuare e valutare tempestivamente potenziali rischi in materia di protezione dei dati. Lo scopo della VIPD non si esaurisce nella definizione del grado di prevedibilità e nella valutazione dei rischi «elevati». La VIPD è infatti utile anche sul piano pratico in quanto consente in particolare di documentare in modo tracciabile come sono individuati e analizzati i rischi sistemici di sicurezza e di ridurre tali rischi a un livello accettabile sotto il profilo del diritto sulla protezione dei dati, adottando provvedimenti adeguati. Di seguito sono riassunti i contenuti principali della VIPD.

Descrizione del trattamento dei dati

Al momento della prenotazione di un biglietto aereo, le compagnie aeree raccolgono dati quali nome, informazioni di contatto e dettagli relativi al viaggio dei passeggeri aerei. Necessitano di tali dati ai fini della gestione del volo e, nel quadro di PNR, devono inoltre trasmetterli all'unità d'informazione sui passeggeri (UIP).

Il set di dati PNR comprende 19 categorie di dati conformemente all'allegato 1 della legge sui dati dei passeggeri aerei (LDPA).

Descrizione delle persone particolarmente vulnerabili interessate

In questa sezione sono descritte le persone che, in ragione della loro situazione speciale, sono considerate particolarmente vulnerabili. Si tratta soprattutto di:

- **minori:** i minori che viaggiano da soli o che sono accompagnati da una persona diversa da un loro genitore sono particolarmente vulnerabili. Questa categoria di persone comprende i minori non accompagnati di età inferiore a 18 anni per i quali sono registrate informazioni dettagliate quali nome, età, lingua come pure il recapito delle persone che li accompagnano presso l'aeroporto di partenza e di destinazione;
- **persone disabili:** sebbene di solito i dati PNR non contengano direttamente indicazioni sulla disabilità delle persone, il trasporto di una sedia a rotelle potrebbe permettere di intuirlo. Quest'informazione resta tuttavia una supposizione e non è registrata sistematicamente.

Fasi del trattamento

Il vantaggio principale del trattamento dei dati da parte dello Stato risiede nella possibilità di adottare tempestivamente misure preventive e repressive per prevenire o perseguire il terrorismo e altri reati gravi.

Non appena l'UIP riceve i dati PNR, questi sono confrontati automaticamente con i sistemi d'informazione di polizia, le liste d'osservazione e i profili di rischio. In questo modo è possibile individuare sia potenziali minacce riconducibili al terrorismo e alle gravi forme di criminalità sia persone ricercate a livello nazionale o internazionale che sono sospettate di aver commesso simili reati o che sono state condannate a lunghe pene detentive per un simile reato. I dati che durante il confronto non hanno generato alcuna corrispondenza, sono pseudonimizzati dopo un mese e cancellati automaticamente dopo ulteriori cinque mesi. I dati che hanno prodotto una corrispondenza sono comunicati alle autorità competenti (autorità di polizia, autorità di perseguimento penale e servizi delle attività informative della Confederazione e dei Cantoni) e contrassegnati. I dati contrassegnati possono essere conservati per un periodo massimo di cinque anni.

Dopo il confronto automatico, il trattamento dei dati PNR avviene soltanto in singoli casi quando un'autorità competente ne richiede la comunicazione.

Nel trattamento sono coinvolte collaboratrici e collaboratori dell'UIP e delle autorità competenti della Confederazione e dei Cantoni. Visto che annualmente vengono trattati dati di milioni di passeggeri, il numero dei processi di trattamento è molto elevato. Per il trattamento dei dati sono impiegate tecnologie sofisticate e un sistema PNR collaudato dell'ONU. Non è previsto il ricorso all'intelligenza artificiale in tale settore e tutte le misure sono eseguite nel rigoroso rispetto delle prescrizioni legali e degli standard in materia di protezione dei dati.

Inoltre, l'UIP comunica al Servizio delle attività informative della Confederazione i dati PNR relativi a determinate rotte aeree giudicate a rischio, definite dal Consiglio federale, affinché possa trattarli autonomamente.

Rischi individuati

La VIPD ha identificato un totale di 14 rischi sistemici per i diritti fondamentali delle persone coinvolte. I rischi possibili sono rappresentati in particolare:

- dall'accesso non autorizzato ai dati PNR;
- dall'errata classificazione di persone o da dati contrassegnati in modo errato a causa di informazioni incomplete o di insufficiente qualità dei dati;
- dal trattamento non autorizzato di dati personali degni di particolare protezione.

Misure per la riduzione dei rischi

La VIPD ha individuato complessivamente 22 misure in grado di ridurre in maniera efficace i rischi individuati a un rischio residuo ragionevole.

Queste misure sono di natura giuridica, organizzativa e tecnica e mirano a ridurre la probabilità di accadimento e l'entità dei danni legate ai rischi.

Di seguito sono riportati alcuni esempi che illustrano come le misure siano in grado di influenzare il rischio residuo.

- **I controlli più rigorosi degli accessi e le misure tecniche di sicurezza** quali le procedure più efficienti di verifica e di verbalizzazione aiutano a evitare l'accesso non autorizzato ai dati PNR, riducendo il rischio di violazioni della protezione dei dati.
- **Le formazioni regolari destinate alle collaboratrici e ai collaboratori aumentano la consapevolezza e la competenza nel trattare dati sensibili**, contribuendo a ridurre gli errori umani che potrebbero condurre a violazioni della protezione dei dati.
- **I miglioramenti tecnologici e le verifiche regolari del sistema**, compresi i test di penetrazione e le verifiche dell'integrità dei dati, garantiscono la sicurezza e il corretto funzionamento dei sistemi, diminuendo il rischio di guasti tecnici.
- **La chiarezza delle direttive giuridiche e organizzative** assicurano una migliore compliance e una maggiore responsabilità all'interno dell'organizzazione, contribuendo a ridurre i rischi giuridici e operativi.
- **La minimizzazione dei dati e le migliori pratiche in materia di protezione dei dati**, quali la cancellazione automatica o la pseudonimizzazione dei dati alla scadenza dei termini previsti, contribuiscono a ridurre il rischio di utilizzo abusivo di vecchi dati o di dati non più necessari.

L'attuazione di queste misure è fondamentale per garantire la sicurezza e la protezione dei dati personali trattati.

Valutazione da parte dell'IFPDT

L'IFPDT ha esaminato la presente VIPD e ha constatato nel suo parere di aprile 2024 che:

- la VIPD è stata allestita accuratamente;
- le informazioni necessarie per la valutazione sono disponibili;
- i rischi menzionati per la personalità o i diritti fondamentali delle persone interessate coprono l'intero processo di trattamento dei dati previsto dalla LDPA;
- nel caso dovessero emergere diversi altri rischi elevati, sono previste misure appropriate di riduzione dei rischi.

Ulteriori informazioni

Il documento completo «Datenschutz-Folgeabschätzung PNR Schweiz» è disponibile su richiesta al seguente indirizzo e-mail: pnr@fedpol.admin.ch.